

2015

# Authentication Aura: A cooperative and distributed approach to user authentication on mobile devices

Hocking, Christopher George

<http://hdl.handle.net/10026.1/3469>

---

<http://dx.doi.org/10.24382/4799>

Plymouth University

---

*All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.*

# Authentication Aura

*A cooperative and distributed approach to user authentication on mobile devices*

by

Christopher George Hocking

A thesis submitted to the Plymouth University in partial fulfilment for the degree of

Doctor of Philosophy

School of Mathematics and Computing

December 2014

## ***Copyright Statement***

---

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior consent.

## ***Abstract***

---

As information technology pervades our lives we have increasingly come to rely on these evermore sophisticated and ubiquitous items of equipment. Portability and the desire to be connected around the clock has driven the rapid growth in adoption of mobile devices that enable us to talk, message, tweet and inform at will, whilst providing a means to shop and administer bank accounts. These high value, high risk, desirable devices are increasingly the target of theft and improvement in their protection is actively sought by Governments and security agencies. Although forms of security are in place they are compromised by human reluctance and inability to administer them effectively. With typical users operating across multiple devices, including traditional desktop PCs, laptops, tablets and smartphones, they can regularly find themselves having a variety of devices open concurrently. Even if the most basic security is in place, there is a resultant need to repeatedly authenticate, representing a potential source of hindrance and frustration.

This thesis explores the need for a novel approach to user authentication, which will reduce the authentication burden whilst providing a secure yet adaptive security mechanism; a so called Authentication Aura. It proposes that the latent security potential contained in surrounding devices and possessions in everyday life can be leveraged to augment security, and provides a framework for a distributed and cooperative approach. An experiment was performed to ascertain the technological infrastructure, devices and inert objects that surround individuals throughout the day. Using twenty volunteers, over a fourteen-day period a dataset of 1.57 million recorded observations was gathered, which confirmed that between 6am and 12pm a significant device or possession is in near proximity 97.84% of the time.

Using the data provided by the experiment as the basis for a simulation of the framework, it suggests a reduction of up to 80.36% in the daily number of required authentications for a user operating a device once every 30 minutes, with a 10 minute screen lock in place. Examining the influence of location alone indicated a reduction of 50.74% in user interventions lowering the average from 32 to 15.76, the addition of the surroundings reducing this further to 13.00.

The analysis also investigated how a user's own authentication status could be used to negate the need to repeatedly manually authenticate and it was found that it delayed the process for up to 90 minutes for an individual user. Ultimately, it confirms that during device activation it is possible to remove the need to authenticate with the Authentication Aura providing sufficient assurance.

# ***Table of Contents***

---

List of Figures .....	iv
List of Tables.....	vii
List of Equations .....	viii
Acknowledgements.....	ix
Author’s Declaration .....	x
1. Introduction and Overview .....	1
1.1 Mobile Insecurity.....	1
1.2 Motivation.....	2
1.3 Aims and Objectives.....	3
1.4 Thesis Structure.....	3
2. Personal Electronic Devices .....	7
2.1 Evolution of Mobile Phones .....	7
2.2 Service Access.....	10
2.3 Current Security Approaches and Limitations.....	12
2.4 Summary .....	18
3. Identification and Authentication.....	21
3.1 Identity .....	21
3.1.1 Philosophical and Psychological Identity .....	21
3.1.2 The Person and Their Environment .....	25
3.1.3 Affordance.....	26
3.1.4 Summary .....	28
3.2 Individuation.....	28
3.3 Identification and Authentication .....	29
3.3.1 Knowledge Based Authentication.....	29
3.3.2 Possession Based Authentication .....	33
3.3.3 Physical Trait Authentication .....	34
3.3.3.1 Negative Identification.....	39
3.3.3.2 Physiological and Behavioural.....	40
3.3.3.3 Resistance to Attack.....	41
3.3.3.4 Privacy .....	41
3.3.3.5 Multimodal Biometrics.....	42
3.3.3.6 Current Implementation .....	43
3.3.3.7 Summary .....	52
3.3.4 Polled and Non-polled.....	53
3.4 Conclusion .....	54
4. A New Approach to Authentication.....	57
4.1 The Concept of an Authentication Aura.....	57
4.2 Justification of the Aura Concept .....	59
4.2.1 Experiment Design .....	60
4.2.2 Gathered Data.....	65
4.2.3 Data Analysis .....	68
4.2.4 Discussion.....	77
4.3 Conclusion .....	78
5. Elements of an Authentication Aura.....	81

---

5.1	Inter-Device Trust.....	83
5.2	Functional Requirements .....	83
5.2.1	Non-intrusive .....	84
5.2.2	Flexible metrics .....	85
5.2.3	Rigorous authentication.....	86
5.2.4	Supports multiple identities.....	86
5.3	Influence of Location.....	87
5.4	Taxonomy of Device Interaction .....	87
5.4.1	Own New or Un-trusted Device .....	88
5.4.2	Own Trusted and Established Device.....	88
5.4.3	Alien New or Un-trusted Device .....	89
5.4.4	Alien Trusted and Established Device .....	89
5.4.5	Shared Computational Capability .....	90
5.5	Degradation of Confidence .....	90
5.6	Information Policy .....	94
5.7	Data communication .....	96
5.8	Summary .....	97
6.	Authentication Aura Framework .....	100
6.1	Anatomy .....	101
6.2	Sensor.....	104
6.2.1	Message Cache data table (cache).....	105
6.2.2	Authentication Sample data table (auth).....	109
6.2.3	Message identification and format.....	110
6.2.4	Intelligent device monitoring .....	112
6.2.5	Token device monitoring .....	112
6.2.6	Infrastructure monitoring .....	112
6.2.7	Sensor logic .....	112
6.3	Authentication Manager .....	114
6.4	Message Transmitter.....	115
6.5	Policy Manager.....	116
6.5.1	System parameters .....	116
6.5.2	System parameters data table (param) .....	119
6.5.3	Location data table (location) .....	120
6.6	Device Manager.....	122
6.6.1	Device data table (device).....	122
6.6.2	Device discovery and validation.....	125
6.6.3	Device maintenance.....	126
6.7	Aura Manager.....	127
6.7.1	Aura data table (aura) .....	127
6.7.2	Received messages .....	130
6.7.3	Message processing .....	130
6.7.3.1	Authenticated (AUT) .....	130
6.7.3.2	Are You There (AYT) and I am Still Here (ISH) .....	131
6.7.3.3	I Am Here (IAH) .....	132
6.7.3.4	Who Is There (WIT) .....	132
6.7.3.5	What is Your Status (WYS), My Status Is (MSI) and PENding (PEN) .....	133
6.7.4	Member status.....	134
6.7.5	Generated messages.....	135
6.7.6	Aura Manager logic.....	136
6.7.6.1	Process Message sub-process .....	137

---

---

6.7.6.2 Add Aura Device sub-process.....	138
6.7.6.3 Issue Message sub-process .....	138
6.7.6.4 Monitor Aura sub-process and Check Intelligent Device sub-process..	140
6.8 Confidence Monitor .....	143
6.9 Aura Security Manager (ASM).....	145
6.10 System Security Interface.....	146
6.10.1 System Security data table (security).....	146
6.10.2 System Security Interface logic .....	149
6.11 Summary .....	150
7. Evaluation of an Authentication Aura.....	152
7.1 Authentication Aura Simulation.....	155
7.2 Assessment of Extended Simulation Results.....	170
7.3 Lexical Emulation.....	175
7.4 Summary .....	177
8. Conclusion.....	180
8.1 Fulfilment of the Aims and Objectives .....	181
8.2 Research Limitations .....	183
8.3 Future Work .....	184
8.4 The Future for User Authentication on Mobile Devices .....	185
References.....	188
Appendix A. PDA Software .....	205
Appendix B. MATLAB Simulation Script.....	210
Appendix C. Publications .....	219
Appendix D. Experiment Instructions .....	262
Appendix E. Ethical Approval Form .....	272
Appendix F. Data Disc Index.....	293

## List of Figures

---

Figure 2-1. Worldwide mobile phone sales in millions per quarter 2009-13 .....	10
Figure 2-2. Profile of app usage by UK smartphone owners.....	12
Figure 2-3. An example of screen pattern security .....	14
Figure 2-4. A user scanning their fingerprint on a Samsung Galaxy S5.....	15
Figure 2-5. Google Android's face unlock feature © Google.....	16
Figure 3-1. Diagrammatic representation of a person's interaction with their environment ....	27
Figure 3-2. Detection of Unique Phishing Sites.....	31
Figure 3-3. Lloyds bank token based authentication screen.....	34
Figure 3-4. A simplified biometric system.....	35
Figure 3-5. Typical measurements taken during facial recognition.....	36
Figure 3-6. Biometric system performance rates.....	37
Figure 3-7. How the threshold affects the Impostor and Genuine error distributions .....	38
Figure 3-8. Illustration of error tolerated within different application scenarios .....	38
Figure 3-9. The human vocal tract .....	44
Figure 3-10. A digital fingerprint scanner.....	45
Figure 3-11. Steps taken to encode a fingerprint scan .....	46
Figure 3-12. Illustration of a human eye showing the iris and pupil.....	48
Figure 3-13. An iris scan showing the vector regions and derived IrisCode .....	49
Figure 3-14. An example of a palm vein reader .....	50
Figure 3-15. Subdivisions of human gait used for categorisation and identification .....	51
Figure 4-1. The concept of an Authentication Aura demonstrating contributing elements .....	58
Figure 4-2. A PDA with installed RFID node and five RFID tags.....	63
Figure 4-3. User 3's completed tag location form.....	65
Figure 4-4. Subject 3's tag data file sample showing tag id, user, date, time, sequence & strength .....	66
Figure 4-5. A typical subject's weekday observations.....	68
Figure 4-6. The same typical user's weekend observations.....	69
Figure 4-7. Number of detected devices as a percentage of total listens for all participants ....	71
Figure 4-8. A single user's specific device observations during the experiment .....	72
Figure 4-9. A user's isolated single weekday activity .....	73
Figure 4-10. The same user's isolated single weekend day activity.....	73
Figure 4-11. Daily activity for a poor performing experiment subject.....	74
Figure 4-12. Percentage share of each category of detected items .....	74
Figure 5-1. Varying levels of device sophistication and consequent contribution to the Aura..	81
Figure 5-2. The potential inter-device relationship and authentication techniques .....	82

---

Figure 5-3. Graphs of varying approaches to confidence degradation over time .....	91
Figure 5-4. A combination of confidence degradation approaches over time .....	92
Figure 5-5. Confidence graphs illustrating the influence of location .....	93
Figure 5-6. Confidence graphs illustrating the effect of different authentication methods .....	93
Figure 5-7. Comparison of iterative and non-iterative confidence calculation .....	94
Figure 6-1. Authentication Aura implementation framework .....	101
Figure 6-2. Generic message structure .....	111
Figure 6-3. Sensor process flowchart .....	113
Figure 6-4. Example of a My Status Is (MSI) message .....	116
Figure 6-5. Relationship between the device and location data tables .....	123
Figure 6-6. Device Manager flowchart .....	126
Figure 6-7. Relationship between the location, device and aura data tables .....	129
Figure 6-8. Authenticated message syntax and effect (AUT) .....	131
Figure 6-9. Are You There message syntax and effect (AYT) .....	131
Figure 6-10. I Am Here message syntax and effect (IAH) .....	132
Figure 6-11. Who Is There message syntax and effect (WIT) .....	133
Figure 6-12. What Is Your Status message syntax and effect (WYS) .....	134
Figure 6-13. Aura member status state chart .....	135
Figure 6-14. Aura Manager operational overview .....	136
Figure 6-15. Process Message sub-process flowchart .....	137
Figure 6-16. Add Device sub-process flowchart .....	139
Figure 6-17. Issue Message sub-process flowchart .....	140
Figure 6-18. Monitor Aura sub-process .....	141
Figure 6-19. Check intelligent device sub-process .....	142
Figure 6-20. Confidence Monitor flowchart .....	144
Figure 6-21. Aura Security Manager flowchart .....	145
Figure 6-22. System Security Interface flowchart .....	149
Figure 7-1. Control plot of user identity confidence on a device with a 10 minute screen lock .....	157
Figure 7-2. Degrading confidence whilst away from home .....	159
Figure 7-3. Degrading confidence whilst at home .....	159
Figure 7-4. Subject 3's devices detected during the day selected for simulation (day 9) .....	161
Figure 7-5. Simulated Authentication Aura results for subject 3 on the same day .....	161
Figure 7-6. A comparative user's weekend Authentication Aura profile (user 9, day 14) .....	162
Figure 7-7. Intelligent device contribution 10 .....	163
Figure 7-8. Intelligent device contribution 20 .....	163
Figure 7-9. Intelligent device contribution 30 .....	163
Figure 7-10. Intelligent device contribution 40 .....	163

---

Figure 7-11. Intelligent device contribution 50..... 163

Figure 7-12. Token device contribution 0.75 ..... 164

Figure 7-13. Token device contribution 1.5 ..... 164

Figure 7-14. Token device contribution 2.25 ..... 164

Figure 7-15. Token device contribution 3.0 ..... 164

Figure 7-16. Maximum token contribution 10 ..... 165

Figure 7-17. Maximum token contribution 20 ..... 165

Figure 7-18. Maximum token contribution 30 ..... 165

Figure 7-19. Maximum token contribution 40 ..... 165

Figure 7-20. Maximum token contribution 50 ..... 165

Figure 7-21. Subject 3 on the same day with increased location weightings ..... 166

Figure 7-22. User 3 on the simulated day with an increased authentication threshold ..... 167

Figure 7-23. Illustration of user 3 with a location based variable authentication threshold.... 168

Figure 7-24. Simulated host device theft from subject 3 at 2.01pm on the same day..... 168

Figure 7-25. Illustration of initial authentication being delayed..... 169

Figure 7-26. Example of a device that becomes inactive part way through a day ..... 174

Figure 7-27. Screen capture during operation of the lexical emulation ..... 176

Figure 9-1. The visual basic form associated with the PDA software ..... 209

## ***List of Tables***

---

Table 2-1. Mobile device assets with associated risk level .....	11
Table 3-1. Identity matrix person-centric indicators.....	26
Table 3-2. Identity matrix environment indicators .....	26
Table 3-3. List of ten most and least popular passwords.....	30
Table 3-4. Outline of multimodal biometric implementation.....	43
Table 3-5. Criteria comparison of discussed biometric techniques .....	52
Table 4-1. The corresponding cross referenced detail.....	66
Table 4-2. Quantities of recorded readings for each of the twenty experiment participants....	67
Table 4-3. Subject 14's average number of detections in each half hour period .....	70
Table 4-4. Number of detected devices on each listen, combined into experiment groups.....	71
Table 4-5. Percentage of infrastructure detections by subject.....	75
Table 4-6. Percentage of dumb, intelligent and infrastructure items when only a single one identified .....	76
Table 4-7. Percentage of mixed types of detections by subject .....	76
Table 5-1. The key ISO Biometric standards defined by ISO committee SC37 .....	84
Table 5-2. Summary of locations.....	92
Table 6-1. Database structure .....	102
Table 6-2. Message cache data table definition .....	107
Table 6-3. Authentication sample data table definition .....	108
Table 6-4. Message acronyms.....	111
Table 6-5. Vocabulary syntax and transmitted detail .....	115
Table 6-6. Extract from the System parameter data table .....	120
Table 6-7. System parameter data table definition .....	121
Table 6-8. Location data table definition .....	121
Table 6-9. Example of the Location data table at system installation .....	122
Table 6-10. Device data table definition .....	124
Table 6-11. Temporary Aura data table definition.....	128
Table 6-12. System Security data table definition .....	148
Table 7-1. List of parameter values used in the simulation .....	158
Table 7-2. Subject 3's tagged equipment and associated rankings .....	160
Table 7-3. The number of simulated authentications shown per user per day.....	171
Table 7-4. The number of simulated authentications with higher location tariffs shown per user per day.....	172
Table 7-5. The number of simulated authentications with higher location tariffs but without influence from the Aura .....	173

## ***List of Equations***

---

Equation 5-1. Relationship between time and identity confidence .....	91
Equation 5-2. The core confidence calculation equation .....	93
Equation 5-3. The contribution to confidence made by an intelligent device.....	95
Equation 5-4. The contribution to confidence made by an inert device .....	95
Equation 5-5. Combined identity confidence equation .....	97
Equation 7-1. Combined identity confidence equation .....	152
Equation 7-2. Core confidence calculation .....	153
Equation 7-3. Calculation of the current time iteration.....	153
Equation 7-4. Intelligent device contribution .....	154
Equation 7-5. Dumb device contribution .....	155

## *Acknowledgements*

---

I firstly want to acknowledge the unwavering support of my supervisory team Professors Steven Furnell, Nathan Clarke and Paul Reynolds. Without their timely guidance and help I am sure I would not have negotiated the maze of daunting bewilderment that is a PhD. I have not always been the most visible of students but without question they have made themselves available when needed and at no time questioned my commitment. During the course of my study I have encountered numerous bouts of ill health which have undoubtedly impacted upon my research and stunted my progress but at these times they have willingly given me the extra support I required, enabling me to hit publication deadlines. For all of this I am forever grateful.

I also wish to thank Orange-France Telecom for the sponsorship they have so generously given, providing a means for me to study and attend conferences. I hope they will find the work contained within this thesis of value to their ongoing research and trust they are satisfied with the delivered outcomes.

The help, advice and support given by my friends in A304 Portland Square has provided encouragement when needed and grounding when deserved. I wish to acknowledge Dr Mark Culverhouse, Dr Ibrahim Zincir and especially Dr Fudong Li who all befriended this old and greying student with understanding and unreserved help, encouraging me to finally reach this goal, with generosity and without expectation. I thank you all this day, tomorrow and beyond.

Living a less than regular life and requiring a lot of help in and around the home, my heartfelt gratitude is also extended to 'H' and the team who support me on a daily basis. They have nagged when needed, consoled when appropriate and learned to keep quiet in moments of stress. Without them my life would be far from easy, so although I say "thank you to you all" it is meant in a way that conveys so much more.

Finally my unreserved love, thanks and admiration must go to my parents, Ruth and Roy. The immeasurable love, support and encouragement through this and the rest of my life has given me the foundation and belief to achieve so much. Any success I may encounter is fundamentally down to them and for that I am and will be eternally grateful. I dedicate this tome to you both and trust the pride it gives will provide you with strength in the months and years to come.

## ***Author's Declaration***

---

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

Work submitted for this research degree at the Plymouth University has not formed part of any other degree either at Plymouth University or at another establishment

This study was financed with the aid of sponsorship from Orange-France Telecom.

Relevant scientific seminars and conferences were attended at which work was often presented; external institutions were visited for consultation purposes and several papers prepared for publication.

### Publications:

Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2010), 'A distributed and cooperative user authentication framework', *6th International Conference on Information Assurance and Security (IAS 2010), Atlanta, USA, 23-25 August 2010*, pp. 304-310.

Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2011), 'Authentication Aura - A distributed approach to user authentication', *Journal of Information and Assurance*, vol. 6, iss.2, pp. 149-156.

Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2011), 'A preliminary investigation of distributed and cooperative user authentication', *Proceedings of the 9th Australian Information Security Management Conference (secAU 2011), Perth, Australia, 5-7 December 2011*.

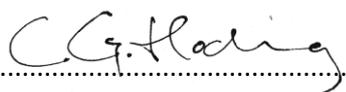
Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2013), 'Co-operative user identity verification using an Authentication Aura', *Computers and Security*, vol. 39, part B, pp. 486-502.

### Presentations:

Sixth International Conference on Information Assurance and Security (IAS 2010), Atlanta, USA, 23-25 August 2010.

Sixth Collaborative Research Symposium on Security, E-learning, Internet and Networking (SEIN 2010), University of Plymouth, UK, 25-26 November 2010.

9th Australian Information Security Management Conference (secAU 2011), Perth, Australia, 5-7 December 2011.

Signed .....  .....

Date ..... 16<sup>th</sup> December 2014 .....

---

# **Chapter 1**

## **Introduction and Overview**

---

# 1. Introduction and Overview

---

In the fast paced world that exists today individuals are utilising mobile electronic equipment consistently throughout their daily lives both whilst at work and during their leisure time. On average users are reported as accessing their mobile phones (or cell phones as they are known in America) more than 1,500 times a week and it has become the de facto “go-to-gadget” of choice (Woolaston, 2014). These highly desirable expensive devices are becoming fashion icons and inhabit an evermore centric role in 21<sup>st</sup> Century life. The research presented in this thesis is aimed at improving the protection of these valuable items and the personal information they hold by producing a novel and robust approach to mobile device security that will adapt to location, and leverage the detected presence of other personal items and equipment that are ported on a daily basis.

This chapter will introduce weaknesses in the current security methodology and how users and even governments are unanimously calling for improvements to be made. It will then proceed to further describe the motivation for this research, its aims and objectives and finally outline the structure of this document.

## ***1.1 Mobile Insecurity***

As smart phones and other sophisticated mobile items are widely adopted, technological boundaries are stretching and the devices are evolving with expanding storage capabilities and processing power, enabling the porting of greater amounts of information and personal details. With this becoming the norm for us all, these expensive personal items are an ever-growing target for theft, and the consequence of loss is increasingly severe (CPP, 2010; Home Office, 2009). In 2012 more than 10,000 handsets per month were reported stolen in London every month, a rise of 12% on the previous year (Prynn, 2013). Correspondingly in the USA as a whole more than 3,000,000 devices were stolen in 2013, although 44% of these were because the owner had unwittingly left the item in a public place (Eadicicco, 2014). With the scale of these figures commonplace the consequential requirement to protect and secure the potentially large volumes of sensitive and personal information contained within these desirable pieces of equipment is imperative, and even acknowledged and supported by Government (DARPA, 2012; Design Council, 2010; Rohde, 2001).

Authentication of the user’s identity by any device provides the first line of defence in the battle to maintain data confidentiality following theft or loss. Although different, identification and authentication both rely upon the recognition of the identity of a user interacting with a device at any given moment. Hand held mobile devices typically assume the identity of the

user and utilise personal identification numbers (PINs) to authenticate this at point-of-entry, a documented frailty (Clarke, 2011; Vu et al., 2007). Establishing as far as possible that the operator is whom they purport to be provides a device with the necessary degree of confidence to allow unrestricted access and service utilisation. Once access has been gained the ability to view emails, activate banking apps and view sensitive documents is readily available without further challenges being made. However, although steps have been taken to ensure the devices are only accessed by accredited individuals, the ubiquitous point of entry user identity code and password has been rendered susceptible to abuse through the inability or unwillingness of individuals to protect and administer this sensitive information correctly (Albrechtsen, 2007; Clarke and Furnell, 2005). Indeed a survey in 2013 revealed that 36% of mobile phone users had not activated either password or PIN protection for their mobile phone, and 30% of respondents admitted attempting to hide passwords in notes held on the device (Siciliano, 2013).

The current inadequacy of security on mobile devices and the inherent risk to personal information provided the primary motivation for this research. However, during the initial phases other potential benefits such as delaying authentication whilst maintaining high security materialised and are now described in the following section.

## ***1.2 Motivation***

As introduced above the threat of theft, forgetfulness or individuals' lackadaisical approach to the protection of their mobile devices has provided the majority of motivation to undertake this research. Additionally, with the repeated use of mobile devices throughout the day and the requirement for many to utilise PCs and other equipment requiring authentication to be performed, the recurring intrusive accreditation process becomes laborious and inconvenient. The implementation of security is a necessity but the consequence of doing so maybe a factor in the observed reticence of many to use it. There must be a route via which this burden can be lessened without negatively affecting the level of security being provided.

People regularly carry a number of electronic devices and pseudo intelligent items such as contactless payment cards simultaneously during everyday life. This personal bubble of technology and possessions travels with the individual throughout their waking hours and is omnipresent even when they sleep. As disparate items, each in its own right is vulnerable and exists in isolation. However, if a cooperative route could be identified that would enable these pieces of equipment and possessions to know about each other, reassurance could be imparted and leveraged to bolster security. As a caveat to this, if communication channels

were established it should also be possible for sophisticated devices to perform authentication on behalf of items that are unilaterally incapable of doing so, enhancing their security.

The final factor that has directed this research is the movement of people throughout their daily lives. Typically they commence their day at home, have a period at work either in a specific locale or whilst remaining mobile, and then return home again in the evening. Current security treats all situations and locations identically; it is a one-size-fits-all approach that with modern technology and associated processing power need not be the case. It is reasonable to propose that a device's security can be more relaxed when in familiar surroundings, yet exhibit heightened levels of caution when in an alien environment.

In summary the motivations for this research are improved convenience, adaptability and robustness whilst producing a security approach that is easy to utilise but cooperates with the user, their working practices and their environment.

### ***1.3 Aims and Objectives***

The aim of this research is to produce a novel method of security that will provide the user with heightened confidence, yet lessen the burdensome inconvenience of performing repeated authentication across multiple devices, whilst improving overall device security. It investigates current techniques employed on mobile devices, identifying shortcomings before proposing a novel solution and approach that will enable simulation and analysis to be performed, whilst providing a route to prototype production.

The objectives for this solution are drawn from the motivations outlined in section 1.2, the detail above and are presented in the following points:

1. To fully investigate the true meaning of identity and the current approaches to authentication.
2. To assess the potential held in users' equipment and possessions to provide information that can be leveraged for security enhancement.
3. To design an architecture that will enhance device security via mobile devices and personal items, that is resilient to equipment development and will incorporate new and emerging authentication techniques.
4. To simulate and evaluate a security mechanism that will cooperate with familiar trusted devices, adapt to location and adjust security responses accordingly.

### ***1.4 Thesis Structure***

To fulfil the aims and objective stated in section 1.3 this thesis commences in Chapter 2 by investigating the development of personal electronic equipment from its humble beginnings to

the near ubiquitous adoption that it has today. It examines current approaches to security and the risks associated with the information contained within and devices' installed applications.

Chapter 3 then explores the true meaning of the term identity from philosophical, psychological and technological standpoints, to establish the elements that combine to make one individual distinguishable from another. The section then continues to outline the fundamentals of authentication and explores the techniques that are currently employed upon state-of-the-art devices.

Continuing from this, Chapter 4 introduces the concept of a new approach to cooperative security that utilises surrounding devices, personal items and the user's current location. To ascertain the potential contained within these elements the chapter details an experiment that has been performed in cooperation with 20 volunteers, who were recruited in four groups of five individuals, with each participating continuously for two weeks. Analysing the gathered data it investigates the significance of the findings and establishes if there is unharnessed potential that can be leveraged, and the categories of items that can be used.

Chapter 5 builds upon the experiment and further explains the general concept, outlining the requirements that must be met. It then investigates elements of cooperation and how information can be exchanged between devices. It also discusses erosion of service availability over time and the influences that will contribute to this function and even potentially reverse the process.

The framework is presented in great detail in Chapter 6. All the logical elements are described, the anatomy required to produce a functioning agent is illustrated, and the vocabulary for efficient and effective communication specified. The framework is neatly divided into individual autonomous sub-agents that have designated functions, are easy to develop, yet unite to provide an effective solution to the aims and requirements outlined in Chapters 4 and 5.

Chapter 7 utilises mathematical modelling software to simulate an operational framework and assess its efficacy. It utilises the data gathered during the experiment to simulate authentication requests and graphically illustrates how service availability can indeed be made dependent upon the elements discussed above. Mathematical analysis quantifies the potential improvement achieved through the implementation of this novel approach to security and reports significant reduction in quantity of authentications that a typical user might expect to make. Device cooperation and the messaging system are also validated, laying the foundation for further work.

Finally, Chapter 8 reviews the detailed research and assesses how the aims and objectives have been met. It further recounts difficulties that were encountered during the undertaken work and how they may have influenced the produced results. It concludes by suggesting research that can continue beyond the findings detailed in the preceding chapters and work that is currently beyond the scope of this document.

---

## **Chapter 2**

# **Personal Electronic Devices**

---

## 2. Personal Electronic Devices

---

Modern computing can be traced back to Charles Babbage's model of a mechanical calculating device or "difference engine" which he proposed to the Royal Astronomical Society in 1822 (Computing History, 2012; MacTutor, 1998). However, it was not until the launch of R2E's Micral in 1973 and the Scelbi "personal computer" kit in March 1974 that computing truly became personal (Bellis, nd; Howard-Spink, 2008; Freiburger, 2013). In comparison, mobile communication finds its roots in recent history when the first vehicle based telephone call was made on 17 June 1946 (AT & T, 2012) although it was not until 1979 that the first commercial cellular telephone network was launched in Tokyo (Connected Earth, nd). Ameritech took a further four years to open the first American based service in Chicago (Connected Earth, nd) and the UK two years more, when in January 1985 Vodafone and Cellnet launched their respective networks (Salford, 2010).

From these humble and very different beginnings personal electronic devices have converged and developed into the sophisticated and computationally powerful devices that are ever present in today's connected world. For the invention of the integrated circuit in 1958 and its successors miniaturisation has been the evolutionary catalyst (Fairchild Company History, 2014; IEEE Global History Network, 2013), supported by Moore's Law that correctly predicted the exponential rise in computational power for minimal extra cost (Moore, 1965; Moore 1975).

This chapter starts by examining the development of the mobile phone and how the technological improvements have been reflected in the astronomical rise in worldwide sales. With the security of these devices being of utmost importance, the next section reviews service access and how devices generally operate on an "authenticate-and-forget" (Clarke, 2011, p.216) principle. A thorough review of current approaches to device security is then made, outlining weaknesses in both employed techniques and device design, and providing a comprehensive understanding of the state-of-the-art. Finally the chapter concludes with a summary of the presented information and indicates how it forms a basis for this research.

### ***2.1 Evolution of Mobile Phones***

The mobile phone has been subject to a rapid evolutionary process during the past forty years. The drive to innovate has been the desire to miniaturise whilst providing increased battery life and corresponding talk-time. The disappearance of the pavement based telephone box is apparent to the majority of the population within the UK, further underlying the speed of the technology's adoption and how it has become a ubiquitous accessory for most. This section

briefly reviews the history of the mobile phone, examining the development in technology and illustrating its global spread.

On 3<sup>rd</sup> April 1973 Motorola's inventor of the mobile phone made the first call choosing his perceived chief rival at Bell laboratories to receive it. On that day Martin Cooper dialled Joel Engel and is reported as saying: "Joel, this is Marty. I'm calling you from a cell phone, a real handheld portable cell phone" (Seltzer, 2013). This historical event was undertaken on the first mobile phone weighing over 1.1kg, with a maximum talk time of 30 minutes, was 250mm in length and took over 10 hours to recharge; not a convenient pocket sized device (Goodwin, 2013).

In the USA the potential for commercial mobile phone use was unleashed when the Federal Communications Commission allocated analogue frequencies upon which the networks would operate in 1982, establishing the parameters for the first generation or 1G technology (Kaur et al., 2011). The following year, the first commercial model not designed for a car was produced by Motorola, the DynATAC (Dynamic Adaptive Total Area Coverage) 8000X (Motorola, 2014). "The Brick" as it became fondly known on release cost \$3,995 (\$8,700 at today's prices), could store 30 numbers and had a talk time of 30 minutes (Buck, 2013; Goodwin, 2013).

1989 witnessed the first flip phone, the Motorola Microtac 9800X; a pocket sized device that was easily transportable although the convenience still came with a high cost to the consumer, a price tag of \$3,000 (CBR, 1989; Motorola, 2014). Until this point mobile phone communication had been restricted to within regional borders. However in 1991 this changed when Motorola demonstrated the first Global System for Mobile (GSM) communication working prototype in Hanover. This second generation or 2G of mobile phones brought additional capabilities; text, picture and multi-media messages became standard and text messages now had the additional advantage of being encrypted (HSW, 2000; Kaur et al., 2011; Motorola, 2014).

In 1993 technology took another step forward when collaboration between Bellsouth and IBM introduced the Simon personal communicator costing \$899. This was the first to exhibit additional smartphone capabilities such as a stylus controlled calendar, e-mail, calculator and clock; setting a new benchmark for the competition (MPN, 1993; Sager, 2012). Mobile phones started to crossover into the world of fashion as prices fell and they came within affordable reach of the image conscious younger population. In 1998 Nokia launched their 5100 model which came with colourful snap-on covers, giving the owners the ability to personalise their mobile to a small degree (Salford, 2010).

The new millennium saw the introduction of the 3G technological specification, supporting mobile and fixed wireless internet access, video calls and mobile television (Kaur et al., 2011). Additionally, the first mobile phone to be sold with embedded Bluetooth technology, the Ericsson T36 was shipped with tri-band GSM capability and ready for Wireless Application Protocol (WAP) (Rohde, 2000). This meant that it could be used across all three GSM regions and was able to browse information from the emerging internet whilst on the move. Another first for 2000 saw Samsung releasing the first phone with an in-built camera, when in June they brought the SCH-V200 to market in South Korea (Hill, 2013; Salford, 2010).

2005 witnessed the introduction of to date the largest selling mobile phone of all time, the Nokia 1110; it subsequently sold an enormous 250 million units and exhibited an incredible standby time of up to 380 hours (Delaney, 2013; GSM Arena, 2014; Telegraph, 2013).

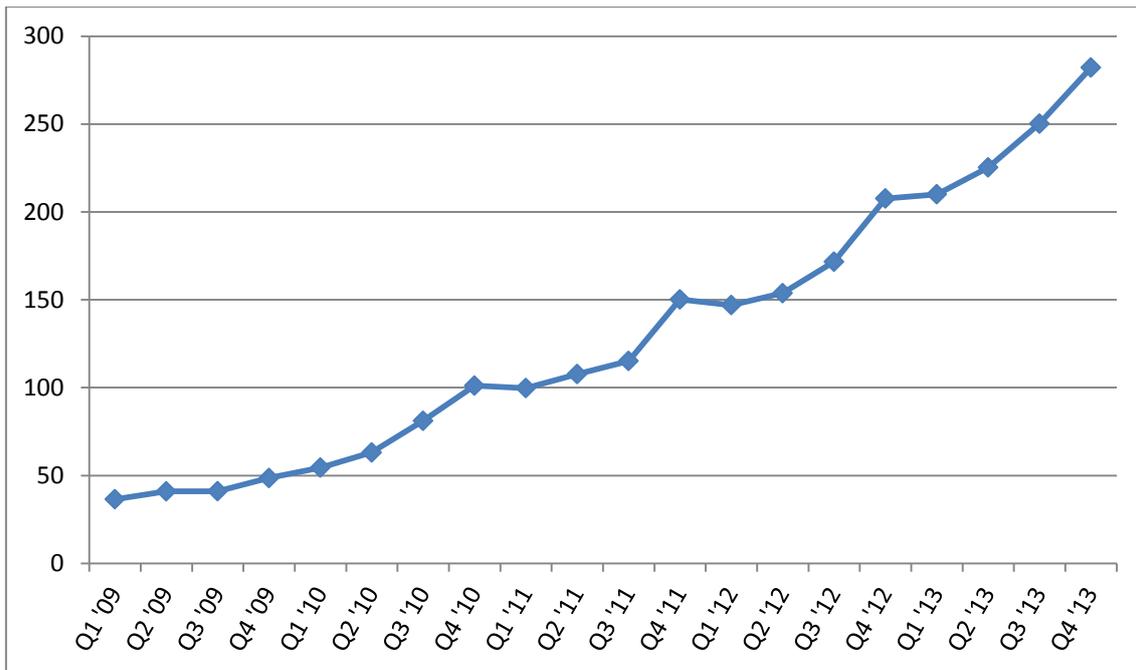
In 2007 the smartphone truly arrived when Apple ventured into the mobile phone market and released the iPhone running the iPhone OS (Apple, 2010). Having released a software development kit (SDK) to the developer arena and encouraging the submission of applications (apps) to their App Store, owners were invited to purchase and download apps to customise the functionality of their iPhone. The era of the app had dawned (Block, 2007; Kempster et al., 2014).

Consumers' desire for high bandwidth mobile data requirements such as mobile video streaming were serviced in 2009 when the first 4G (4<sup>th</sup> generation) mobile network was launched late in 2009 in Stockholm and Oslo by TeliSonera. It was based on the Long Term Evolution (LTE) international standard and a complete IP based data transmission protocol (Jansson, nd).

Microsoft made their biggest leap in phone technology when they marketed their Windows 7 OS on a Samsung Omnia 7 handset in May of 2011. It finally broke with their tradition of producing a mixture of PDAs both with and without the ability to be used as a phone. It was the first mobile phone to exhibit "live tiles" which displayed calendar appointments, weather and information such as news headlines updated in real time. One downside was that the new OS was not backward compatible and so users who were on an upgrade path could not utilise their pre-owned applications and software (HardwareZone, 2011).

Since the introduction of 4G a rapid increase in worldwide mobile phone sales has been witnessed as reflected in Figure 2-1 below. With increased competition driving prices down and ever expanding coverage opening new marketplaces, the appetite for these devices is unabated (Statista, 2014). More recently the development of mobile phone technology has

concentrated upon revisiting the physical appearance and ergonomic design of the human-phone interface. With the introduction of curved phones and flexible displays, manufactures are promoting ease of use, manageable size increase and unbreakable screens as the next big evolutionary step (Kelly, 2013; Woollaston, 2013a). Couple this with Google glass and its ability to provide the wearer with continuous internet interactivity and messaging (both text and voice) capability, the next few years will witness another paradigm shift in mobile phone technology (Glass Almanac, 2014).



Adapted from Statista, 2014

Figure 2-1. Worldwide mobile phone sales in millions per quarter 2009-13

## 2.2 Service Access

The introduction and prolific adoption of the smart phone as discussed above has witnessed a consequential surge in installation and use of apps and services. Currently there are more than 1.2 billion smart phones in use worldwide, accounting for 16.7% of the total mobile phone population, with an average of 26 apps installed on each of the disparate devices (MobiThinking, 2014; Richter, 2013).

This uptake of smart phones is further supported by the adoption of app running tablet computers throughout the population. An extremely rapid growth has been witnessed since the introduction of the Apple iPad in 2008 with worldwide sales spiralling to 116 million units in 2012 and then almost 207 million units in 2013, a year-on-year growth of 78% (Apple, 2010; Gartner, 2014a; Gartner, 2014b).

Apps and services vary hugely in sophistication and use, ranging from simplistic games on which users spend a few minutes a week or month, to those that are accessed more often such as weather apps and news feeds. The majority of these will access and utilise some personal or location details and usage data but even so remain relatively low risk because of their potential to do little harm and low cost of utilisation. Overarching these are the apps and services that if compromised and access gained by unscrupulous persons, have the potential to do serious harm or have excessively high cost implications; phone calls, bank account management, payment portals, text messaging (Short Message System, SMS), email and social networking sites all fall into this category. Compound this with research indicating that 72% of available Android apps have access to at least one high-risk system permission and the logical conclusion is that their protection should be paramount (Sverdlove and Cilley, 2012). Ledermuller and Clarke (2011) presented a mechanism to assess the risk associated with particular apps and services (assets) and their results are shown below in Table 2-1.

<b>Asset category</b>	<b>Risk level</b>
E-Mail (corporate)	8
E-health	8
E-banking	7
Remote access (corporate)	7
Stored business documents	7
Remote access (private)	6
Voice communication	5
Physical device	5
Personal information (online synchronised)	4
E-Mail (private)	4
Messaging	4
Web access (browser)	4
Social networking	3
Personal information	3
Stored documents	2
Maps & Navigation	2
News client	1
Utilities	1

Adapted from Ledermuller and Clarke (2011)

**Table 2-1. Mobile device assets with associated risk level**

The Federal Reserve published a report on mobile banking habits in 2014 which indicated that customer use of this service was on the increase (Federal Reserve, 2014). They found that 33% of mobile phone users and 51% of smartphone owners had utilised this facility within the preceding twelve months. Although of those customers 93% used the portal for reviewing statements and recent payments, 51% acknowledged that they had used the facility to transfer money between accounts. Indeed, these findings from America are reflected in statistics from

the UK, where 51% of smartphone owners use mobile banking and 50% shop online as illustrated in Figure 2-2 below (Styles, 2013).



Source: Styles (2013)

**Figure 2-2. Profile of app usage by UK smartphone owners**

When utilising mobile and indeed most computing devices, once a user has gained access via enabling the device and passing any authentication measures, the ability to use services, applications and programs is generally unrestricted and the user is free to navigate the system unchallenged; it is very much an authenticate-and-forget approach to device security. Although the individual applications may have in built security requiring the user to log on or authenticate during activation, this layers an extra level of inconvenience upon the user, whilst the actual ability to initiate the process is open and unrestricted, remaining so for the duration of the activated session.

Even when point-of-entry security is available, many device owners do not choose to invoke it. In a recent survey 36% of respondents aged over 44 confessed to not using any form of security on their mobile phone, although overall across all age groups 81% employed a Personal Identification Number (PIN) as a safeguard on phone activation (ContinuityCentral, 2014). When a PIN is implemented human beings are predictably unimaginative with over 10% of all users choosing 1234 as their security gateway (DataGenetics, 2012). There is clearly scope for a better approach to be implemented and adoption encouraged amongst device owners.

### ***2.3 Current Security Approaches and Limitations***

The previous sections have reviewed the evolution of mobile devices, how they have been universally adopted and briefly discussed service access and its associated security. This

section builds upon this by reviewing the limitations of currently implemented security on mobile devices and the associated weaknesses.

The majority of mobile device security is based upon secret knowledge that is supposed to be kept private and confidential by the device's owner. It is usually achieved via three common methods, password, PIN or pattern entry. Although these are listed separately they are simply variations of a single method; a password is generally regarded as an alphanumeric string of characters, a PIN is a numeric sequence as outlined above, whilst a pattern or sketch is depicted by the dragging of a user's finger across the device's touch screen in a recognisable shape.

By their very nature personal electronic devices are highly mobile, ported consistently by users and accessed frequently because of human nature's tendency to communicate in "inhomogeneous or bursty" patterns (Jo et al., 2012). If the user is in any way security savvy it is likely that they will implement a screen lock and although this is superficially secure, the combination of this with the frequency of use introduces frailty. Repeated unlocking of the device whilst in close proximity to others provides plentiful opportunity for password entry to be observed, rendering the secrecy ineffective (Dunphy et al., 2010).

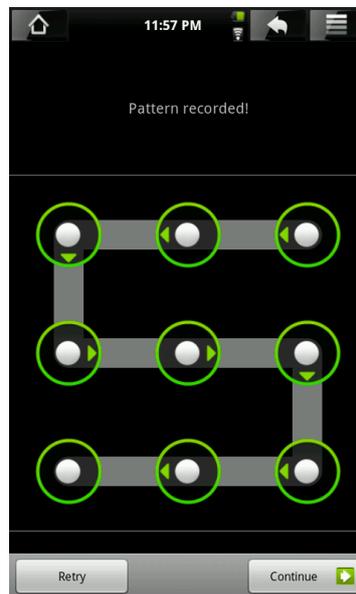
Mobile phones generally differ in their use of passwords and although they have the capability to utilise the full character set, historically manufacturers have limited security to a four digit PIN which can be applied to both the phone and the SIM card within (Furnell et al., 2008). Immediately it is clear that this method will drastically restrict the number of possibilities available to the user to a relatively tiny 10,000 ( $10^4$ ). This is further compounded by the inconvenience of repetitively entering the pass code which subconsciously encourages the user to select a PIN that is easily typed (Bonneau and Preibusch, 2010; Florencio and Herley, 2007). Even so it is surprising how humans exhibit their lack of imagination with the most common PIN found to be 1234 in a sample of 3.4 million numbers, when other combinations such as 8068 are used by only 0.000744% of individuals with twenty five occurrences in the extensive sample set (ContinuityCentral, 2014; DataGenetics, 2012).

Some manufacturers of mobile devices with touch screens have introduced longer PIN options under the guise of pattern entry. To achieve this, the device owner drags their finger across the screen in an established pattern, over a grid of nine nodes (these can be regarded as digits 1-9<sup>1</sup>) with the start point, end point and all points visited in between constituting the

---

<sup>1</sup> Digit 1 is the top-left corner of the grid with numbers progressing sequentially from left to right, top to bottom.

password. For example, in Figure 2-3 below the entered pattern would equate to 321456987 but intuitively to the observer the created 'S' pattern is much easier to remember than the longer nine digit PIN (Meitiv, 2010).



Source: (Meitiv, 2010)

**Figure 2-3. An example of screen pattern security**

There is however one restriction in using a pattern as opposed to a straight forward PIN and that is the number of available permutations. When entering a pattern the user is restricted in choice and movement from all but the centre node, for instance at digit position 3 the user has only three choices available 2, 5 and 6, it is impossible for them to move directly to 9 because 6 is in between. As such the available permutations for a six digit PIN reduce from 1,000,000 using a standard ten digit keypad to 92,448 utilising pattern entry with the described nine node layout, less than one tenth (Meitiv, 2010).

To counteract pattern entry weakness researchers have also combined approaches and incorporated elements of keystroke dynamics to assess the speed and style with which the user swipes their finger across the screen. Using dynamic time warping De Luca et al. (2012) outlined how they were able to distinguish between users entering the same pattern on an iPhone regardless of the sketch's simplicity, reducing the consequence of pattern compromise.

Another frailty of the pattern entry system is created inadvertently by the human body. As a user swipes their finger across the touch screen from one node to another the oils that lie on the surface of the skin have been shown to leave a smudge on the screen that can be revealed under certain lighting conditions. Although this will not immediately reveal the code, the start and end nodes are relatively easy to identify which consequently restricts the number of feasible possibilities and makes a security compromise much more likely (Aviv et al., 2010).

More recently in an attempt to overcome the smudging and shoulder surfing weakness of pattern and traditional password entry some manufacturers have introduced a pictorial approach. In this the user is urged to select a busy image with a large number of significant elements, numbers are then randomly superimposed on top of the image and the user has to drag them around until one digit is at a pre-designated location. Tapping the confirm button then validates the selections and either permits or declines access to the device (Halevy, 2014). Being able to move several digits before and after the significant one prevents spectators from knowing which is the vital movement to unlocking the phone, protecting the device and the information held within.



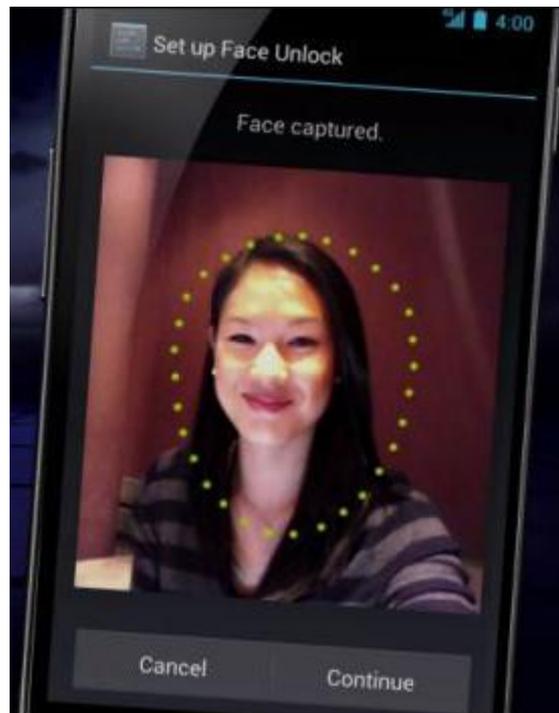
Source: Anthony (2014)

**Figure 2-4. A user scanning their fingerprint on a Samsung Galaxy S5**

Other manufacturers have introduced technology to enable users to employ fingerprint scans as their security mechanism. Rather than a static scan, the user swipes their finger across the scanner to capture the fingerprint and authenticate (Drummond, 2014). Both Apple and Samsung actively promote this as a secure method of protecting their devices (Apple, 2014; Lynch, 2014; O' Boyle, 2014) although researchers have managed to circumvent this approach with the use of false fingerprints (Kerr, 2014; Prabhu, 2014). During the research the tested Apple iPhone 5S's fingerprint security was able to be circumvented but did limit the investigators to only five attempts before it locked. More concerning, the Galaxy S5 as shown in Figure 2-4 permitted an unlimited number of attempts and also allows the user to provide a fingerprint as a means of accessing payment applications and secure data (Kerr, 2014).

Google and Apple have also both implemented facial recognition in their respective Android and iOS mobile phone operating systems as part of their security regime. Although vitality

tests were built into the process, requiring the user to blink, it was demonstrated that a photograph could be doctored to simulate this process and subsequently open the device (Colon, 2013; Kelion, 2013). In 2013 Google filed a patent application which extends the process and requires the user to stick their tongue out, wrinkle their nose or pull a strange facial expression in an attempt to counteract the flaw (Gorman, 2013). Figure 2-5 illustrates Google Android's face unlock feature in operation.



Source: Woolaston (2013b)

**Figure 2-5. Google Android's face unlock feature © Google**

Other aspects of mobile phone technology also pose a security flaw in their own right. For instance, many handset manufacturers are embedding voice control into their products or providing routes for app developers to do the same; these enable users to unlock their device, dial contacts or even send text messages (Cozma, 2012; Velazco, 2012). However, this capability is not matched to a specific voice, rather a recognised specific command or word and will function if used by almost everybody (Culzac, 2014). Another technological weakness is the use of accelerometers in handsets. Data from these has been captured by researchers and analysed to ascertain if this gave any indication of passwords or entered PINs, it did. Although it was not possible to precisely determine the entered character string, it did give an indication of likelihood that at worst would vastly reduce the list of potentials (Ward, 2013).

With these methods all demonstrating weakness and the ability to be compromised, researchers have been investigating transparent and even continuous user identity authentication as a means of securing mobile devices. As far back as 2002 Clarke et al.

proposed key stroke dynamics as a method of transparently authenticating users whilst they were typing on their handset. Although they investigated several approaches because of its overall performance and technology restrictions at the time, they deemed this the most suitable candidate (Clarke et al., 2002). As technology advanced and the corresponding processing power of mobile devices increased this research was developed into a proposed Intelligent Authentication Management System (IAMS) which introduced the concept of degrading service availability and invoked non-intrusive transparent authentication when confidence in the user's identity fell below an operational level (Clarke and Furnell, 2007). A further evolution then saw this renamed as a Non-Intrusive Continuous Authentication framework (NICA) and developed into a functioning prototype, although even at this time widespread use of the system was still restricted by technological limitations (Clarke et al., 2009; Furnell et al., 2008).

Transparent authentication was given a further endorsement in 2009 when Jakobsson et al. argued that because of the mainly monogamous relationship that mobile devices have with their user, they have an ideal opportunity to harvest behavioural data which can be leveraged for authentication, and security and usability will be improved when compared with traditional intrusive methods (Jakobsson et al., 2009). Behavioural information was also proposed as a method of authentication by Briggs and Olivier in 2008 when they outlined a so-called "biometric daemon". In their proposal once an enrolment process of initiation had been performed, their "electronic pet" monitored the user and grew its knowledge of the operator's behaviour, refining its identification ability as it learnt; it even started to "die" if left unattended for any length of time but they saw it as "the basis for secure, usable and engaging identification and authentication" (Briggs and Olivier, 2008). The "ePet" approach is further supported by the work of Tanviruzzaman et al. (2009) who indicate that mobile phones will learn to recognise their owner.

Crawford et al. (2013) also suggest that because of mobile devices "are generally used by a single owner" they enjoy "a long term, persistent relationship with a user that can be exploited for authentication purposes" supporting the feasibility of the electronic pet. In their behavioural biometric approach to authentication they propose a framework to collect behavioural data during use of the handset which transparently learns the patterns of interaction that the device's owner exhibits (Crawford et al., 2013). Once a user profile has been built the framework monitors and records keystroke or voice data and compares this with the known characteristics, which in turn either increases or decreases the device's confidence in the user's identity. This maintained numeric value is then used to either permit or deny the activation of services based upon either system default or user defined thresholds.

Without use, the system degrades the identity confidence, invoking a specific request for authentication upon reuse by the owner. With the “bursty” usage patterns exhibited by users it is however likely that authentication will be frequent and intrusive, although during experimental research with a user invoking an action every ten minutes they observed a 67% reduction in authentications (Crawford et al., 2013).

The overriding issue with this all these approaches to security is that it focuses upon the single device. With methods that learn and continuously monitor the user’s actions as intimated earlier they die if unused for any length of time irrespective of how many other actions the user is performing. An individual might be concentrating on using another device, logging on and authenticating as required but all this potentially useful information is ignored and going to waste. The weaknesses of a lone device fighting and repelling threats harks back to Aesop when he suggested that “united we stand, divided we fall” (Your Dictionary, nd), a route to a united security solution is surely advantageous.

## ***2.4 Summary***

During the past 40 years, miniaturisation and increased performance has driven the incredible advances witnessed in both personal computers and mobile phone technology. The review given in the previous sections reminds one of the distances that have been travelled and yet the journeys appear to be far from over. With Google glass and other wearable technology, convergence and amalgamation of currently disparate products is the future; couple this with increased connectivity and already our surroundings are being seen as an “internet of things” (Randewich and Carew, 2013).

This chapter has examined the evolution of the mobile phone and the prolific rise in its adoption throughout society at large. Both these and other personal electronic devices are becoming omnipresent in everyday life, both inside and outside of the home, being ported in individuals’ handbags and pockets, and growing into status symbols and even items of fashion. They enable the population to be virtually continuously contactable and are viewed as a vital component of modern society. As size has diminished, capability has inversely grown, providing the means to execute processor hungry applications and perform tasks which until relatively recently could not have been envisaged.

This section has also investigated the security mechanisms that are used to protect these desirable and ubiquitous items of equipment, highlighting the shortcomings of the employed approaches. Building upon this a review of the research that is aimed at counteracting the weaknesses is presented, which in addition to providing understanding illustrates how most approaches are unilateral and only use information on a single device. There is a great deal of

detail that could be employed but is currently going to waste, providing an opportunity to leverage this in a novel security implementation.

In the next chapter a comprehensive examination of what constitutes identity is made, yielding further understanding and a basis for an additional exploration of authentication techniques beyond.

---

## **Chapter 3**

# **Identification and Authentication**

---

### **3. Identification and Authentication**

---

This chapter will address identification and authentication, although it is important to highlight that within the scope of this document authentication refers to the process of user authentication (human to system) rather than machine authentication (system to system). Machine authentication (e.g. the use of the secure sockets layer (SSL) protocol that is used to create a secured connection to a web-site) simply verifies machine identities for a given communication session and gives no assurance of the identity of the person using the machine (O’Gorman, 2003). This is the role of user authentication; the process via which a user can confirm their identity to an electronic device, allowing them to authenticate and utilise the services and information held within.

Firstly however, an exploration of philosophical and psychological approaches to identity will be made, establishing a detailed understanding of the meaning of identity and the human processes involved in recognising an individual after a period of time. Continuing from this, the chapter will then examine individuation and how any given person can be differentiated from another. Finally it will then proceed to review the methods and approaches used to perform physical identification and authentication of a user’s claimed identity, examining current techniques, their strengths and weaknesses, and how these are employed on personal electronic devices.

#### ***3.1 Identity***

This section explores the meaning of the term ‘identity’ and how it relates to individuals in two distinct phases. Initially the psychological and philosophical approaches and understanding of identity are examined, succeeded by an exploration of identification and authentication from a physical perspective.

It further reflects upon the interaction people have with their environment and indeed the way in which the environment can dictate behaviour, both of which are routes to identity determination. Establishing these concepts at this stage provides a solid foundation for this research and potentially a route for an alternative approach to authentication.

##### **3.1.1 Philosophical and Psychological Identity**

Varela (1997) suggests that “the entire enterprise of defining life, the organism and cognition scientifically is doomed to fail”, however whilst not attempting to define ‘life’ this section considers the philosophy and psychology of identity in its true and strict sense. Examining this view of identity and the discussions held within that tranche of academia enables a fuller understanding of individuation to be obtained.

The noun 'identity' from a philosophical perspective, literally refers to an object, fact or person being the same or exactly alike to itself and nothing else (Shoemaker, 2006). However, there are two views of identity that require clarification, numerical identity and qualitative identity. Numerical identity refers to something being one and the same thing as defined above, for instance a cat is intuitively identical to itself. By contrast qualitative identity refers to entities that are exactly similar in a way that one twin may be exactly similar to their brother or sister. They are qualitatively identical but because they are separate human beings with individual thoughts, beliefs, motivation and concerns they are not deemed to be numerically identical. This research is focused upon the identification and authentication of specific individuals and hence this discussion will address numerical identity.

Some of the earliest philosophical work into identity and its properties was conducted by the German philosopher Gottfried Wilhelm Leibniz (1646-1716). From his writings on this matter has been drawn what is now known and commonly accepted as Leibniz's Law (derived from his work the Indiscernibility of Identicals) which states that, "A is identical to B if, and only if, A has every property that B has, and B has every property that A has" (Feldman, 1970).

Interpreting this principle from a mathematically logical standpoint, identity has three properties;

- Reflexive: if object A is identical to object B, then object B is identical to object A;
- Transitive: if object A is identical to object B and object B is identical to object C, then object A is identical to object C;
- Symmetrical: everything and anything is identical to itself.

(Shoemaker, 2006)

Although Leibniz' opus is hard to dispute, René Descartes in his Meditations on First Philosophy attempted to undermine the principle by stating that he could not doubt his own existence<sup>2</sup> (his being) but he could doubt the existence of his body as it could simply be a figment of his imagination. He argued that his being and his mind were consequently not one and the same because one possessed a trait that the other did not and therefore he was different from himself; a contradiction of Leibniz' work (Veitch, 1901). However, following the publication and circulation of his manuscript numerous counter arguments (supporting Leibniz Law) have been proposed using reasoning based upon reductio ad absurdum (reduction to the absurd).

---

<sup>2</sup> The now famous "I think therefore I am"

Over time the term *identity* has become skewed to signify the way we look and the way we appear to others. Additionally in modern language *identity* is interpreted to mean an entity, something that is possessed or an object that can be lost or stolen. In this sense it is also even possible to refer to identities (in the plural) indicating that an individual can be expected to own more than one and manage a multiplicity. A person that loses their *identity* is still the same person that they were before the loss and so in examining the contemporary terminology what is lost is not what makes the person what they are<sup>3</sup>. In a strict sense their identity remains and to acquaintances they are still easily recognisable as the person known a-priori to the event. Hence as Shoemaker (2006) suggests “instead of thinking of an identity as an individual essence, we might do better to think of it as something, perhaps a set of traits, capacities, attitudes etc., that an individual normally retains over a considerable period of time and that normally distinguishes that individual from other individuals”.

The unique set of traits (so called identity matrix) that an individual possesses and retains over time is what individuates them from the next person. However, recognition can only be successful with existing personal knowledge. “In its ordinary everyday sense, to recognise means to re-cognise, to discern someone or something with which we are already acquainted” (Jones, nd). This principle underlines the requirement for some familiarity and basis upon which to form a judgement of recognition; one must have met and mentally stored a unique identity matrix which is sufficiently unchanging over time to enable them to recognise a particular individual in the future.

Quine (1950) argues a similar point using the analogy of a river in answering Heraclitus’s problem that “you cannot bathe in the same river twice, for new waters are ever flowing in upon you”, suggesting that a river’s identity is ever changing as water flows through it. He suggests that you can bathe in the same river twice but not the same river-stages, where river-stages are sections of a river defined in space and time. We understand bathing in the same river twice as bathing in two river-stages that are indeed stages of the same river. A river is a process through time, its stages are the momentary parts and it is only possible to recognise and identify a river if we truly understand what constitutes different sections of the same river and therefore its ontology (Quine, 1950). In terms of Identification and Authentication this can only be done successfully if a thorough understanding of each element of the identity matrix and how they interact is achieved.

---

<sup>3</sup> To clarify, identity theft should be thought of as the act of someone acquiring the ability to pose as the person whose identity was taken away. In terms of physical possessions the victim is no worse off than they were prior to the intervention of the perpetrator. They are of course more vulnerable to fraud and monetary loss but they are not necessarily immediately disadvantaged.

One of the major issues is the temporal effect on identity determination. "People are likely to change substantially over time or, more precisely, that the degree of change depends on the stability of context" (Fraleay and Roberts, 2005). The simple question is persistence or "sameness" - if an individual exists at a historical point in time and is encountered again on some future occasion what has persisted that enables the decision of *sameness* to be reached? (Bulot and Rysiew, 2007) Indeed, is it that the same person has been encountered twice or have there been two separate encounters of different people? (Xu, 2007) Over a long period of time a person's appearance can change dramatically, weight can be gained, hair can change colour or be lost, and without exception ageing will have occurred. Of course, these are all physical attributes but equally an individual can undergo a personal trauma or significant event in their life that colloquially makes them *not the same person they were*. Qualitative differences have evolved but numerical identity has remained.

In philosophical literature there are three responses to the question of persistence and how it may be established:

i. Psychological approach

A person P on a particular day  $D_1$  has specific memories and experiences  $PD_1$ . The following day the identical person  $PD_2$  remembers what they knew the day before but additionally gathers new memories and experiences. Thus the person has persisted across the time span of a single day. By extrapolating this theory to some point in the future  $D_n$  the person is considered identical if they have the same memories<sup>4</sup>, experiences etc. that they had at  $D_1$ . Continuity of identity can then be tracked and established through time from  $PD_1, PD_2, PD_3, \dots, PD_{n-1}, PD_n$ .

ii. Somatic approach

A person P on a particular day  $D_1$  has a specific body  $PD_1$ . The following day the body  $PD_2$  can have its origins traced with very little change from the body  $PD_1$ . Through this argument persistence was maintained via the near unchanging physicality of the body in question during the two days. Again this can be extrapolated to a third day, a fourth and onwards to some future point  $D_n$ , with continuity being confirmed by tracking  $PD_1, PD_2, PD_3, \dots, PD_{n-1}, PD_n$ .

---

<sup>4</sup> Some of the specifics of the memory may have faded with time but the core impression remains

iii. Simple approach

This third approach does not discount the first two but rather states that although physical continuity and/or psychological continuity are usually present in persistence of identity they are not enough to guarantee it. Only continuity of identity itself is enough to guarantee true and unequivocal identity; for any object there are no criteria for identity through time (Merricks, 1998).

Arguments have been proffered to support and counter all three approaches ranging from brain transplants (both whole and as two separate hemispheres (fission), to rebuilding a ship at sea plank by plank (Blatti, 2007; Shoemaker, 2006; Merricks, 1998). To get entrenched in a full and extensive investigation of identity, its true and strict philosophical meaning and all the discussions for and against is beyond the scope of this document. Arguably, for the purposes of this research, persistence of identity across time will be found in a mixture of the first two approaches (i and ii); part psychological, part physical and an element of epistemic tracking<sup>5</sup>.

### 3.1.2 The Person and Their Environment

A person will incur a detectable impact upon their immediate locale when carrying out an action, caused by their physicality and psychology. The impact can be directly upon the piece of equipment that is being used, or equally upon the environment in which the individual is working. In this latter instance the environment can be both the immediate physical surroundings such as an office or workspace, or more covertly the technical infrastructure such as a network or database. These result in the ability to approach the measurement of impact from a number of perspectives, however it initially divides into two distinct aspects, the person and the environment.

The factors listed in the two tables below range from those that can be immediately measured from the individual during a session of interaction (e.g. physical attributes or memory), to those that require a considerable amount of time to ascertain (e.g. temperature). Further, some factors are considered to be unique and will function well in isolation, whilst others although individually collectable will perform best in combination. By establishing the existence of such factors or combinations, the recognition and measurement of identity becomes more tangible.

---

<sup>5</sup> Epistemic tracking refers to cases in which the target individual cannot be perceived but can be located or identified on the basis of indirect information gathered by such sources as reasoning or communication. For instance, historians and archaeologists are expert epistemic trackers because they routinely locate and identify bygone individuals (persons and artefacts) on the basis of indirect evidence, such as archives or archaeological vestiges. (Bullot and Rysiew, 2007)

Person-centric traits and attributes that can be considered for inclusion in the identity matrix are shown in the table below.

Attribute	Trait
Physical attributes	Measurement of an individual's physicality and bodily structure
Behavioural attributes	Assessing the way in which an individual uses their body
Reaction to stimuli	Reaction to light or sound
Intelligence	Gauging an individual's mental capacity
Approach	Closely tied in with personality traits shown below, how one person reacts and interacts with another
Personality	Measurement of the universally accepted five main personality traits i.e. Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness (John, 1990)
Memory	Recall of significant knowledge
Language	Linguistic profiling (Pennebaker and King, 1999)

**Table 3-1. Identity matrix person-centric indicators**

Similarly to the person-centric indicators (Table 3-1) environmental factors<sup>6</sup> can also be measured and used as part of the identity matrix; these are outlined in Table 3-2 below.

Environmental factor	Indicator
Temperature	Individuals adjusting the temperature of their working environment
Lighting	Brightness of lighting, lights may be switched off or additional lamps used
Network traffic	How much an individual impacts upon the network
Data trail	Databases accessed, websites visited, applications used
Man-machine interface	Methods of working, keyboard shortcuts
Furniture	Arrangement of furniture within the working environment
Noise level	How much noise an individual makes
Personal items	What items are carried at any given time

**Table 3-2. Identity matrix environment indicators**

### 3.1.3 Affordance

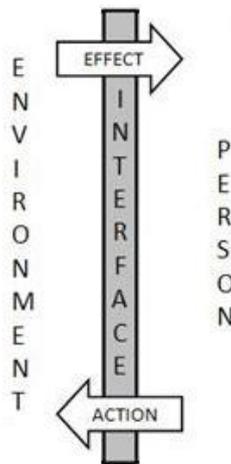
Affordance dictates a user's orientation to the physical environment and the social world (Gibson, 1979). That is, an individual is restricted and influenced by their immediate surroundings and the people they interact with, constraining and creating perceived multiple identities.

<sup>6</sup> The environmental 'footprint' that an individual incurs when performing an action

During the formation of the identity matrix it is imperative that consideration to affordance is made because the criteria that are selected may limit or affect the behaviour of subjects during data acquisition. The projected influence must be minimised and if at all possible eliminated to enable true and accurate readings to be obtained. Removing this skew factor will allow consistency in evaluation to be achieved, aiding the identification process.

However, assessment of affordance is subjective. Different elements of the environment will influence action and reaction to varying degrees and in numerous ways (Amatrudo, 2008). No single approach will scientifically be able to accurately measure and appraise the cause and effect of all environmental variables to facilitate irrefutable minimisation.

Figure 3-1 has been constructed to highlight the relationship between the person and the environment as it passes across an interface. This interface will change depending upon the combination of activity and object for any given task. For instance, the act of an office worker initiating a telephone call utilises the numeric keypad as the interface. Equally though, once the call has been connected and the conversation initiated the mouthpiece then acts as the interface to the network beyond that carries the digital voice data.



**Figure 3-1. Diagrammatic representation of a person's interaction with their environment**

The diagram additionally demonstrates how the environment offers affordance to the person across the interface and therefore will affect and even limit the action that can be taken. Continuing with the phone call analogy from the previous paragraph, once the call has been connected, during the act of holding the conversation, only the voice is available as a contribution to the identity matrix and therefore afforded. Interaction with the keypad would not be afforded at this time and it would be unrealistic to utilise this as an element for the individual's recognition. It is clear, affordance exerted by the environment or even user action, can restrict and alter the potential elements available for identification purposes.

### **3.1.4 Summary**

This section has provided an understanding of what is truly meant by the term identity. Although some of the philosophical views maybe considered by some to be beyond the scope of this work, they provide a viewpoint that is supportive and contributory to the project as a whole. They suggest that persistence over time is the greatest factor when establishing identity, the unbroken chain of affirmation gives the confidence necessary to make informed and accurate decisions.

It has also been discussed how factors are available which can be used to individuate a population. By combining these, practical methods can be established and utilised effectively within the technical environment.

## **3.2 Individuation**

With any method of authentication it is imperative to fully understand what separates one individual's identity from another and therefore how people can be individuated and consequently identified. Identification and authentication are two subtly different concepts and for clarity it is important to emphasise the distinction.

Identification is the process of using claimed or observed attributes to deduce who the entity is (EU, 2005). That is, a set of discovered attributes are used to select one particular individual from a population of known individuals without any initial idea of whom the person is. To achieve this, a comparison using the attributes must be undertaken with each member of the population until a match is found and identity established. On average this process must perform  $n/2$  test comparisons for a population containing  $n$  known individuals. Although this is an exhaustive process, dependent upon the observed attributes it would be possible to subdivide the entire population into sets of matching individuals. For instance, if eye colour was employed and the population indexed accordingly, only 8% of the world's population have blue eyes, immediately reducing the size of the identification matching process (Ask, nd). However, continuing the analogy, it should also be noted that there are large variations across the world with blue eyes being extremely rare throughout Asia and Africa, whilst in countries such as Estonia the percentage is as high as 99% (CompuServe, nd).

Authentication however, is the corroboration of a claimed identity by the comparison of the known attributes of the individual, whose identity has been claimed, with the observed attributes of the claimant. In this instance a single evaluation has to be undertaken, the direct comparison of the observed identity with the claimed identity (OWASP, 2014).

Although different, identification and authentication both rely upon the collection of a set of traits or knowledge from a subject interacting with a device at any given moment, and the subsequent matching of this detail against a known identity.

### **3.3 Identification and Authentication**

As discussed at the start of this chapter the process of user authentication (human to system) establishes confidence in the identity of the person using the machine. To augment this understanding further authentication can be regarded as “how computers can confidently associate an identity with a person” or “the process of verifying the validity of a claimed user” (O’Gorman, 2003). With reference to person centric traits as outlined in Table 3-1, it is clear that there is *common ground* between identification and authentication from a philosophical perspective and that of a technological standpoint<sup>7</sup> (Smith, 2001).

It is well established that authentication is based upon one of three key approaches, something the subject knows, has or is; for instance and respectively a password, a swipe card or a fingerprint (Wood, 1977). Each of these methods will now be explored in turn, examining their own distinct strengths and weaknesses and how they are employed within modern technology.

#### **3.3.1 Knowledge Based Authentication**

Knowledge based authentication has traditionally relied upon a user identity code and associated password that is supposedly only known to or more strictly “memorized by” the owner (O’Gorman, 2003). To this end the password system would appear to be secure with just a single person knowing what has been set and to all extent a seemingly infinite population to choose from. For instance, if an eight letter case sensitive password with 72 available characters (A..Z, a..z, 0..1 plus ten others such as !# + etc) is utilised, this generates a sample space of 722,204,136,308,736 possibilities<sup>8</sup>. Even if the passphrase is not case sensitive this still yields 20,047,612,231,936 potential passwords<sup>9</sup> and so superficially it is a surprise that password systems are deemed inherently weak (Birget et al., 2005; Brostoff and Sasse, 2000; Sobrado and Birget, 2002).

In 2011 Burnett released a list of the 10,000 most commonly used passwords (Burnett, 2011). In his analysis he examined 6,000,000 user identity-password combinations and found that his

---

<sup>7</sup> In this instance the technological identification refers to the establishment and verification of a user's system identity; not the technical security meaning of identification

<sup>8</sup> Each of the 72 available characters can appear in any of the eight positions yielding  $72^8$  possibilities

<sup>9</sup> Removing case sensitivity limits the number of characters to 46; therefore there are  $46^8$  combinations

list of 10,000 accounted for 99.8% of all passwords that he encountered, with “password” topping the list having been used 32,027 times. Table 3-3 lists the ten most popular choices of password that Burnett identified alongside the corresponding least common choices.

Rank	Password	Occurrence	Rank	Password	Occurrence
1	password	32,027	9,991	chateau	51
2	123456	25,969	9,992	chas	51
3	12345678	8,667	9,993	charlie2	51
4	1234	5,786	9,994	dogggg	51
5	qwerty	5,455	9,995	doll	51
6	12345	4,523	9,996	19729172	50
7	dragon	4,321	9,997	pzaiu8	50
8	pussy	3,945	9,998	quaint	50
9	baseball	3,739	9,999	viking1	50
10	football	3,682	10,000	voltron	50

Source: Burnett (2011)

**Table 3-3. List of ten most and least popular passwords**

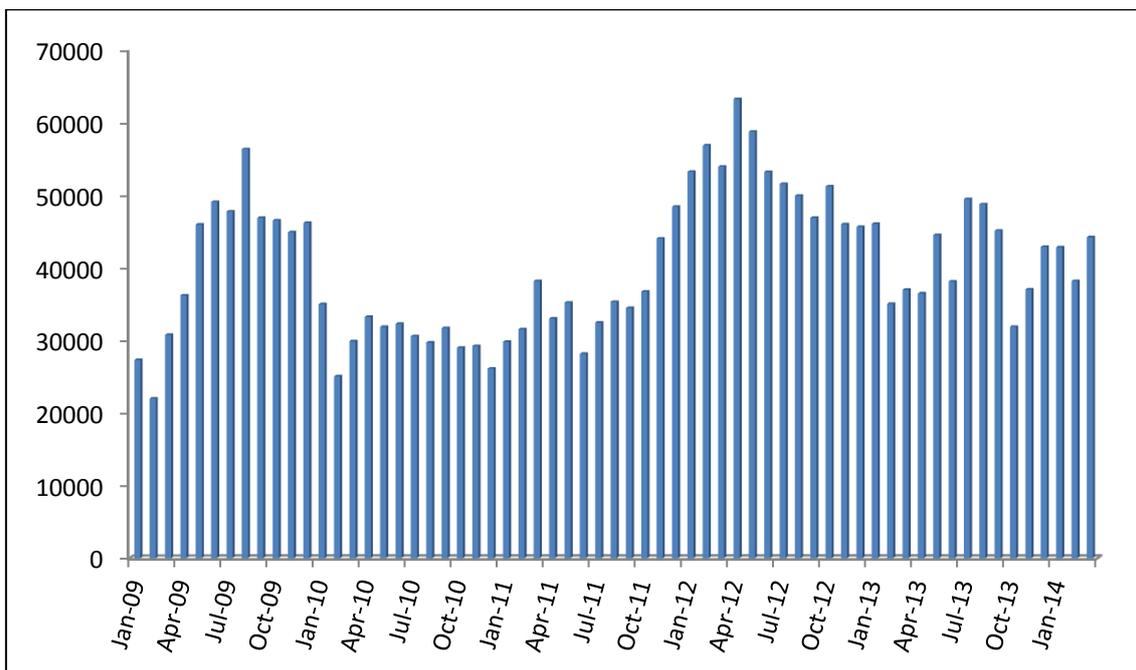
In the analysis Burnett excluded case sensitivity from his analysis and so “PassWoRD” is counted as being identical to both “PASSWORD” and “password”, increasing the number of coincident choices to some extent. It is clear from this study that human imagination and ingenuity is the greatest flaw in the use of a password system, and it also underlines the disregard that many give to what should otherwise be a secure and protective process. However, it is somewhat more surprising that given humans’ nature to select words that are easy to type and remember (Bonneau and Preibusch, 2010; Florencio and Herley, 2007) that short words such as “chas” and “doll” appear at the bottom of the list of favourites, an area where imagination would be expected to flourish.

Inherently human beings are forgetful creatures and have an inclination to trust others. Passwords are often written down, placed in desk drawers or even left attached to the underside of keyboards on post-it-notes (Albrechsten, 2007; Grama, 2010, p.400; Smith, 2001). Although the writing down of passwords is often regarded as extremely bad security practice, there are some that argue that it is better to write them down and have many different passwords than memorise a few and re-use them (Hayes, 2014).

Re-use of a password across multiple sites exposes the user to multiple compromise should a single set of log-on credentials be lost, intercepted or hacked. However, this practice is extremely common. In 2012 CSID undertook a customer survey of the US market in which they

quizzed subjects about their password management and habits; 61% admitted they used the same password across multiple websites, 54% only have five unique passwords or less and despite this 89% felt secure in their password management and security (CSID, 2012). Interestingly, the worst age group for password reuse were 18-24 year olds the so called “digital natives”, where 76% said that although they were security conscious they wanted to choose memorable and secure passwords and then reused them multiple times (Kurkovsky and Syta, 2010).

Historically, if asked by a work colleague to divulge their password for some spurious reason, most people would freely do so. In a survey carried out in 2004 it was revealed that “more than 70% of people would reveal their computer password in exchange for a bar of chocolate” and “34% of respondents volunteered their password when asked without even needing to be bribed” (BBC Online, 2004). However with extensive press coverage of password insecurity following this revelation the situation improved. When the chocolate survey was repeated in 2007 the figure had dropped slightly to 68% and then in 2008 there was a significant improvement when only 21% of respondents were willing to share their password (Grama, 2010, p.400).



Source: APWG (2014)

**Figure 3-2. Detection of Unique Phishing Sites**

Phishing and social engineering also pose a serious threat to knowledge based personal security as attacks try to discover personal information that can be used to compromise the security of the target. Although these attacks are generally aimed at gaining banking and other personal credentials rather than direct access to passwords, they do give an indication of how

the naivety of users is regarded by predators and how they hope to gain such information. In the twelve months between the beginning of 2005 and 2006 the Symantec Network Probe detected an 81% increase in phishing e-mails indicating the real start of the threat (Symantec, 2006). From this point there was a rapid growth in the detection of dedicated phishing websites reflected in the global industry, law enforcement, and government coalition APWG's reported findings shown graphically above in Figure 3-2 (APWG, 2014).

After the initial surge in detected phishing websites, an early peak in August 2009 was noted. Subsequent stabilisation and a decrease in numbers was then experienced but from the second half of 2011 an increase was once again witnessed, aligned with the uptake of internet availability and usage within China. More recently figures suggest that once again the trend has stabilised and fallen from a height in April 2011.

However, an individual who is trying to compromise security without specific knowledge has little probability of success. The only way in which a password can be identified (without direct communication) is down to pure guesswork. Of course when choosing a password people often use dictionary words, names of relatives or places, birthdays, car registrations or pet names as an aide memoir. These methods can be easily broken by readily available software from the Internet, for example "ophcrack" which can be downloaded from the Sourceforge website (Ophcrack, 2014); but if dictionary words and obvious choices are avoided it becomes a far greater challenge for even the most determined hacker. In this instance software tools have to revert to brute force approaches, where increasing length combinations of every letter and available digit are tried in turn or by the use of rainbow tables which utilise a pre-compiled series of randomly generated character chains (Orbit, 2012). Clearly these can take a significantly long time if the password is long enough; a combination of length and randomness is the most astute choice. Negatively though a password such as Q2{g!L£37yKl is of course not easy to remember, humans as ever are the weak link in the process.

As discussed in the previous chapter mobile phones generally use knowledge based authentication in the form of a four digit PIN, although some are more recently extending this via the implementation of pattern entry. As was highlighted, all methods come with associated weaknesses such as predictable choices of codes (Bonneau and Preibusch, 2010; Florencio and Herley, 2007) and smudging (Meitiv, 2010). Despite this, implementation of knowledge based authentication remains popular because it is extremely straightforward and has an inherited acceptance by the established user base (Crawford and Renaud, 2014). Being entirely a test of what the user knows the system firstly needs to enrol the user and allow them to create the secret piece of information. This is then stored in permanent memory in either an encrypted or plain form, for instance encrypted upon the SIM card of a mobile phone. When accessing the

system, the individual attempting to authenticate enters what they believe to be the correct knowledge which is then compared directly with the stored sample. The resultant decision is Boolean and without ambiguity, it is either correct and the user is granted access or incorrect and the user is declined access.

### **3.3.2 Possession Based Authentication**

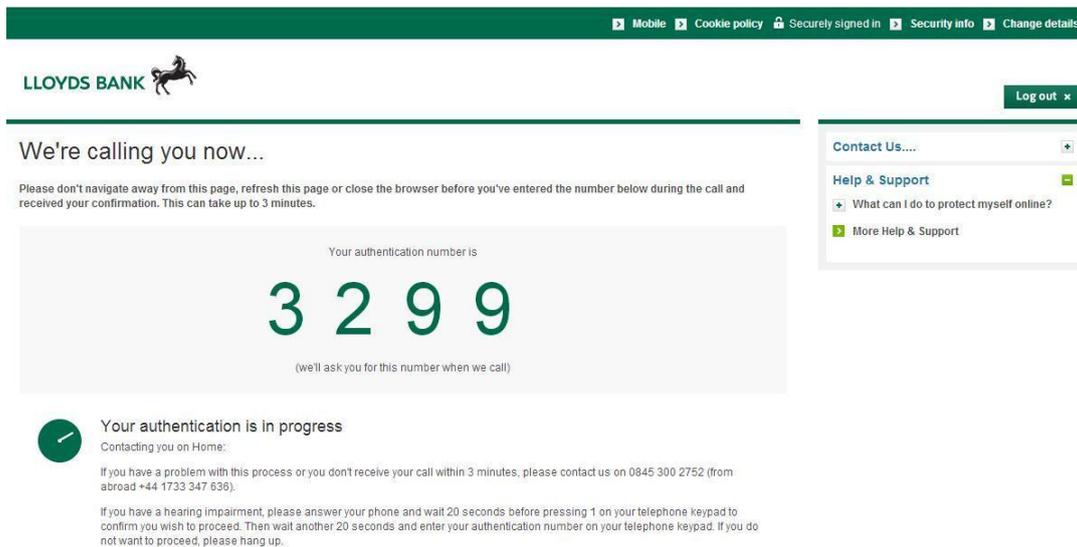
Possession or token based security is founded upon an item that an individual carries about their person. Items suitable for this form of security range from keys, to magnetic swipe cards, to devices with inbuilt near field Radio Frequency Identity (RFID) chips. Identification and authentication are confirmed by the presence of these tokens during the access process; for instance, swiping an identity card with a magnetic stripe through a corresponding card reader to gain entry into a laboratory. Indeed, even the everyday process of returning home after work and using a key to open the front door, is in fact a form of token-based security.

Once again, the human owner is the greatest vulnerability. In the same way that passwords are shared amongst colleagues, tokens are often treated in the same way (Matyas and Riha, 2002). However, not all vulnerabilities stem from the carelessness of the owner. Over recent years a number of large-scale applications have been introduced that utilise RFID based contactless smartcards; public transport systems being a prime example. In July 2003, the Oyster Card was introduced in London to enable cashless travel on the London Underground, buses, the Docklands Light Railway, over-ground trains and trams; it is a contactless smartcard that is based around the MIFARE technology. Although these cards were favourably received and deemed secure, in 2008 Garcia et al. published a technical paper on how to remotely read and clone an Oyster Card (Garcia et al., 2008). However, rather than rework the now more than 10 year old technology, Transport for London decided to wait and introduce contactless payment points so commuters can pay as they go (Judge, 2014).

Another form of possession based security that is superficially less obvious is employed in the protection against fraudulent action on some banking apps. For instance, when setting up a new payee on Lloyds Bank's app or website the system generates an automatic phone call to either a pre-registered land line or mobile number and the user is required to confirm a code displayed on screen before they can continue as shown below in Figure 3-3. By being in possession of the phone and able to provide the code the bank has confirmed the presence of the token (the phone) and permitted the user to proceed (Lloyds Bank, nd).

Implementation of this form of authenticated security is subtly different to a knowledge based approach. Enrolment is performed in one of two ways, either the user is issued directly with the token (e.g. a swipe card) and the action performed to inform the system of the user's

token credentials; or in the case of a phone or other piece of equipment being used, the details of the secondary device are entered and a test transmission is performed, allowing the user to submit the supplied code and confirming the eligibility of the token. When authentication is required, the process is repeated by swiping the appropriate card, receiving and entering the pass code, or even double tapping a paired mobile phone, and access is then either granted or declined (Kastrenakes, 2013).



**Figure 3-3. Lloyds bank token based authentication screen**

The search for unobtrusive methods unable to be compromised by unconscious or subversive human action has gathered importance with bodies such as the US Government's Defense Advanced Research Projects Agency (DARPA) calling for new and innovative approaches to security, and so the spotlight has turned upon personal characteristics that cannot easily be replicated by others, biometrics (DARPA, 2012; Welch, 2014).

### 3.3.3 Physical Trait Authentication

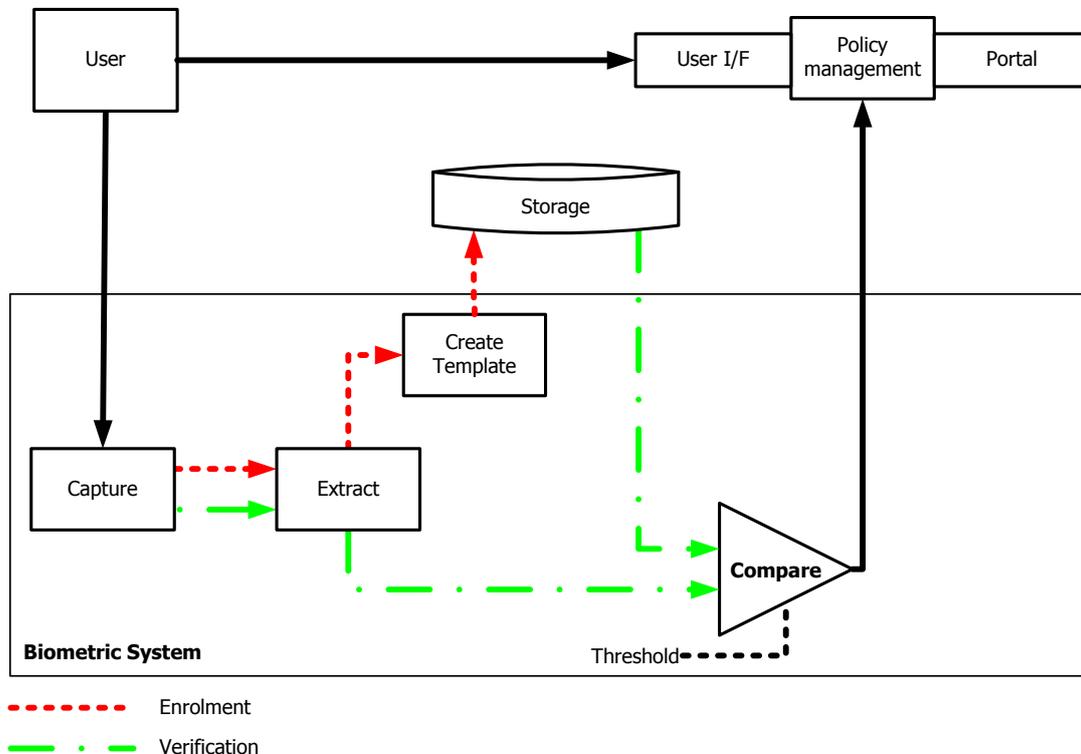
Physical trait authentication (something that a person is) within the security field has become known as Biometrics, a portmanteau word being formed by the blend of two Greek words; bios meaning 'life' and metrikos meaning 'metric' or 'measure' – 'life measurement'. For as long as man has inhabited the Earth, humans have used an individual's characteristics such as their face or voice to individuate one person from another. In the middle of the 19th century the Paris police department under the guidance of Alphonse Bertillon evolved the idea of using various body measurements (for example length of arms, feet and fingers) in criminal identification. Fingerprints were a natural progression from this initial concept and with Galton's discovery of distinctiveness the idea of recording criminals' fingerprints and storing them for future reference was adopted by many major law-enforcement agencies. In time, police were able to extract matches from typically fragmented crime scene fingerprints

(latents) and the birth of the use of biometrics as a form of identification had unwittingly occurred (Crime Scene Forensics, nd).

Any human behavioural or physiological trait can be utilised as a biometric as long as the following seven criteria are met (Prabhakar et al., 2003):

- **Universality.** All people should possess the same characteristic, or in a composite system be able to exhibit at least some of the required characteristics.
- **Permanence.** Over time the element of the trait that is being measured should remain sufficiently constant.
- **Distinctiveness.** The characteristic of any two people must be identifiably different.
- **Collectability.** The trait must be quantifiable, measurable and able to be gathered.
- **Acceptability.** Harmless and readily accepted by users.
- **Performance.** Agile and accurate enough to function within the available resources.
- **Circumvention.** Sufficiently robust to repel attack and fraudulent use.

Implementation of a biometric system is far more complicated than the previously discussed approaches to authentication. Figure 3-4 below illustrates the processes involved in a simplified biometric system and the flow of information within.

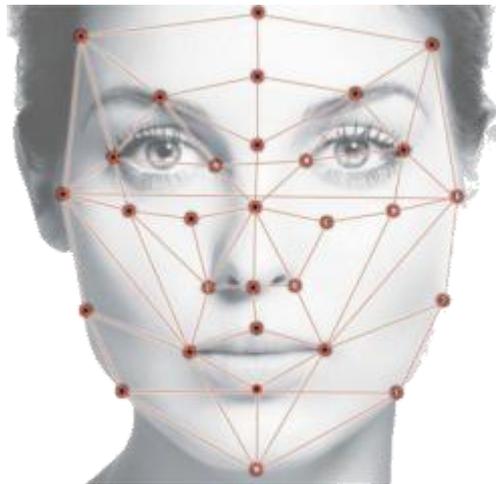


Adapted from CESG (2002)

**Figure 3-4. A simplified biometric system**

To enable a biometric authentication system to function a user must first enrol and provide specimens of the measurements or traits that will be utilised in the identification process. These are processed and stored as a reference template. During the verification procedure, a user has similar measurements taken which are then compared to the specimen template to establish a degree of certainty of likeness (generally a normalized value between zero and one). A threshold is then applied to this value to dictate whether or not the sample is accepted or rejected.

For instance a human face contains about eighty significant features that can be used for biometric recognition such as the distance between the eyes, width of the nose, depth of eye sockets and the length of the jaw line. Figure 3-5 illustrates some of the recognisable nodal points and how they are utilised to form a unique identification matrix for an individual which can then be stored as a template (Heyce Technologies, 2014).



Source: Heyce Technologies (2014)

**Figure 3-5. Typical measurements taken during facial recognition**

Any authentication system that utilise biometrics as a means of individuation is foremostly judged by two significant results which are used to test the acceptability of the process and whether or not it could be adopted. The first is the False Acceptance Rate (FAR) and is defined as the percentage rate at which an impostor can pass as a valid subject; the second, the False Rejection Rate (FRR) is the proportion of times when a valid user is identified incorrectly as being an impostor. The Equal Error Rate (EER) is the point at which the FAR and FRR are coincident. Figure 3-6 shows in graphical form the relationship between FAR, FRR and therefore EER. The diagram indicates the influence of the tolerance/threshold<sup>10</sup> setting on the system performance; slack tolerance will clearly lead to FRR tending towards 0% and FAR

<sup>10</sup> The threshold controls how easily a user can pass the identification process. A reduced threshold dictates that a low matching score will be accepted as a match whilst an increased threshold implies that a higher score must be achieved to attain the same result.

neering 100%, whilst tight tolerance will result in a FAR approaching 0% and FRR 100%. The most desirable design of system will result in a minimal EER with the ultimate biometric authentications returning an EER of 0%.

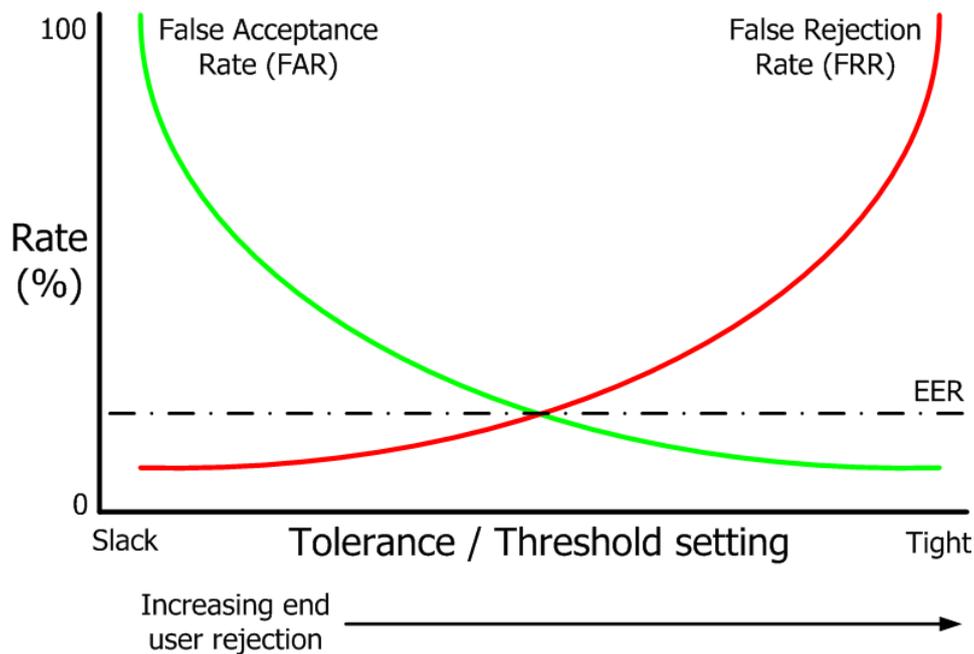


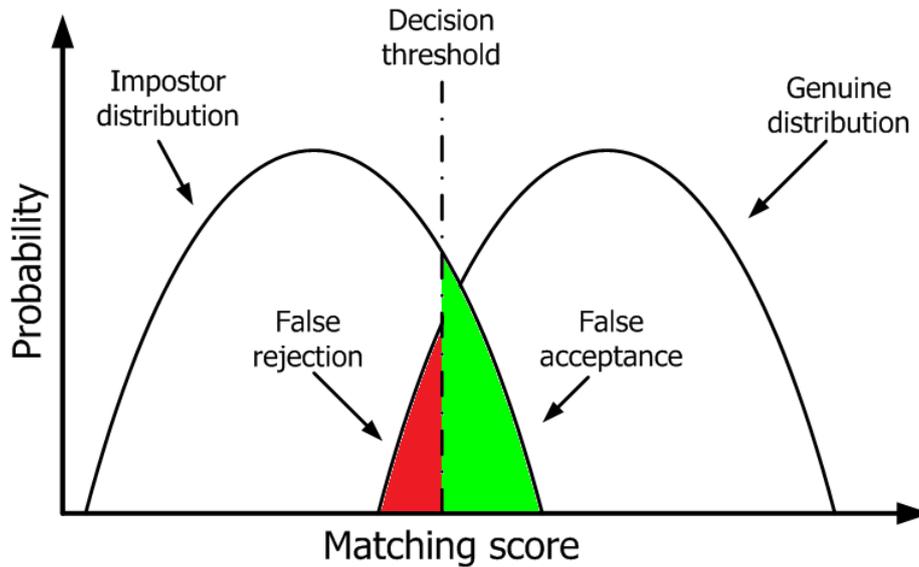
Figure 3-6. Biometric system performance rates

Although the FAR and FRR are the primary benchmarks by which biometric authentication systems are judged, there are two further error rates that should be highlighted. The Failure to Enrol Rate (FER) is the proportion of individuals who are unable to enrol on the biometric system because of either a technical failure, or absence of the required trait or feature. Clearly a high FER will significantly impinge upon the usefulness of a biometric system because a large percentage of the population would be excluded from using it; without being able to enrol they cannot be identified or authenticated.

The second error rate is the Failure to Acquire Rate (FAqR); the proportion of times that the attempted capture of a biometric sample fails. Failure to acquire can typically be caused by an equipment fault or external environmental conditions that are distorting the process in some way. For example, an external door entry system might use a video camera and facial recognition to control access. Poor lighting or extreme weather conditions might affect the image quality and therefore incur a high FAqR; or equally something as simple as vandalism might be the cause (Heyce Technologies, 2014). Whatever the reason, this could lead to a high degree of frustration being experienced by the subject attempting to use the system, affecting the confidence and general acceptance of the access control (Golfarelli et al., 2007).

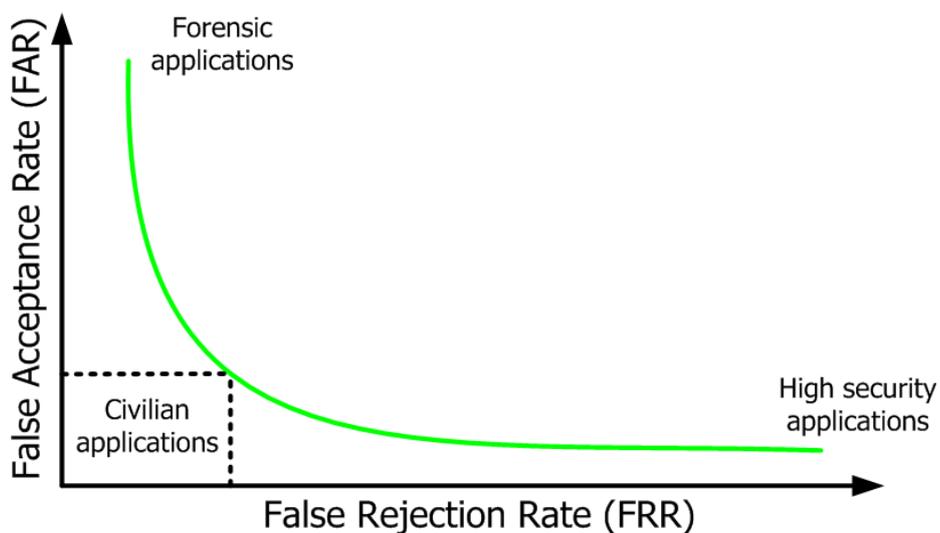
In a biometric authentication system the assessment of an individual's likeness to a known sample or template will deliver a matching score as illustrated below in Figure 3-7. Applying an

acceptance threshold will then dictate the proportion of attempts that occur in either the false acceptance or rejection regions. A tighter threshold with a higher matching score will shift towards the upper extremity of the impostor distribution and therefore reduce false acceptance. Conversely reducing the decision threshold increases the likelihood that a genuine user will be accepted (by reducing rejection) but equally the number of impostors passing will grow (Golfarelli et al., 2007). Figure 3-7 and Figure 3-8 are adapted from Prabhakar et al. (2003).



**Figure 3-7. How the threshold affects the Impostor and Genuine error distributions**

The level at which the threshold is set is greatly influenced by the arena in which the biometric authentication is to be used. Prabhakar et al. (2003) illustrate this influence and the accepted degree of associated error in Figure 3-8 shown below.



**Figure 3-8. Illustration of error tolerated within different application scenarios**

In Figure 3-8 it is illustrated that “civilian applications” occupy the middle area of the graph where the EER is located and the balanced minimisation of FAR and FRR leads to applications

that provide the best security with low hindrance to the subjects; that is, people are falsely accused of, or rejected as, being someone who they are not at an acceptable rate. In comparison, high security applications accept a high FRR because as far as possible these require minimal false acceptance, only allowing authorised individuals access into the protected system or environment. It leads to high rejections, forcing subjects to re-authenticate or seek authorisation elsewhere. Prabhakar et al. (2003) refer to “forensic applications” as ones that might be employed to undertake criminal identification, and suggest that they require minimisation of FRR. In these scenarios, false rejection is not identifying a known criminal or wanted person when their image is analysed. Authorities are willing to accept a high FAR in which a large volume of individuals would be wrongly identified, requiring manual resolution; they much prefer to check many to ensure none are missed.

Many physical human traits have been proposed and trialled as biometric indicators from overtly visible parts of the body, through the way people walk and speak (Bazin et al., 2005; Pennebaker and King, 1999; van Halteren, 2004), to patterns exhibited when undertaking familiar tasks but to fully understand the power and shortcomings of biometrics further exploration is required (Dowland and Furnell, 2004).

### ***3.3.3.1 Negative Identification***

Negative identification is the process whereby the “system establishes whether the person is who they (implicitly or explicitly) deny being” (Prabhakar et al., 2003), which further defines the “forensic applications” outlined in the previous section and Figure 3-8. It is used by governments and airport security to check that a subject is not a known terrorist or wanted person, it must be executed in identification mode. However if a high performing biometric system operates with a FAR of only 0.1%, in a large airport processing 175,000 passengers per day statistically 175 false alarms<sup>11</sup> would be expected. Although this does not appear at first to be a significant number the inconvenience, embarrassment and personal stress caused to the wrongly identified individuals could pose a public relation disaster for the airline/airport concerned. Bolstering the procedure by adding traditional individual recognition tools such as passwords or PINs would clearly be inappropriate for this process of negative identification.

Only recently have automated biometrics operating at a high rate of throughput become accurate enough to support large-scale identification applications, and arguably they provide the only solution where negative recognition is required. By operating it (and accepting the inevitable FAR) in conjunction with a human to scan all false alarms might arguably produce acceptable results whilst saving on a purely manual system (Planet Biometrics, 2014).

---

<sup>11</sup> This equates to approximately one every 8 minutes 14 seconds.

If the system aim is negative identification it is the FRR that is much more *politically* sensitive. In the scenario outlined above the FRR dictates how many sought individuals would be statistically expected to pass the security checks without being identified. In the worst case it would only require one *persona non grata* with terroristic intentions to be allowed through to result in a potentially catastrophic outcome; a risk that few commissioning entities would entertain.

### **3.3.3.2 Physiological and Behavioural**

Biometrics can be categorized in one of two ways: physiological and behavioural. Physiological techniques draw on geometrical attributes of the human body; typically fingerprints, but even hand geometry, retina scanning or vein pattern recognition can all be used. This category of biometric is considered more robust and reliable than behavioural metrics because the physical attributes offer greater resistance to change over time and are more likely to be unique across a large population (Gamboa and Fred, 2004; Monroe and Rubin, 2000). Behavioural biometrics utilise aspects of human behaviour to differentiate between individuals with measurements and comparison of voice, use of written language and even typing techniques being employed (Ahmed and Traore, 2007; Araújo et al., 2005; Cho et al., 2000; Dowland and Furnell, 2004;). This category of biometric is more prone to be affected by external environmental factors. For instance, background noise can seriously impact upon the quality of a captured voice sample, which would severely influence the observed performance level (Ngo et al., 2006; Pennebaker and King, 1999; van Halteren, 2004).

Physiological biometrics is more often preferred for identification purposes because of the greater degree of uniqueness, experienced consistency and resilience to external corruption. However, they are best suited to point-of-entry scenarios where an individual would be happy or certainly less discontent to tolerate the inconvenience necessary to undergo the required process of identification (IBG, 2006). For instance, having to place a hand upon a particular device, or head at a specific angle, to enable the relevant scan to be taken are both obtrusive procedures that should not be mandatory more than once in any session.

Conversely, behavioural biometrics suit authentication scenarios where the identity of the individual is already established and confirmation of a user's continuing presence is sought. In this mode of operation repeated unobtrusive/transparent samples could be captured and analysed to support the ongoing confidence in the user (Bazin et al., 2005; Clarke and Mekala, 2007; Pennebaker and King, 1999; van Halteren, 2004). This fundamentally supports the idea of a new approach to mobile device security where continuity of assurance is vital and presents advantages when compared with point-of-entry authentication. A review of the current state-of-the-art is made in Section 3.3.3.6.

### **3.3.3.3 Resistance to Attack**

Intuitively biometrics appears to be resistant to attack because they are generally measurements of subconscious or physical traits and therefore not something that can be lost or forgotten. They are complicated for attackers to counterfeit - creating a false finger with an embedded fingerprint is not a straightforward exercise and for an attacker there are no economies of scale in undertaking such an exercise, it is just as difficult to create the fourth or fifth facsimile as it is the first. However, making a speech recording to pass voice verification authentication is far easier and so fake biometric attacks remain a serious concern.

The threat posed by hackers can be addressed in two ways. By developing multimodal biometric authentication systems a user would be required to pass two or more specimen tests simultaneously; for instance, undergoing a retina scan whilst providing a speech sample to a voice recognition system (see section 3.3.3.5).

The second method involves building vitality detection mechanisms into the employed systems. Prompting a user to recite a randomly selected phrase or alternatively detecting signs of pulse during a hand geometry scan should be sufficient to establish the live presence of the subject.

The measures outlined above will make it very difficult for a hacker to mount a successful circumvention of security but there remain two further factors that should be highlighted. If an attack is successful and a biometric is compromised because of its permanence it remains compromised for eternity. A subject cannot supply or use an alternative, they have what they have. Additionally, with a wide adoption of biometrics it is likely that different access security systems would employ the same technique; thus once the biometric key has been acquired multiple systems become vulnerable (Prabhakar et al., 2003).

### **3.3.3.4 Privacy**

Although an in-depth investigation of privacy is beyond the scope of this document it is sensible to offer a brief review of this area of concern to ascertain implications that will need consideration in the future. As mentioned in section 3.3.3.3 once compromised a biometric cannot be changed and therefore when this occurs it remains an issue for the subject for their entire life. In many cases individuals do not have the choice to opt out of supplying biometric samples because of policy requirements that have been introduced by entities. There is no decision to be taken and the ability of the individual to choose is entirely removed (Down and Sands, 2004).

The use of particular biometric techniques in criminal investigation has incurred negative connotation and a barrier to general acceptance. Strong identifiers such as DNA or fingerprints

facilitate the possibility of unwanted identification. For safety reasons some people may be forced to legally maintain an alias which could be easily circumvented by biometric identification. This is often cited by objectors as a means by which government or corporate organisations could accumulate information and reduce the autonomy of individuals (Prabhakar et al., 2003).

It is near impossible for users to repudiate a biometric identification and with the unlikelihood of FAR's ever reaching 0% misidentification of individuals is always a possibility. In the future, biometric identification may be used as evidence in legal cases but however sophisticated the systems become it is unlikely they will be entirely accurate and so a degree of doubt will always exist.

With the advance of genetic and genome research it is possible that some physiological malformations might be associated with genetic disorders. Biometric samples are biological measurements which might inadvertently provide evidence of an individual falling into a high risk category and therefore afford a basis for discrimination (Fairhurst, 2003). With many biometric traits being overtly displayed (e.g. gait or a person's face) the opportunity to covertly identify people either in real-time or from recordings is possible. Additionally, in the desire to cut costs governments who are a significant driver of the technology are likely to outsource data and facilities to service providers, further raising privacy concerns (PR Newswire, 2014). Individuals could in fact be denied their right to privacy as biometrics are adopted and accepted more universally (Bazin et al., 2005).

Legislation and enforcement by independent regulatory bodies are the two main ways in which privacy issues can be addressed. With the potential for abuse, such entities are likely to face fierce objection from opposition parties with doubt being expressed regarding the impartiality of the regulators. An underlying agenda will always be assumed.

#### **3.3.3.5 Multimodal Biometrics**

“Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates” (Ross and Jain, 2004). With individual biometrics failing to meet appropriate levels of acceptance attention has been turned to combining techniques in multimodal authentication systems (Arandjelovic et al., 2006). Biometric systems are constructed from four main elements (see Figure 3-4); sample capture, extraction, template matching and decision, and fusion of information can occur at three levels; data/feature level, matching level or decision level.

It is believed that the most effective systems integrate information as early as possible with the best recognition results being achieved with data fusion at the feature level. However, this is extremely difficult to achieve because of data incompatibilities and limits of data access provided by commercial biometric applications. Fusion at the matching level is more common (Ross and Jain, 2004).

Number of Biometrics	Method of Processing	Detail
Single	Multiple sensors	Multiple sensors record the same trait
Single	Multiple classifiers	One sensor, one sample, multiple calculations
Single	Multiple units	E.g. integration of two irises or multiple fingers <sup>12</sup>
Multiple	One unit per biometric	E.g. voice, hand, fingerprint simultaneously or consecutively. Independence yields improvement

**Table 3-4. Outline of multimodal biometric implementation**

Multimodal systems can operate in three different modes; serial, parallel or hierarchical. In serial mode control is passed consecutively from one stage to the next and each modality narrows the number of possible identities before passing to the next. In this scenario an initial decision can be taken before acquiring the next sample helping to reduce the amount of processing.

In parallel mode, information is gathered and used simultaneously from multiple sources. The greater the number of modalities, the larger the amount of processing that needs to be undertaken. Hierarchical multimodal systems combine individual classifiers in a treelike structure. Typically, pairs of classifier combined at each tier before control is passed on to the next level. This is suitable when a large number of modalities are employed.

Factors to be considered when implementing a multimodal biometrics system are the choice and number of traits, the level at which fusion is to occur, methodology of integration, cost versus matching performance trade-off, and location and mode of data capture (Ross and Jain, 2004). A review of the current state-of-the-art is made in the following section.

### **3.3.3.6 Current Implementation**

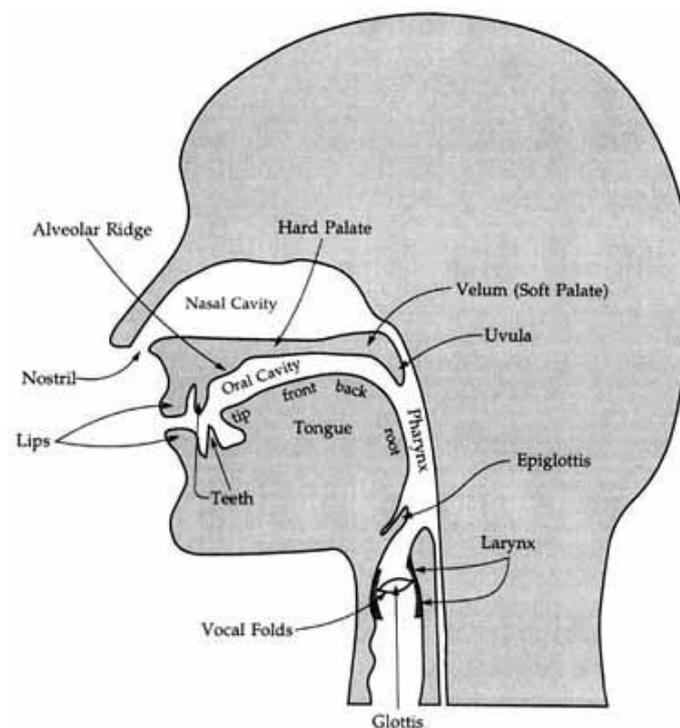
With technologists purporting that mobile biometric authentication will only ever become more significant and universal, and being driven by the need to undertake mobile financial transactions (Beranek, 2014) and protect sensitive information, it is necessary to review state-

<sup>12</sup> Using 6 fingers would stop an individual being able to register as two separate people

of-the-art approaches. The current lead technologies are voice biometrics, fingerprint, facial, iris and vein recognition, although historic proposals such as body odour detection are less likely to feature either now or in the future (Research and Markets, 2014; Welch, 2014).

### Voice verification

The technology that sits most readily with mobile phones has to be voice verification (speaker recognition) because it can be captured and undertaken unobtrusively and without notification. Rather than recognising the actual words that are spoken voice verification captures the sound of the person speaking, converts it to a digital pattern and then compares this to either a specific known voice pattern (authentication) or a database of samples (identification). Speaker recognition is an unusual biometric because it exhibits both physiological and behavioural elements; the voice is created by the physiological parts of the body contained within the voice tract as shown below in Figure 3-9, whilst behaviourally individuals pick up an accent which is usually dictated by region or parental influence (Bayometric, 2013).



Source: Peccei (2006)

**Figure 3-9. The human vocal tract**

With two factors influencing the way in which individuals speak it makes it difficult for imposters to precisely impersonate an authenticated user and gain access via a speaker recognition system, although the system can be fooled by the playback of a recording if a simple passphrase is employed (text dependent mode) (Bayometric, 2013). To counteract this weakness of narrative dependence systems often operate in either text prompted or text

independent (passive) modes (ICR, nd). In comparison, text prompted mode approaches operate by requesting the subject to repeat or utter a number of randomly selected numbers, words or phrases which are then compared to a known voice sample to verify identity; whilst text independent voice recognition usually works in the background, capturing spoken samples as the subject is speaking in general conversation and testing them to establish identity without using any specific narrative (ICR, nd). The quality of captured voice samples can be affected by the health of the subject, the communication channel over which the conversation is occurring and the amount of ambient noise in the background. These factors can intuitively lead to an increase in FRR because the system fails to recognise the speaker.

One big advantage of voice verification systems is that they can generally be implemented for minimal additional cost. With modern mobile devices usually being produced with inbuilt microphones they inherently have the ability to capture the required voice samples without the addition of any extra equipment. The only cost is that involved with the installation and configuration of the system on the device or point at which authentication is required (GlobalSecurity.org, 2011).

### **Fingerprint recognition**



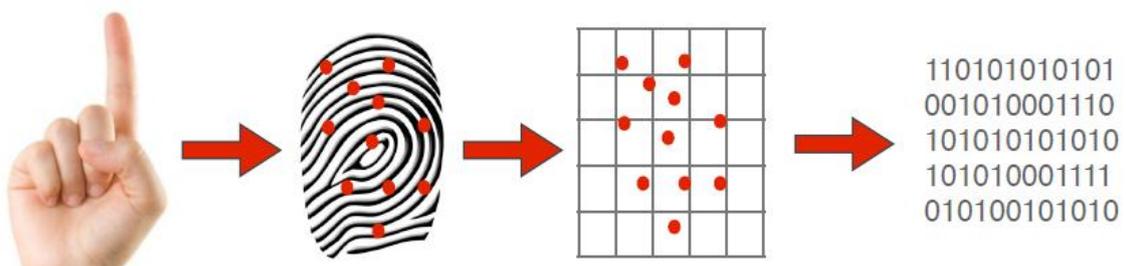
Source: Ridden (2011)

**Figure 3-10. A digital fingerprint scanner**

The previous chapter outlined some of the current implementations of fingerprint recognition on mobile phones and Section 3.3.3 also introduced how Galton had discovered the uniqueness of fingerprints and how they could be categorised and used to identify individuals. He identified that patterns on an individual's fingertip were made up of ridges of skin and corresponding valleys that formed minutiae such as arches, loops, whorls, ridge endings, bifurcations and spots (Biometric-Solutions.com, 2013a). From a user's perspective their adoption by handset manufacturers has made fingerprint security become one of the most

readily accepted biometric technologies. The barriers of historic mistrust have been broken down by familiarity of use either directly or within social circles. Electronic scans of an individual's finger originally utilised a dedicated external reader as shown in Figure 3-10, however more recently the technology has been incorporated into mice, laptops and phones directly increasing its availability (Apple, 2014; Drummond, 2014; Harris, nd).

There are four methods of digitally capturing the detail of a fingerprint, optical scanning, capacitance scanning, ultrasound scanning and thermal scanning (Biometric-Solutions.com, 2013a). They all produce an image depicting the ridges and valleys of the observed finger but perform the operation in entirely different ways. During optical scanning light is shone at the finger and reflected back into the scanner; ridges are closer to the scanner's surface and reflect more light, appearing as bright lines, whilst valleys are conversely dark. Capacitance scanning uses a variation in the skin's ability to store electrical charge (capacitance) to build the respective image. The capacitance of skin varies correspondingly to its distance from a surface imparting an electrical charge; the further skin is away, the lower the capacitance. The height variation of ridges and valleys is sufficient for the detector to differentiate between the two and so compile a corresponding image. Ultrasound scanners transmit sound waves through the epidermal (surface) layer of skin, that are reflected by the underlying dermal layer at different rates depending on whether it is a ridge or valley that is encountered. These variations in timings enable the formation of an image map that corresponds to the subject's fingerprint. Finally, thermal scanning uses the perceived temperature difference exhibited by ridges and valleys to construct the fingerprint image (Biometric-Solutions.com, 2013a; Harris, nd).



Source: Easy Clocking (nd)

**Figure 3-11. Steps taken to encode a fingerprint scan**

When the user places their finger onto or drags it across the scanner, the image is captured and the minutiae identified. These significant points form a pattern which can then be overlaid onto a grid and subsequently encoded into a digital sequence; these steps are illustrated in Figure 3-11.

The various types of scanner all come with associated issues. All but the ultrasound approach require the subject to have clean dry hands in order to be successfully scanned, although this ability and associated accuracy come with a high price tag. Thermal scanning is affected by both ambient temperature and the temperature of the subject, plus the method has a high power consumption rendering it less convenient especially for mobile devices.

Fingerprints do however have the great advantage of persistence over time, once the pattern of ridges and valleys are laid down in the womb they remain with an individual virtually unaltered throughout their life. Even if the surface layer of the skin is removed, during re-growth the same identifiable pattern returns; only if a relatively deep cut is made might the pattern be permanently disrupted although this in itself is a unique identifiable feature (Ramsland, nd).

### **Facial recognition**

Facial recognition is also one of the more common biometrics that have been endorsed and implemented by some of the more popular mobile handset manufacturers (Apple, 2014; Kerr, 2014). With smartphones incorporating both forward and user facing high resolution cameras it became a matter of software implementation to harness this physiological biometric technique. As shown earlier in Section 3.3.3 Figure 3-5 on page 36 facial recognition works by analysing a captured image to detect the face and then ascertain specific points of reference (Biometric-Solutions.com, 2013b); there are up to eighty features that can be used (Heyce Technologies, 2014). From these points spatial geometry calculations are then made and a digital template formed. The identification or verification process then compares the captured sample with known and stored reference templates to locate a match if one exists.

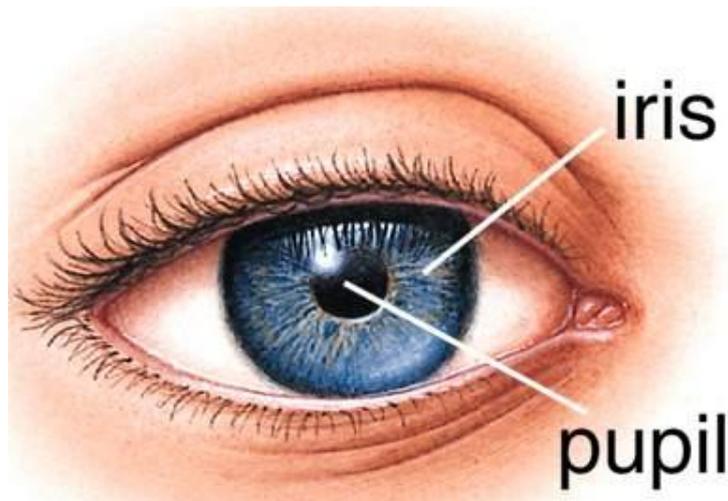
Unlike fingerprints facial images are not persistent. With ageing occurring and individuals growing or removing facial hair although the underlying bone structure remains unaltered, the geometrical template might change or fail to be established. An additional weakness is that the capture process can be easily influenced by external factors such as poor lighting, the subject not looking directly into the camera or even in centralised systems, the resolution of the camera distorting the image leading to template inconsistencies (Biometric-Solutions.com, 2013b).

It has also been demonstrated that some facial recognition systems can be fooled into accepting photographs as valid identification even when vitality tests are incorporated (Colon, 2013; Kelion, 2013). Folding a photograph in a particular way can be used to simulate a blink and be enough to trick the system. To further counteract these flaws some manufactures are

proposing that more extreme facial expressions be used that truly require a live person to perform (Gorman, 2013).

### **Iris recognition**

Iris recognition has for a long time existed in the realm of science fiction and spy films, although more recently it has emerged within real life technology. The iris is the coloured circular structure in the eye which dilates and contracts in response to light, resulting in the appearance that the pupil is correspondingly growing or shrinking (Riverside, 2007).

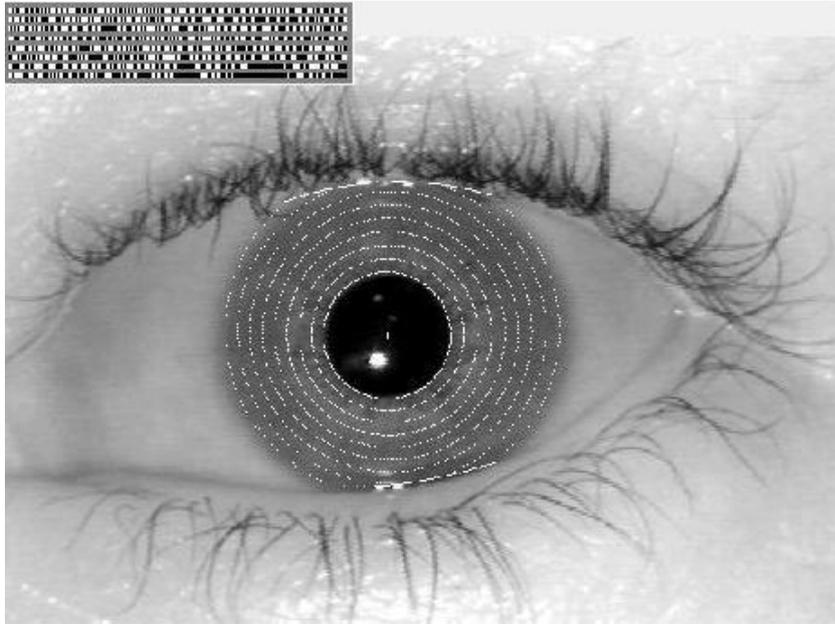


Source: Riverside (2007)

**Figure 3-12. Illustration of a human eye showing the iris and pupil**

Iris recognition utilises the unique colour patterns that occur within the thin structure, an automatic classification algorithm for which was first devised and patented by Dr John Daugman in 1994 (FBI, nd). During the process an image of the iris is captured via a high resolution camera using near infrared light (NIR) to illuminate the subject's eye whilst reducing reflections and without causing them discomfort or harm. The location of the iris within the image is a vital element in the process and requires the accurate identification of the concentric outer edges of the pupil and iris. Often part of the iris is obscured by an eyelid or lashes, further complicating the process (Biometric-Solutions.com, 2013c).

Once the precise location of the iris has been established a two dimensional Gabor wavelet filters and maps the identified region into eight concentric vectors that contain information pertaining to location and spatial frequency. From this information a Daugman's 256 byte IrisCode can be derived and used as the biometric template (FBI, nd); Figure 3-13 illustrates a captured iris scan, the eight vector regions and the calculated binary IrisCode. With a template size of only 256 bytes it enables samples to be compared at a rate of over half a million per second (Biometric-Solutions.com, 2013c) and a misidentification rate of one in 1.2 million (Sheth et al., 2014).



Source: Ibiblio.org (nd)

**Figure 3-13. An iris scan showing the vector regions and derived IrisCode**

Being internal to the body and consequently relatively well protected iris patterns are unflinching and permanent throughout the life of an individual. Failure to enrol rates, that is the proportion of people for which it is not possible to obtain an iris scan, are very low although the process of enrolment itself can be difficult because of lighting issues and intrusive to subjects (Biometric-Solutions.com, 2013c; Sheth, 2014).

### **Retina recognition**

Another form of ocular biometric recognition is retina scanning although because of its intrusive nature, requiring the user to get extremely close to a scanner and have a light shone deep into their eye, it is less commonly employed. The retina is the internal surface of the eye which is rich in blood supply and it is the complex network of capillaries that form unique patterns that can be detected and used for identification (Trader, 2012). As the retina is illuminated with NIR the blood rich capillaries absorb more light than the surrounding surface and appear as dark rivers within the eye. The pattern of light and dark can then be scanned and synthesised into a template. Unfortunately the retina comes without the assurance of guaranteed persistence because conditions such as diabetes, glaucoma and retinal degenerative disorders can all affect the capillaries and therefore alter a scanned sample (FBI, nd; Trader, 2012).

### **Vein recognition**

Another variation of the same approach is vein recognition which leverages the pattern of blood supply within a finger or hand for individuation. This physiological biometric process is non-contact and poses little inconvenience to the subject with the underlying vein structure

being revealed once again by the use of NIR light (Vrankulj, 2014). With the veins being located beneath the subject's skin the pattern is virtually impossible to forge making the approach one of the most secure in today's security conscious world with an associated FRR of 0.01% and FAR of 0.0001% (FindBiometrics, 2014). Although vein size can alter with the age of the subject the relative pattern remains unaltered yielding a high degree of persistence.

Vein recognition systems have the added advantage of being able to be incorporated into other items of technology such as fingerprint scanners; for example the reader depicted earlier in Figure 3-10 has that very function built in (Ridden, 2011). It is also not essential that direct contact with the reader is made, enabling the template to be extracted over short distances as shown below in Figure 3-14 (FindBiometrics, 2014).



Source: Fujitsu (nd)

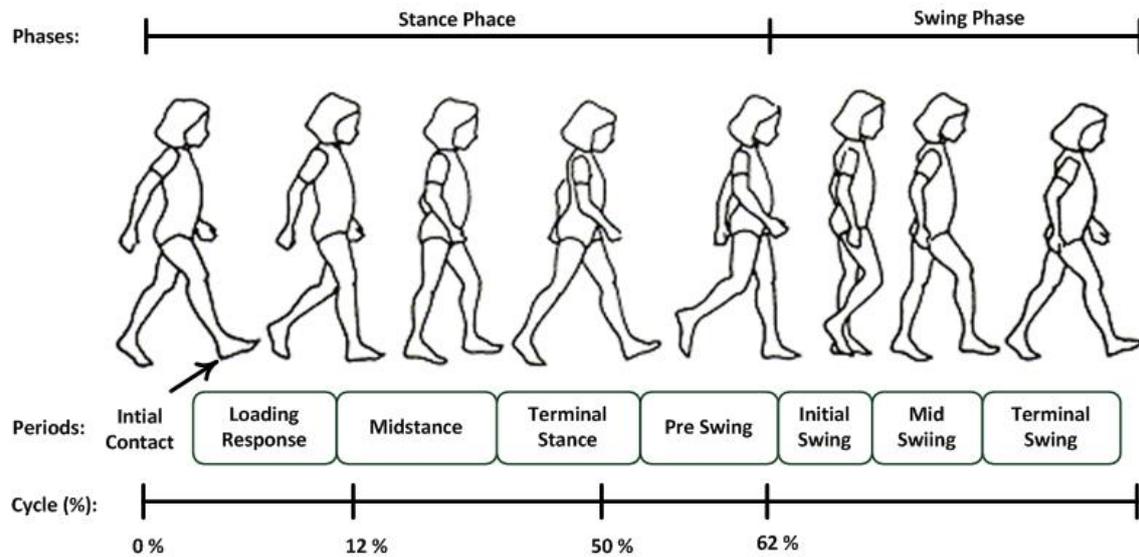
**Figure 3-14. An example of a palm vein reader**

### **Gait recognition**

With the inclusion of accelerometers in smartphones and tablet computers, continuous authentication via the use of gait analysis with minimal implementation costs has become a real possibility (Nickel et al., 2011). Identification via the way in which individuals walk is based upon five detectable motion periods of the stance phase and three within the swing phase as demonstrated by Figure 3-15. There are three employed methods for capturing a person's walk, Machine Vision (MV), Floor Sensor (FS) and Wearable Sensor (WS); the modern devices with inbuilt accelerometers use WS based gait analysis (Derawi Biometrics, 2011).

WS data collection records acceleration information in three axes; vertically, backwards-forwards and side to side and the combination of these readings during the eight periods of a stride are drawn together to form a template (Nickel et al., 2011). Intuitively the effectiveness of gait analysis can be affected by the surface on which the subject is walking, an injury or even the footwear that they are wearing. Having so many external influences it is unsurprising that

researchers are observing EERs of 10-20%, which although useful as a supporting authentication method would be deemed unsuitable for primary security implementations (Nickel et al., 2011).



Source: Derawi Biometrics (2011)

**Figure 3-15. Subdivisions of human gait used for categorisation and identification**

### Keystroke dynamics

If unobtrusive and transparent authentication is the aim one behavioural biometric that is ideally suited to the role is keystroke dynamics. Classification of typing characteristics or keystroke dynamics is based upon the timings with which keys are pressed and for how long they are held down whilst a subject is typing. The latency between consecutive keystrokes (digraph) (Araújo et al., 2005; Bergadano et al., 2003), the length of time it takes to type complete words (Dowland and Furnell, 2004) and associated typing rates (Bartolacci et al., 2005) have all been investigated as a means of classifying an individual. When a key is pressed there are three distinct actions, the key depression, the key release and the holding of the key in the down position. If extended in the consideration of a digraph pair the measurements that can be used for analysis on a keyboard are; the timing interval between the two key depressions, the gap between the release of the first key and the pressing of the second, the total digraph length - the elapsed time between the pressing of the first key and the release of the second (or the first if for some reason this is held longer than the second). It should be noted, that the inter-key latency can in fact be a negative value as often a keyboard operator will have pressed the second key of a digraph before releasing the first. However when implementing keystroke dynamic verification on mobile devices it is clear that some of the timing measurements outlined above will not be applicable in the absence of a physical keyboard that requires the keys to be pressed. It is more likely that this type of implementation will use digraph timings and typing rates.

With subjects regularly using mobile devices to compose emails, text messages and interact with social media, a background keystroke analysis system could easily capture the required data unobtrusively and monitor user identity.

As introduced earlier there are seven criteria that biometric techniques must meet in order to meet implementation requirements; universality (1), distinctiveness (2), permanence (3), collectability (4), performance (5), acceptability (6) and circumvention (7). Table 3-5 below compares the degree to which the criteria are met by each of biometric techniques discussed in this section; 'H' signifies a rating of high, 'M' medium and 'L' low. To aid direct comparison between criteria column 7 should be read as resistance to circumvention in contrast to Jain et al.'s (2006) presentation of the data, and within the table the approaches marked with an asterisk have been added by the author for completeness.

<b>Biometric approach</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>
Facial recognition	H	L	M	H	L	H	L
Fingerprint recognition	M	H	H	M	H	M	M
Gait recognition *	M	L	L	H	L	H	M
Iris recognition	H	H	H	M	H	L	H
Keystroke analysis	L	L	L	M	L	M	M
Retina scanning *	H	H	M	L	H	L	H
Speaker verification	M	L	L	M	L	H	L
Vein recognition *	H	H	H	M	H	M	H

Adapted from Jain et al. (2006)

**Table 3-5. Criteria comparison of discussed biometric techniques**

When the approaches are compared it is evident that vein recognition meets the criteria in the strongest way without any low scores, whilst keystroke analysis is deemed the weakest technique. However, if any of these methods were being utilised as part of a multimodal approach they can contribute significantly and greatly enhance security.

### **3.3.3.7 Summary**

As biometrics are introduced into smartphones and arise in everyday situations user acceptance grows correspondingly. Third party manufactures are releasing software development kits (SDKs) for Apple's iOS, Android and Windows phones that utilise physiological biometrics, enabling developers to easily incorporate these into app security (Mobbeel, 2014). Furthermore, these SDKs provide end users with the ability to layer-up biometrics in an individual combination, yielding a multimodal solution that is specifically tailored (Top, 2013).

Facial recognition security has also been implemented across all the major platforms as a means of securing devices although some go further requiring users to perform a gesture such as a wink or raising an eyebrow in order to pass (Gorman, 2013). Apple have recently taken out a patent in the US to invoke additional control via face recognition, enabling screen savers to be blocked or caller id information to only be displayed when the user is detected as being in front of the screen (Colon, 2013).

Recent reports have estimated that the global government biometric marketplace will grow by 6.8% during the next ten years and be worth US\$6.9 billion by 2024 (Atkins, 2014). With government spending as the key market driver and the desire to implement tighter security at borders, the expectation of the growth in numbers of terrorist groups and the increasing need to protect data, this figure is seen as unsurprising (PR Newswire, 2014).

It has also been suggested that North America will be the dominant marketplace for biometric technology in the upcoming years and it is projected that fingerprint recognition will account for 43% of all biometric business, facial recognition 26% and iris/retina scanning 13.2% (Atkins, 2014). Of course, as technology continues to evolve alternative cheaper methods of implementation might be identified that will counter these predictions and take the marketplace in another direction altogether.

Whatever the future may bring, it is clear that the biometric revolution has begun and as people become more accepting of the technology it will pervade ever further into everyday life. Humans are inherently lazy and in an attempt to ease the security burden manufacturers and developers alike are implementing novel solutions. However, it is apparent that the majority of these are still point-of-entry either upon activation or for unlocking a device. If a device has not been set to timeout and invoke a lock screen or without activation security the device is and will always be vulnerable.

#### **3.3.4 Polled and Non-polled**

Authentication can fall into one of two categories, polled and non-polled and it is necessary to distinguish between these in order to understand how any new concept can utilise aspects of each. Non-polled authentication is user driven in that subjects present themselves to a system and demand to be authenticated with the process being “resolute - once the verdict is determined, it is inviolate until the next authentication attempt” (Jansen et al., 2004), i.e. upon authenticated acceptance or rejection by a system, the respective associated security status remains constant and unchanged until another attempt at authentication. The only action that can alter the status is the process of re-authentication and the user undergoing the entire

procedure again from scratch. Examples of non-pollled authentication are passwords, facial recognition and hand geometry.

Conversely, polled authentication is system driven and uses the presence of tokens or RFID devices. This approach is irrefutable and the detection of such tokens is regarded as being sufficient to establish authentication which remains true whilst the object continues to be present. Upon the device being transported out of detectable range authentication can be repudiated immediately. Continual sensing of the accredited token allows authentication to be reassessed at any time leading to a greater confidence in user continuity. However, any such token can easily be acquired illicitly and if its mere presence is unilaterally enough to engender authentication, the system should not be regarded as secure.

### ***3.4 Conclusion***

This chapter has explored the theory of identification and how sameness and persistence over time forms the foundation for both human-human and machine-human recognition. Although the philosophical and psychological discussion of identity is removed from the purely technical arena, it provides an understanding of what is truly meant by recognition and the process undertaken by the human mind to do so. Elements of this can be used in a novel approach to mobile device security.

It then proceeded to examine each of the three forms of technical authentication, something that is known, something that is possessed or something that we are; reviewing the strengths and weaknesses of each and discussing means of application.

Section 3.3.1 explored the use of knowledge based PINs and how modern technological developments have augmented its implementation. Although superficially these are secure means of authentication, examples of human frailty highlights the need for further development or indeed replacement.

Similarly token or possession oriented authentication has its weakness inextricably linked to human beings and their propensity to lose or share security sensitive items. Although with smart watches becoming more prevalent throughout society the potential to utilise more subconsciously held tokens grows, the threat of loss is still ever present. Consequently focus has turned towards security with greater imperceptibility, biometrics (Donohue, 2013).

A detailed investigation of biometrics has been outlined, discussing how systems operate, their resistance to attack and the difference between physiological and behavioural categories. Contemporary implementations of the technology have also been presented providing an understanding of the current state-of-the-art, although it is important to note these are

standalone, provide security for a single device and are only used if directly invoked by the owner.

In the majority of the reviewed technology and approaches authentication is Boolean and point-of-entry; once access has been gained the user is free to roam through the device, being able to view all information contained within and utilise any of the installed applications and services. Authentication is simply a gateway to unrestricted freedom. With this justification, there is certainly a need for a new and novel approach to security, one that continually reviews the user and assesses on an app-by-app or service-by-service basis what is available for use at any given time. The succeeding chapter introduces a new approach to authentication and how it can be implemented to protect against these obvious shortcomings.

---

## **Chapter 4**

# **A New Approach to Authentication**

---

## **4. A New Approach to Authentication**

---

The preceding two chapters have examined the rise in proliferation of mobile devices, their increased portability and processing power, and the current approaches to security upon which owners rely to protect these valuable and desirable items of equipment. Currently manufacturers and developers provide security that is unresponsive or adaptive to threat, environment or use, and is primarily focussed on keeping out persona non grata at point-of-entry.

As the public at large routinely carry more devices and move towards ubiquitous connectivity it is reasonable to suspect that an opportunity exists to harness this potential and in some way use it in a novel approach to security. This chapter explores the premise by firstly examining the potential that exists within an individual's locale and how this might be harnessed. It then continues to discuss an experiment that has been performed to assess this potential, and analyses if data obtained during the experiment provides sufficient evidence to support this theory.

The chapter then concludes by introducing a novel approach to user authentication that is both adaptive and responsive, which can grow and develop with technology and provide the user with assurance not currently seen. It enables the device's owner to adapt the security per application or service, setting levels of access reflective of location and familiarity of surroundings and because it liaises and cooperates with other items of equipment, it even has the potential on occasions to dispense with obtrusive authentication.

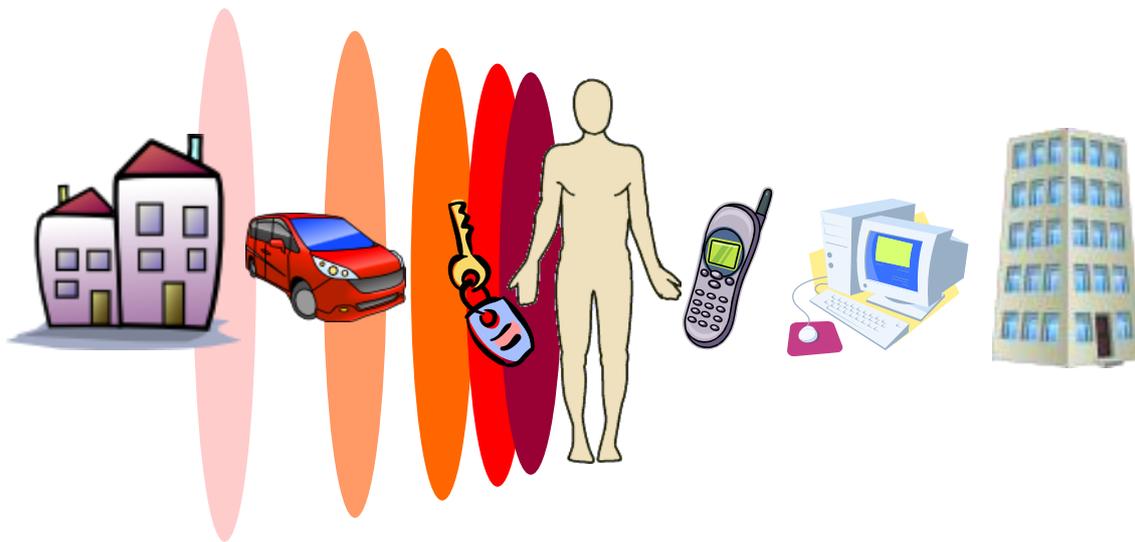
### ***4.1 The Concept of an Authentication Aura***

In everyday life individuals are enjoying almost total connectivity as they go about their everyday life with pressure of work and addiction to social networking encouraging uninterrupted access to the internet, email and the mobile phone network. Coupled to this, people are concurrently carrying numerous pieces of electronic equipment such as laptop computers, tablets, smart phones or MP3 players, and with the internet of things becoming reality, a bubble or aura of technology is forming around each and every person. This is not a single location or a fixed set of equipment but a fluid and ever changing environment, which alters as an individual physically travels throughout the day, going about their business, interacting with technology and the environment.

Within this bubble devices are utilised both in isolation and unison depending upon the process being performed. For instance sending a text message requires the use of just a mobile phone, whereas printing a document from a laptop utilises both the computer and printer

concurrently. During each interaction or device initiation a level of security and user identity confidence is established and exists between the user and the device(s); this in turn 'radiates' within the user's personal localised environment. Couple this confidence and bolster it with other readily available information within the locale such as details of communication infrastructure, and the concept of an Authentication Aura is born.

To summarise this and for the purposes of the research an Authentication Aura is defined as an area of close proximity to an individual in which an increase in user identity confidence can be gained from other trusted and present devices, their current state of authentication confidence, the surrounding location and the behaviour of the individual.



**Figure 4-1. The concept of an Authentication Aura demonstrating contributing elements**

If the concept of Aura as illustrated in Figure 4-1 is extrapolated across a population it is clear that several individuals will coexist in a single location at any given moment in time, being concurrently close to items of known infrastructure and even sharing equipment. Although elements of the Aura are not mutually exclusive, with the incorporation of personal electronic items and even superficially inert (dumb) belongings, it becomes unique. For instance, car keys and contactless payment cards are items that are covertly carried, with a capacity for detection and the potential to individuate one person from another but in themselves are unable to perform computation or interact autonomously. Furthermore, with the internet of things materialising, home appliances such as refrigerators and televisions are becoming internet enabled and will also have the inherent ability to contribute (Fritz, nd).

With its capacity to be unique it is proposed that an individual's Aura can be leveraged to provide a novel approach to device security. As discussed earlier, current approaches to security all function unilaterally, treating each particular device as an island without knowledge of surroundings and other possessions. As users authenticate on one device, trust is

established and the respective device has a high degree of confidence in its user's identity. This knowledge is currently kept private but if shared amongst the user's other equipment a personal network of assurance could be established benefitting all items within the Aura. Conversely if an Aura is established and a device has knowledge of its counterparts and surroundings, if for some reason it is then removed and it detects a change in location the device can react accordingly and immediately reduce service availability. Security becomes responsive.

Attaining this cooperative and reactive approach to security will definitely improve upon the unilateral methods in existence today but intuitively this premise requires justification.

## ***4.2 Justification of the Aura Concept***

Having defined an individual's Aura and proposed how people exist in proximity to a unique set of devices, infrastructure and possessions, it is necessary to investigate this concept to establish to what extent this is the case. To enable this, information regarding the presence of devices and possessions in close proximity to an individual at any given moment needs to be collected and analysed. It is not sufficient to simply take a number of snap shots of a lone individual at distinct points in time, rather a continuous and extended survey is required to capture the number and types of device that are encountered throughout daily life. Any undertaken survey must be able to identify intelligent devices, inert possessions, infrastructure and even home appliances and equipment that might become enabled in the future, and then record details of the identification (such as the date and time, and for how long they were detected). The proposal additionally outlines that each and every person has their own unique set of devices (Aura) that coexists with acquaintances and strangers alike, as they move throughout their daily life. At any given locale, at any point in time there maybe any number of Auras which simultaneously need to be identified and the presence of their constituent devices recorded.

To achieve this, a data capturing experiment is required which will assess the quantity and type of equipment that surrounds individuals within close proximity throughout the day, and provide information which can be analysed to further this research. Importantly the experiment will need to concurrently survey a number of people who live or work together so an assessment of how Auras simultaneously exist within the same space can be made. Not only will each experiment subject's device details need to be identified and recorded, but those of their friends and colleagues will also require the same. This dual data will provide sufficient detail to ascertain the importance of the role of devices considered alien to an individual's Aura.

For the concept of Aura to function a user must regularly encounter two or more devices simultaneously and so it is thus proposed that the hypothesis for this experiment should be: an individual regularly encounters two or more devices from which user identity confidence can be gleaned and combined to form an Authentication Aura.

In the succeeding sections the experiment is proposed and explained, outlining the rationale behind the selected approach, examining the gathered data and the analysis of that data. Finally a discussion of the results is performed, concluding the experiment's efficacy, potential support for the Aura concept, and whether or not to accept the hypothesis.

#### **4.2.1 Experiment Design**

As outlined above the experiment needs to record time-stamped information that can be used to identify each specific device, in addition to the quantity and types of device surrounding a number of individuals at any moment, and for how long each item remains in close proximity. This will allow meaningful analysis to be performed on the data in a variety of ways. It would be relatively straightforward to execute such a task on entirely intelligent devices because software could be designed, written and installed that would record the subject's daily activity and other detectable equipment that was encountered. However the premise dictates that both dumb objects and equipment that might become intelligent in the future are also included.

To summarize the three key requirements of the experiment are:

1. The ability to sense infrastructure such as Wi-Fi access points.
2. The capacity to detect a wide range of device types some of which may not currently possess the ability to communicate (but will conceivably be able to in the future) e.g. mobile telephone, laptop, personal computer (pc), printer, mp3 player, television, telephone, car keys, wallet, refrigerator, handbag or briefcase, watch.
3. To capture and record sufficient time-stamped information to enable a statistically significant investigation to be undertaken and a decision to be made to either accept or reject the hypothesis.

An obvious solution would be to provide experimental subjects with pen and paper to record devices and items that surround them at any given moment, over a period of days. Intuitively this is far from practical. Forgetfulness and sheer imposition renders this an inappropriate approach; an alternative means of surveying an individual's surrounding locale had to be found.

Consideration was also given to a mixed solution; develop software to run on a mobile phone that would automatically record details of surrounding devices and infrastructure via Wi-Fi and Bluetooth, whilst providing an interface for the user to manually record inert items. Again this was thought to be too intrusive, impractical and unreliable.

To enable analysis that identifies the user and those that were encountered it is necessary to record the user identity, the detected device identity, the time and date that the device was observed and (if possible) an indicator to reflect the proximity of the entity to the user. If this process is repeated at short intervals it will illustrate the arrival and disappearance of users and their equipment, whilst providing a near continuous picture of the local environment. Thus, the experiment needed to be able to detect and record data autonomously, without intervention from the subject, continuously throughout the day, with the requirement to include dumb and currently incapable devices. Additionally it required the ability to differentiate between users' Auras, so the approach had to identify owned and unowned devices in such a way as to provide separation at the analysis stage; precisely identifying each item and knowing its owner would provide the required detail post-experiment. To achieve this radio frequency identity (RFID) was identified as a means of fulfilling the experiment's requirements. This was selected because it provided the ability to attach RFID tags to a diverse selection of objects, irrespective of capability and independent of power, that would possess a unique identity whilst remaining portable and unobtrusive.

An RFID tag is a small low power electronic object that will transmit a unique numeric or given identity, across a short distance, which can be detected by a collector or reader. RFID tags are either active with an inbuilt battery powered transmission capability or passive with no obvious power supply (Weinstein, 2005). Passive tags are triggered into emitting their identity by a reader, extracting induced power from the requesting transmission. Passive tags can be obtained for relatively low cost and typically have a small physical footprint, their one major drawback is that they are limited to operating over very short distances (less than 0.5m). The readers required to utilise a passive RFID system are bulky hand held devices that would need to be carried by the experiment volunteers (Weinstein, 2005).

In comparison, active tags are larger, more costly but with their inbuilt power supply are able to transmit their identity constantly and autonomously. Additionally they operate over much greater distances (up to 15m) and can be detected through walls and other solid objects. With the constant chatter that they generate, active tags can be detected by several readers at once, enabling multiple subjects to be in the same location without the threat of disruption to the experiment. The associated reader for active tags has a smaller and more practical

footprint which can generally be worn attached to a belt or carried in a pocket (Weinstein, 2005).

It was clear that an individual furnished with a number of RFID tags could then attach these to devices, infrastructure and personal items, enabling a reader to detect and record their presence. By extrapolating this across a number of co-workers, data could be simultaneously gathered for the group and detection of one another's possessions obtained, providing the required details for analysis. Active tags provide a continuous transmission stream of their identity, enabling the users to move freely and immediately identify equipment when in close proximity.

To facilitate the experiment equipment was sought and purchased to enable the recording of data simultaneously for five subjects. Although in an ideal world as many candidates as possible would undertake the experiment at any one time, the prohibitive cost of equipment restricted the sample groups to five, an affordable number that would yield a meaningful set of results. The personal digital assistant (PDA) RFID readers were Dell Axim x51s running a Windows mobile operating system and each was equipped with a CompactFlash RFID node, capable of reading both passive and active RFID tags. With the need to detect Wi-Fi points and other infrastructure, it was deemed prudent to secure active tags that would communicate over a greater distance. The price of the tags with batteries was £23 each and with the need to equip each participant with as many as possible the cost immediately became an issue. However, it was necessary to acquire a sufficient quantity to allow items to be tagged both at work and home so monitoring across a full day was possible, whilst enabling a cross section of devices and belongings to be selected. Funding to underwrite the purchase of seventy five tags was secured enabling each individual volunteer to be supplied with fifteen, permitting them to identify and record a sufficient number of devices both at home and in their workspace.

To record the observed data software was written in VB.net using Visual Studio 2008 and released to the PDAs; the program is listed in Appendix A. It was designed to operate on a 24 hour basis, sleeping for 50 seconds, awaking and then listening for 10 seconds, recording all the tags it identified in the near vicinity during the process. The system was designed to maintain two flat text data files during operation; the first was a summary file that recorded the subject's number, the number of detected tags, date, time and a sequential number that would increment upon each listen. The second file recorded the details of each tag that was detected during each listen and held the unique tag reference, the subject's number, date, time, the listen sequence number and the signal strength of the tag's transmission.



**Figure 4-2. A PDA with installed RFID node and five RFID tags**

Figure 4-2 above shows one of the purchased PDAs with an installed CompactFlash RFID node and five of the active RFID tags with their visible batteries in situ.

Intuitively the tag data files had the propensity to become extremely large, for instance if on average only five tags were detected at every listen a single day would generate 300 data items every hour or 7200 items every day. If the experiment was to run for a week, that figure would extrapolate to 50,400 separate tag detects. On a laptop or tablet with sufficient processing capability these figures are manageable, however on a PDA with much less computational power and storage capacity the text file data capture becomes restrictive. To counteract this, the system was designed to record the data on a day by day basis and at midnight close the current files and create a new ones ready to receive the upcoming information.

During trialling and development it was discovered that the PDAs upon first detection of a tag set a lock which blocked it from communicating with any other reader. Thus if two participants were simultaneously in the same locale, the first to arrive would lock the surrounding tags and prevent the later arrival from sensing any of the beacons. In order to prevent this shortcoming a release command had to be issued at the conclusion of each listening window, to remove the lock and allow other readers access to the tag. In addition, to prevent two readers having their activity at the same time, the internal clocks of the five PDAs had to be precisely synchronized and each staggered with a different start time during a minute. For instance, PDA number one

was programmed to start its listening period at precisely the start of each minute, PDA number two at twelve seconds after the start of each minute, PDA number three at 24 seconds, four at 36 seconds and finally the fifth at 48 seconds or twelve seconds before the start of the next listen by PDA number one. By separating the listening periods in this way it prevented any of the PDAs from blocking any of the others.

Instructions were then compiled (Appendix D), ethical approval sought and granted (Appendix E), and the experiment was prepared; all that remained was to recruit the experiment's subjects.

It was decided to run each experiment for a period of 14 continuous days to provide a sufficient quantity of readings that incorporated both weekdays and weekends. Groups of volunteers were sought who worked in a single location to provide some crossover of Auras, with each individual receiving fifteen tags and instructed to place these on or by devices or personal belongings both in the workplace and at home. Some tags were to be placed on communal equipment that would be shared and used by many during a normal working day. For instance, it was suggested that a photocopier or printer be chosen, or even a refrigerator within a communal kitchen. The precise list of suggestions that was made to the volunteers was mobile phone, work PC, home PC/laptop, work Wi-Fi point, home Wi-Fi point, TV(s), car interior, car keys, wallet/purse, MP3 player, work bag/briefcase, home telephone, bedside clock, fridge, Hi-Fi and coat pocket.

Companies outside of the academic arena were specifically targeted because it provided an opportunity to explain the research to lay people, gauge their reaction and whether they believed there was merit in the novel approach to authentication. Each of the companies approached had to be of a sufficient size to ensure five co-workers would be willing to volunteer and in fact several companies immediately refused to participate on the misunderstanding that the experiment would contravene in situ privacy policies and Data Protection. Eventually four companies agreed to cooperate: a school, a firm of local accountants, a scientific research establishment, and a highways department within a local authority. Each company was visited in turn, the volunteers briefed and the experiment performed.

Anecdotally the majority of volunteers at first meeting expressed a reticence at participating and were keen to understand more fully any potential impact upon their privacy. However, once the data collection was verbally explained in detail and how the information would be used any signs of mistrust disappeared. Universally they were extremely interested in the concept and understood how it could benefit them as users, agreeing that they found the onus

of repeated authentication burdensome. Two of the accountancy staff felt that they used technology so infrequently that it would not impact them significantly, although if it were extended to PC desktops (which it could easily be) they would acknowledge increased convenience.

#### 4.2.2 Gathered Data

**Tag Inventory**

Please fill-in the table below as you are positioning the tags (blue plastic blocks) so upon completion of the experiment it will be possible to analyse the data in a meaningful way. Failure to do this accurately will render your participation in the experiment unusable, so please take care when entering the information.

Number	Tag id code (code written on tag)	Location (home, work, car, N/A)	Equipment description (e.g. mobile phone, work PC etc.)
1	44	WORK	Fridge/Kettle in Van (ALU) <del>Antenna Lab</del>
✓ 2	14	WORK	Asbestos LAB microscope
✓ 3	8	"	Locker
✓ 4	10	"	Desk computer
✓ 5	36	"	Fax machine
✓ 6	41	"	Mobile phone (work)
✓ 7	7	HOME	Kitchen - <del>fridge</del> Fridge
✓ 8	42	"	LOUNGE - DESK TOP Comp
✓ 9	9	"	Bedroom - Phone (also next to clock)
✓ 10	38	BAK (work/home)	-
✓ 11	15	N/A	Coat pocket
✓ 12	9	N/A	Wallet
✓ 13	37	HOME	TV (also next to wireless & hi-fi)
✓ 14	12	MY CAR	-
✓ 15	40	<del>WIFE'S CAR</del> HOME / CAR	MP3 player
16			

Figure 4-3. User 3's completed tag location form

Upon completion of each 14 day tranche of the experiment the created data files were downloaded and the PDAs reset in preparation for the next set of volunteers. Each of the seventy five tags possesses a unique 12 digit hexadecimal reference that it would transmit (e.g. 8A11F411574C) but for user convenience had been labelled with a sequential number 1-75. As part of the experimental process each volunteer was requested to identify each of their tags with an item of equipment, stating its location and whether it was situated at home or work. In

turn, each subject's tag data was imported into a single Excel spread sheet and then cross referenced to ascertain the respective item of equipment.

Figure 4-3 above shows the user form completed by subject 3 illustrating how they described their RFID tag placement, and Figure 4-4 illustrates a two minute extract from the same volunteers detected tag comma separated variable (CSV) data file showing the unique tag reference, the subject's number, date, time, the listen sequence number and the signal strength of the tag's transmission.

```
8A112711574C, 3, 11/03/11, 12:48:28, 2647, 31
8A112B11574C, 3, 11/03/11, 12:48:28, 2647, 19
8A112311574C, 3, 11/03/11, 12:48:28, 2647, 51
8A11DC11574C, 3, 11/03/11, 12:48:28, 2647, 23
8A11FA11574C, 3, 11/03/11, 12:48:28, 2647, 44
8A11D311574C, 3, 11/03/11, 12:48:28, 2647, 55
8A11FF11574C, 3, 11/03/11, 12:48:28, 2647, 59
8A112711574C, 3, 11/03/11, 12:49:28, 2648, 35
8A112B11574C, 3, 11/03/11, 12:49:28, 2648, 13
8A112311574C, 3, 11/03/11, 12:49:28, 2648, 51
8A11DC11574C, 3, 11/03/11, 12:49:28, 2648, 25
8A11FA11574C, 3, 11/03/11, 12:49:28, 2648, 45
8A11D311574C, 3, 11/03/11, 12:49:28, 2648, 57
8A11FF11574C, 3, 11/03/11, 12:49:28, 2648, 63
```

**Figure 4-4. Subject 3's tag data file sample showing tag id, user, date, time, sequence & strength**

From the tag data it is evident that during the two listens that have been shown (one at 12:48:28 and the second at 12:49:28) the same seven tags were detected on both occasions.

Tag Identity	Label	Owner	Location	Equipment	Type	Dumb/Intel
8A112711574C	50	2	W	Printer	D	D
8A112B11574C	62	2	W	PC other's	D	I
8A112311574C	54	2	W	PC	D	I
8A11DC11574C	41	3	M	Mobile	D	I
8A11FA11574C	15	3	M	Coat	O	D
8A11D311574C	38	3	M	Bag	O	D
8A11FF11574C	10	3	M	Laptop	D	I

**Table 4-1. The corresponding cross referenced detail**

Introducing the transcribed information from the user forms as shown above in Table 4-1 it is possible to decipher what is occurring. The location indicates that the equipment is situated at work (W) or is mobile (M) and not fixed in a single position, type specifies if the equipment is a device (D) or something else, other (O), and under the 'Dumb/Intel' column the equipment is categorised as being either intelligent (I) or dumb (D). In addition in a full dataset an item can

also be located at home (H) and have a type of 'I' indicating that it is regarded as infrastructure.

If the cross reference detail is applied to the data and noting that the tag data is recorded by subject 3 (as shown in Figure 4-4), it can be deduced that subject 3 had entered subject 2's office; user 2's PC, printer and 'PC other's' were detected, revealing the location of the meeting. User 3 was also close to their mobile phone, coat, bag and laptop. It could be conjectured that subject 3 was perhaps leaving for lunch or returning after it as the readings were taken at 12:48 and 12:49, carrying their personal belongings with them, and on the way they entered subject 2's office to speak to them. During this innocuous everyday occurrence it revealingly becomes apparent just how much information is available and currently going to waste.

Operating the PDA RFID readers constantly was battery intensive and so recharging was necessary to be undertaken twice a day; an extended overnight charge, and ad hoc periods during the day when subjects were at their desk and it was convenient to return the device to its charging cradle. However, upon return of the experiment equipment it rapidly became apparent that users had experienced problems in maintaining charge because within the captured data blocks of time were absent and corresponding data missing. Despite this 1,576,340 separate tag readings were captured at an average of 78,817 per subject, with a standard deviation of 33,430.64. As such 100% of the reading sizes are within three standard deviations of the mean, indicating that the data is indicative of a normal distribution, and more that one and half million samples are easily sufficient to have significance and provide meaningful analysis. Table 4-2 below lists the number of observed tags identified during the experiment for each of the twenty participants.

Subject	Readings	Subject	Readings
1	43,540	11	95,970
2	117,054	12	31,097
3	105,087	13	104,029
4	12,805	14	90,109
5	45,453	15	95,203
6	121,256	16	49,587
7	37,970	17	82,147
8	122,484	18	91,665
9	119,057	19	88,554
10	66,773	20	56,500

**Table 4-2. Quantities of recorded readings for each of the twenty experiment participants**

It is evident from the data tabulated above that there is a large variation in the quantity of recordings made with user 4 (only 12,805 observations) performing particularly poorly and subjects 1, 5, 7 and 12 also recording comparatively few. Anecdotally user 4 reported afterwards that during the fortnight's experiment they had suffered illness and been confined to bed for a number of days which impacted upon their participation in the experiment. The following section undertakes analysis of the data for individuals and the subject group as a whole.

### 4.2.3 Data Analysis

It is firstly important to note that upon initial investigation the recorded data between midnight and 6am remained consistent and unwavering. During this time, it was evident that users had understandably replaced their PDA on its respective cradle to be charged and so it remained in a static location repeatedly observing the same tags located in the near vicinity. This data was deemed to be insignificant in terms of investigating the Aura concept and was consequently ignored during analysis. This resulted in a 22.527% reduction in the observed dataset size, lowering it to 1,221,243 readings.

Additionally because of the persistently large volume of data involved and the need to plot and review the findings graphically, the granularity of the images that follow have been reduced to either fifteen minute periods rather than each individual minute. For each hour four datum points will be drawn instead of the full sixty, increasing clarity and enabling inferences to be made. Also, removing the data that occurred between 6am and midnight resulted in the horizontal axis only representing 18 hours rather than a full 24, further aiding clarity and interpretation.

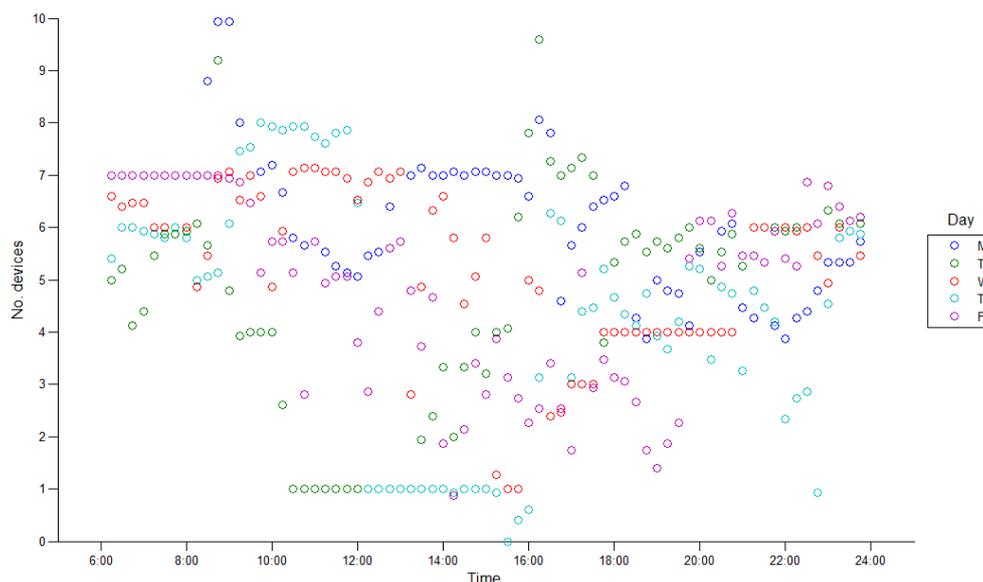
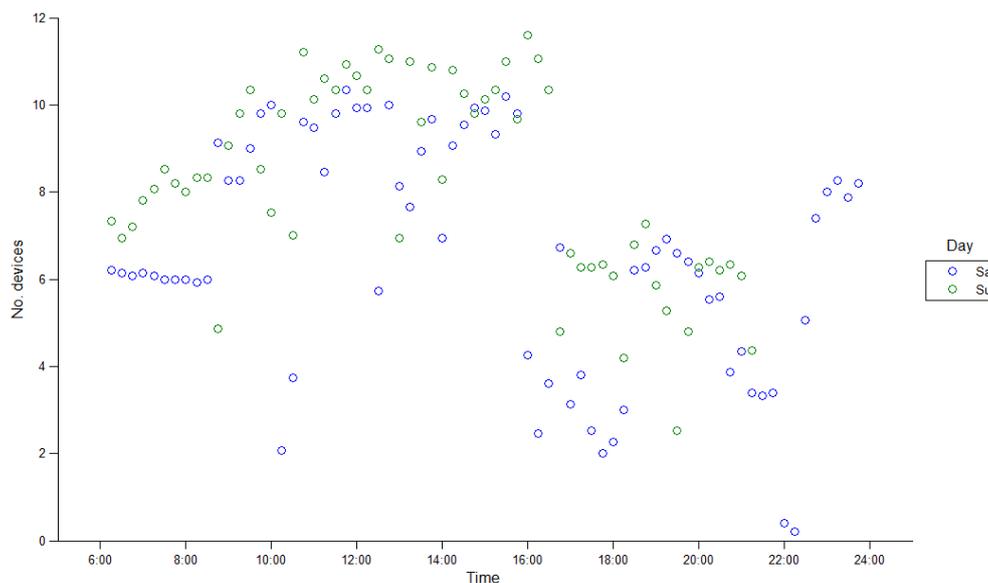


Figure 4-5. A typical subject's weekday observations

Figure 4-5 illustrates the number of unique devices observed by an individual during a working week (Monday-Friday). Each day is plotted as a separate set of readings with individual data points representing the average number of detected devices within a fifteen minute period plotted against the time of day that the observation was made. In comparison Figure 4-6 illustrates the weekend tag data for the same user.

Examining the plots in unison it is evident that the weekday diagram exhibits a maximum average of ten devices being detected in any given observational period whilst at the weekend this figure peaks at twelve, suggesting that more static tags were located at home rather than at work. However, with such a high number of observations being recorded at both home and work it is apparent that the majority of tags were placed on portable possessions that the subject carried with them throughout the day. During the workdays there appears a high degree of variation in the number of observed devices implying that this subject is active during their employment and even spends time out of the office. Time away from their usual location can be perceived from the data on Tuesday and Thursday between 10am and 4pm where the average falls to a single unit.



**Figure 4-6. The same typical user's weekend observations**

It is also possible to observe from the weekend data that a greater number of devices are detected through the morning and up until 4pm. After 4pm the quantity drops suggesting that the subject was away from home or at least changing their location, without porting some of their personal devices with them. Whatever the movement of the user or the day that is observed, it is clearly apparent that a significant quantity of devices are consistently detected throughout; the subject is consistently within close proximity of contributable possessions.

If subject 14 is examined in isolation because they had a near median number of total detections, and the data is grouped into 30 minute sections, the average number of devices found during each listening window throughout their experiment participation is shown below in Table 4-3.

Viewing the data in this way immediately highlights the completeness of the data for this average user, with the empty data cells illustrating periods of down time or time out of reach of any personal devices. The highest average number of devices found was 15.67 and was recorded on the second Tuesday of the experiment for the half hour from 13:30 until 14:00. The data also indicates that when devices are found they are seldom in isolation, the lowest average number is 1.2 and was recorded in the period running up to midnight on the second Monday but only a total of 14 of the observations shown have an average less than 2.0. Examination of the summary data indicates that during this period the PDA performed 12,470 listens with only 269 of these failing to identify any devices, a success rate of 97.84%. Extending this one stage further reveals that only 167 attempts detected a lone device, just 1.34% of the total observations.

Time	W	Th	F	Sa	Su	M	Tu	W	Th	F	Sa	Su	M	Tu	W
06:00			5.20	4.00			3.93	3.57	3.23	2.73		4.47	2.77	1.97	1.37
06:30			7.23	4.00			3.77	3.70	3.47	2.87		4.67	2.80	2.10	1.40
07:00			7.00	4.00			3.83	3.93	3.70	4.60		4.27	2.90	2.93	1.43
07:30			7.13	4.00			3.87	4.33	4.17	4.83	3.21	4.23	2.33	3.13	1.87
08:00			5.55	4.17		13.00	6.64	4.58	6.13	8.67	3.77	4.33	4.64	3.36	2.67
08:30			2.00	4.07		10.47	13.30	10.90	6.53	4.03	3.87		3.33	11.33	5.26
09:00	7.50			4.37		14.03	13.90	8.60	3.00	2.00	3.63		10.57	13.53	9.53
09:30	9.00			5.20		12.10	13.97	8.13	2.56	1.80	3.50		13.17	13.33	11.77
10:00	12.70			5.40		12.90	14.23	7.47	1.97	2.00	3.43		12.83	11.83	12.77
10:30	11.62			5.37		13.23	13.17	8.40	1.87	2.00	3.83		12.93	11.70	13.00
11:00	10.88			5.47		6.36	13.43	6.47	1.87	2.00	4.57		12.73	12.03	13.07
11:30	12.30			5.57		14.37	15.60	8.43	1.93	2.00	4.03	3.20	12.53	13.47	13.13
12:00	10.03			5.23		12.13	15.10	9.73	2.00	2.00	4.17	3.45	13.17	13.77	13.17
12:30	8.60			5.27		12.00	13.37	10.57	2.00	2.00	4.20	3.17	12.33	14.07	13.43
13:00	5.00			5.50		13.00	4.50	8.30	2.00	2.00	4.17	3.23	13.87	14.70	12.77
13:30	9.58			5.47	6.62	12.93	3.00	7.97	2.00	1.97	4.13	3.43	13.57	15.67	12.73
14:00	12.90			5.30	3.93	13.67	8.55	11.70	2.00	2.00		2.93	12.80	14.07	12.97
14:30	10.77			5.50	4.33	13.13	11.30	9.43	2.00	1.93		3.20	11.83	14.37	12.50
15:00	11.52			5.37	4.63	13.53	12.13	13.10	2.00	2.00		4.23	12.33	14.83	13.00
15:30	13.10			5.40	4.47	14.17	11.70	13.63	2.00	2.07		3.90	12.10	14.60	
16:00	13.07			5.17	4.53	12.93	11.37	11.67	1.93	3.00		4.40	13.60	14.83	
16:30	11.40			5.37	4.17	13.13	12.10	13.03	2.00	3.00		3.83	14.03	13.53	
17:00	8.53			5.43	4.03	10.80	3.77	12.08	4.21	4.76		3.43	10.80	10.03	
17:30	2.87		5.00	5.27	4.17	6.37	2.00	5.07	4.23	5.40		3.90	2.44		
18:00	7.67		3.80	5.30	3.80	5.00	4.83	4.17	3.03	5.37		4.00	3.87	3.03	
18:30	6.53		3.37	5.30	3.87	5.00	5.07	4.00	3.13	5.50		3.57	3.67	3.47	
19:00	6.03		3.43	6.90	3.47	4.97	5.97	3.93	3.13	5.57		3.13	3.93	3.07	
19:30	5.67		3.50	6.70	3.50	4.83	6.13	3.40	3.07	5.43		2.90	4.03	2.97	
20:00	4.07		3.83	6.37	3.43	4.97	5.50	3.70	3.00	5.00		2.80	4.03	2.90	
20:30	3.45		4.27	6.13	3.93	5.17	5.33	3.90	3.03	5.23		2.87	3.90	2.40	
21:00	3.13	6.75	3.80	6.33	4.07	5.07	5.30	3.97	3.13	4.23		2.93	3.93	2.27	
21:30	3.63	5.40	3.87	6.00	5.43	4.87	5.57	4.00	3.87	3.70		2.77	3.23	2.43	
22:00	3.77	5.07	3.97	5.67	4.13	4.97	5.57	3.60	3.97	3.73		2.60	3.87	2.60	
22:30	2.13	5.13	4.03	5.73	2.31	5.00	5.67	3.47	3.87	3.57		2.83	2.17	2.97	
23:00	2.30	4.97	4.00	6.20	2.40	5.00	5.63	3.27	3.87	3.67		3.77	2.33	3.33	
23:30	2.13	4.93	4.00	4.17	2.13	4.07	4.13	3.37	3.90	3.83		4.10	1.20	2.83	

Table 4-3. Subject 14's average number of detections in each half hour period

If the data from all the experimental groups is combined, these two figures can be compared against the experimental average as a whole; Table 4-4 shows the number of detected devices for each listen when the experiment data (post 6am) is combined for each group of subjects. Furthermore Figure 4-7 illustrates this in graphical form and from this it can be seen that no devices were detected on 2.36% of occasions and a single device on 9.96%. These figures are higher than those experienced by user 14 although it still supports the hypothesis and indicates that elements of an individual’s Aura were detected on the majority of attempts.

Number of devices detected	Experiment group				Total detections
	1-5	6-10	11-15	16-20	
0	1,171	2,591	1,686	558	6,006
1	7,018	3,663	4,243	10,413	25,337
2	7,167	6,832	6,957	12,381	33,337
3	6,808	3,744	9,812	15,878	36,242
4	5,783	4,189	8,046	10,844	28,862
5	4,703	4,354	7,470	9,535	26,062
6	7,756	7,337	6,946	5,977	28,016
7	6,616	9,852	4,514	2,339	23,321
8	3,416	10,251	2,930	4,590	21,187
9	1,766	7,155	1,138	220	10,279
10	1,061	1,490	1,177	3,525	7,253
11	834	7	1,367	36	2,244
12	149		1,658	8	1,815
13	34		1,897	2	1,933
14			1,313	12	1,325
15	1		784	2	787
16			312		312
17			81		81
18			24		24
					254,423

Table 4-4. Number of detected devices on each listen, combined into experiment groups

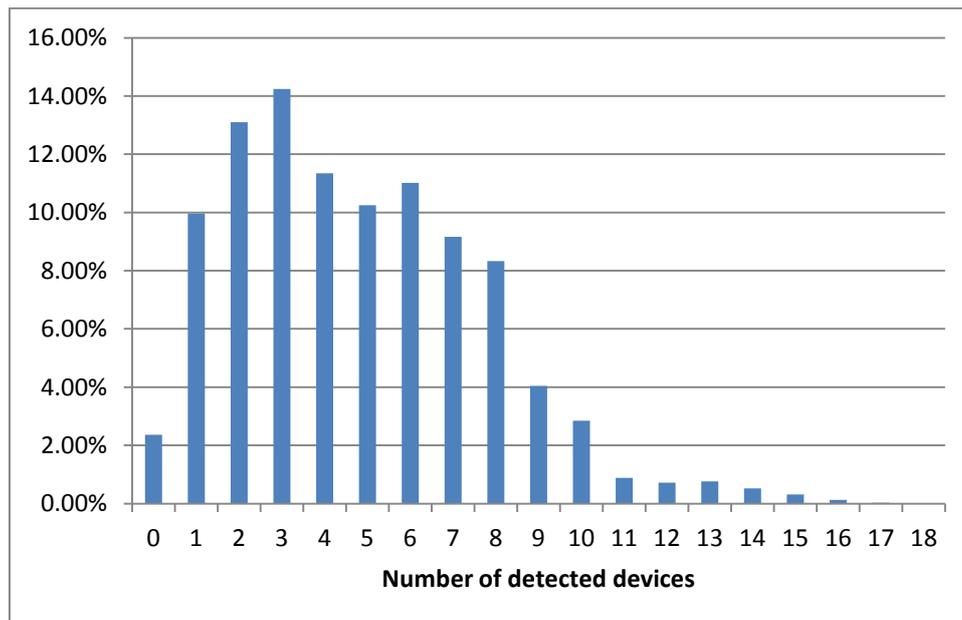
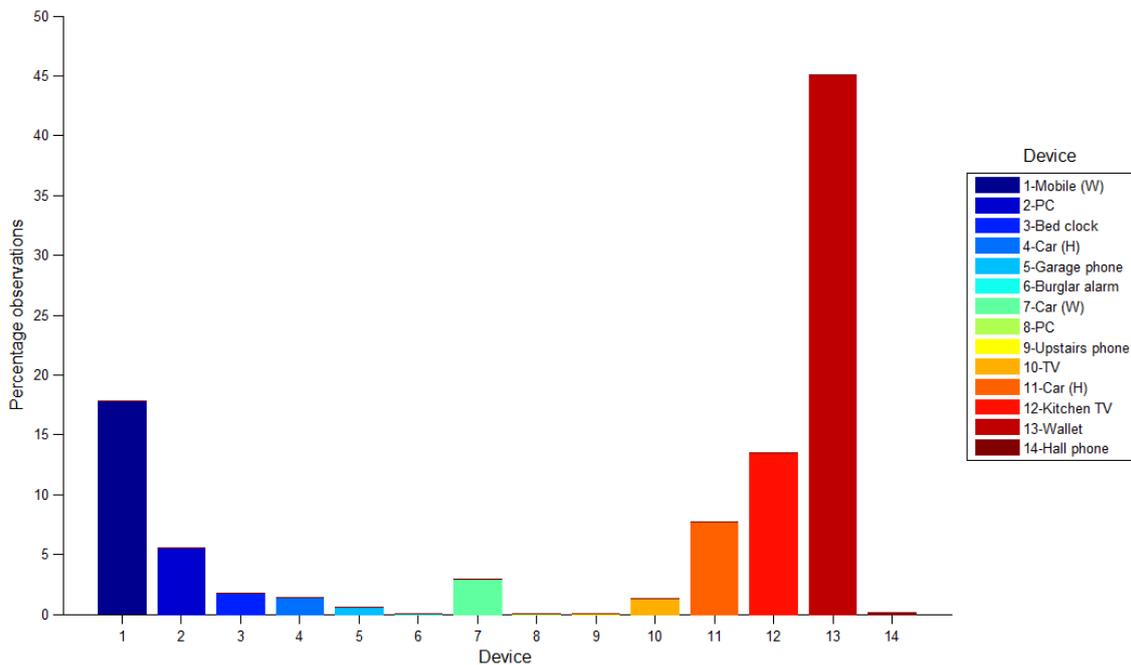


Figure 4-7. Number of detected devices as a percentage of total listens for all participants

It is vital to also understand the types of device that are being detected in addition to just the quantities. Examining a single user in isolation the breakdown of their device detections reveals the distribution shown in Figure 4-8 below. This indicates the percentage of observations that recorded each of their fifteen RFID tags, cross-referenced to identify the specific devices or items of equipment. Clearly from this histogram, there is one personal item that was detected far more often than any other. The subject's wallet was observed during approximately 45% of all recordings executed during the two week experiment in comparison to their burglar alarm, PC, upstairs phone and hall phone, all of which were detected far less than 1% of the time.



**Figure 4-8. A single user's specific device observations during the experiment**

It is therefore imperative to compare the rate at which inert devices or personal items are detected as opposed to intelligent ones. For the same user, by plotting days' observations in isolation (Figure 4-9 and Figure 4-10) it is possible to visually examine more clearly how the user's routine affects the number and type of devices that are detected. These diagrams illustrate the continuity of presence for each possession or item of equipment across the day in ten minute periods, when contact is established and when it is lost. Additionally, other users' devices (Other devices) and infrastructure are also shown indicating when they are also detected. Intuitively, these foreign device contacts only appear on the weekday plot (Figure 4-9) because the other members of the experimental group were all work colleagues.

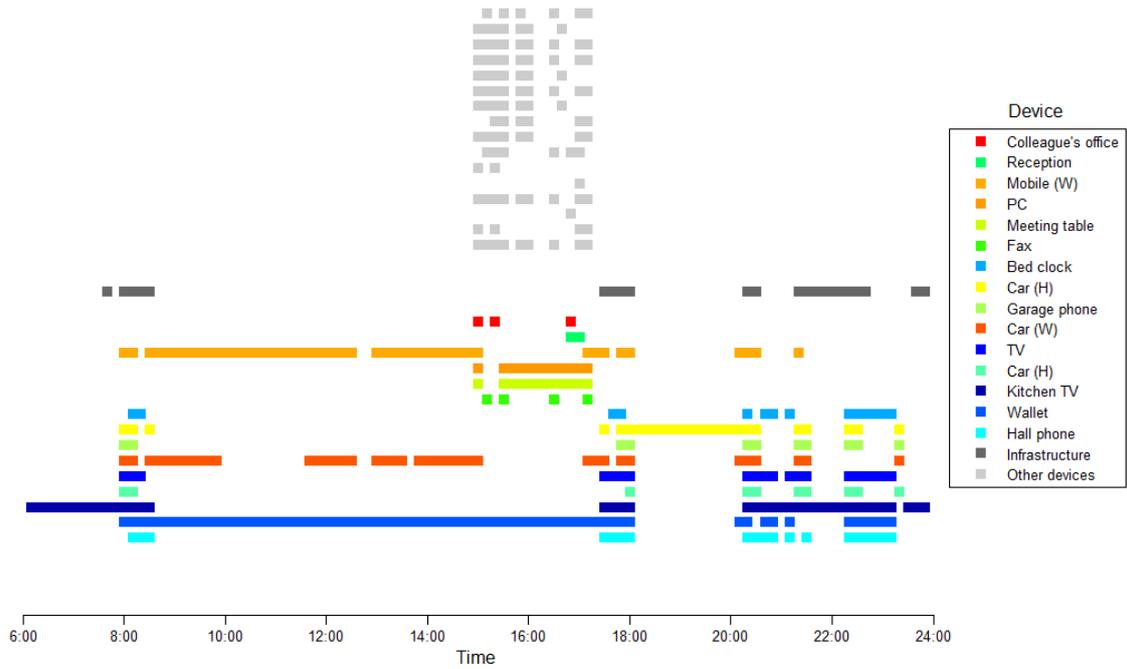


Figure 4-9. A user's isolated single weekday activity

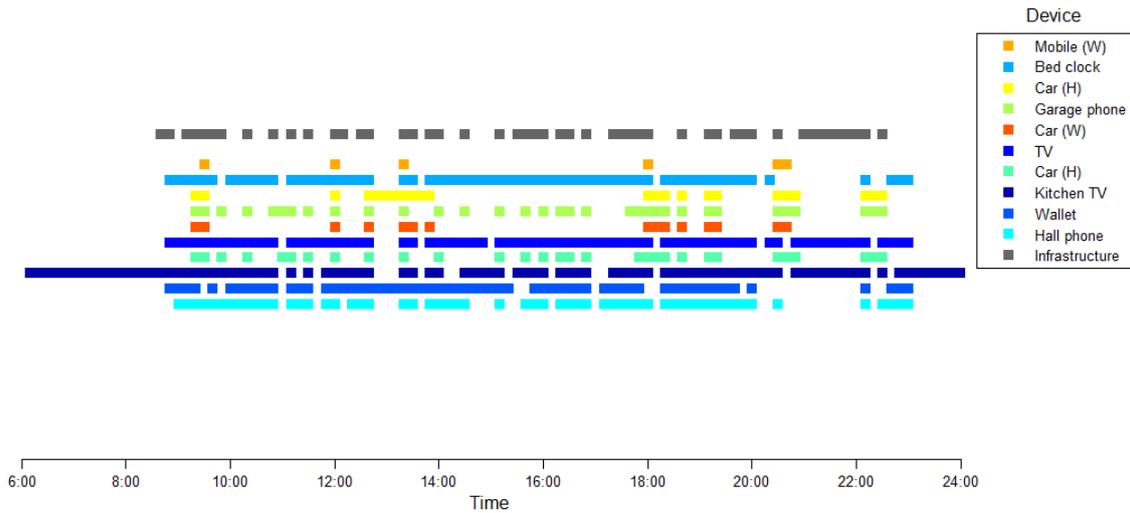
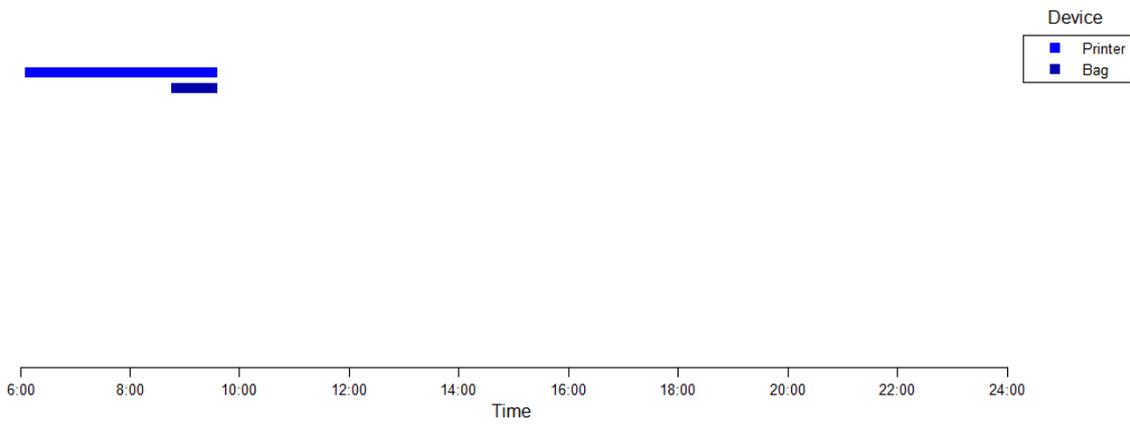


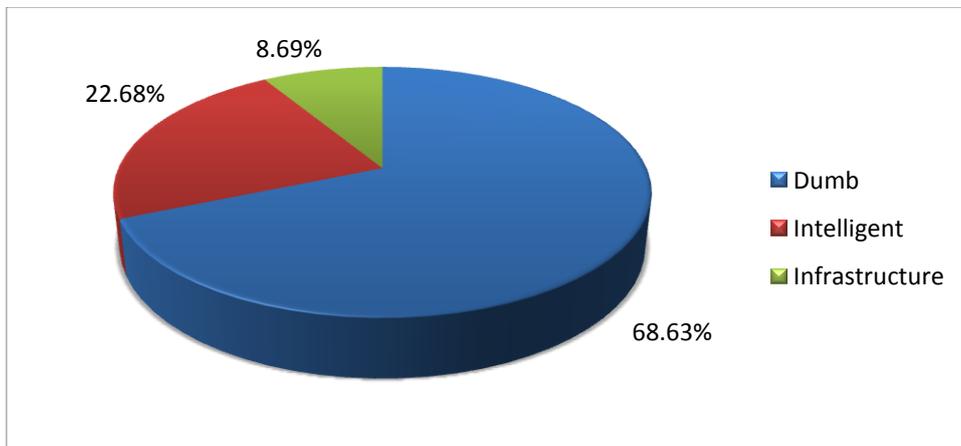
Figure 4-10. The same user's isolated single weekend day activity

Illustrating the earlier discussion, in both examples nearly the entire observation window from 6am to 12pm has at least one device within detection range at any given moment. Indeed, closer examination appears to suggest that the inert devices are present most consistently throughout the day, supporting the potential for leverage. Indeed within the entire dataset coats, work bags and hand bags all topped the frequency chart for particular participants.



**Figure 4-11. Daily activity for a poor performing experiment subject**

The diagrams presented above have been selected to indicate a good spread of devices throughout the day where the user did not run into any experimental difficulties. Compare these figures above with a user who did not manage to fulfil the criteria and ran into problems as shown above in Figure 4-11. It is immediately evident that the lack of captured data is meaningless in terms of the experiment analysis, although it does serve to remind that these anomalies should be expected. A full set of these charts are available on the data disc included with this thesis as indexed in Appendix F.



**Figure 4-12. Percentage share of each category of detected items**

One of the most important elements of the experimental observations to be considered is Wi-Fi infrastructure such as public hot spots, work and home access points. As people move throughout their daily routine it is one of the main factors that could be utilised to establish location, being unseen and static there is a real potential to leverage the information it provides. If the number of infrastructure detections is examined it superficially appears that only 8.69% of detections fell into this category as shown in Figure 4-12. However on further consideration and analysis this figure is misleading.

Subject	Infrastructure detected	Subject	Infrastructure detected
1	47.70%	11	23.61%
2	42.98%	12	62.19%
3	70.40%	13	26.71%
4	12.06%	14	28.16%
5	0.55%	15	58.04%
6	60.93%	16	31.20%
7	3.19%	17	59.91%
8	8.61%	18	9.32%
9	70.94%	19	3.99%
10	4.28%	20	30.75%

**Table 4-5. Percentage of infrastructure detections by subject**

The volunteers who partook in the experiment all decided to place the majority of their tags on dumb and intelligent devices rather than infrastructure, the most items of infrastructure that anyone chose was two. Consequently it is expected that infrastructure will constitute a minimal share of the total number of readings. A far more indicative statistic is to examine what percentage of readings encountered at least one item of infrastructure; analysis discovered that 35.24% of all captured data met this criteria. However, viewing the subject-by-subject results as shown in Table 4-5 it is clear there are significant fluctuations in the observations with the highest detection rate experienced by subject 3 when during their participation they detected infrastructure on 70.40% of their reads but in contrast user 5 only achieved 0.55%. This further analysis certainly suggests that infrastructure detection can contribute significantly to an individual's Aura.

Figure 4-12 also indicates the observed relationship between intelligent and dumb devices, with the computationally incapable items being detected three times as often as their sophisticated counterparts. This bias is fundamentally reflective of everyday life; people have a tendency to carry more inert items than intelligent ones. Although several intelligent devices are carried and used, items such as wallets and handbags are kept close by their owners and ported throughout the day. All experiment subjects tagged more of these than the high value items leading to the 69%:23% disparity.

If the type of detected device is examined further and the occasions when only one category is identified as shown in Table 4-6, it is apparent that only dumb devices were detected on 25.07% of occasions, only intelligent on 1.51% and only infrastructure 0.09% of the time. Once again though, these

figures are slightly misleading with three subjects observing only dumb devices more than 70% of the time. All volunteers detected just a single type at least once with user eighteen the lowest overall figures recording 1.12%, 2.45% and 0.00% for the three device types respectively. Fourteen subjects experienced no infrastructure only listens but only one, user ten, no dumb only reads.

Subject	Dumb	Int.	Inf.	Subject	Dumb	Int.	Inf.
1	30.16%	0.75%	0.00%	11	74.63%	0.00%	0.00%
2	1.74%	2.24%	0.00%	12	36.27%	0.00%	0.00%
3	3.06%	2.02%	0.14%	13	7.47%	0.35%	0.00%
4	61.81%	0.00%	0.00%	14	70.47%	0.00%	0.00%
5	3.96%	2.46%	0.00%	15	13.42%	1.91%	0.00%
6	8.10%	0.07%	0.20%	16	66.28%	0.00%	0.00%
7	71.90%	0.00%	0.64%	17	40.09%	0.00%	0.00%
8	10.61%	0.00%	0.30%	18	1.12%	2.45%	0.00%
9	10.75%	0.07%	0.40%	19	32.15%	0.00%	0.00%
10	0.00%	4.51%	0.35%	20	0.38%	11.45%	0.00%

**Table 4-6. Percentage of dumb, intelligent and infrastructure items when only a single one identified**

Extending this analysis to the next stage, when the data is examined to ascertain on what percentage of reads a mixed sample of device was encountered (that is at least two of the three types during any single listening period) the results shown in Table 4-7 below are produced.

Subject	Mixed detections	Subject	Mixed detections
1	69.09%	11	25.37%
2	96.02%	12	63.73%
3	94.78%	13	92.18%
4	38.19%	14	29.53%
5	93.58%	15	84.67%
6	91.63%	16	33.72%
7	27.46%	17	59.91%
8	91.84%	18	96.43%
9	88.78%	19	67.85%
10	95.14%	20	88.17%

**Table 4-7. Percentage of mixed types of detections by subject**

These results indicate that overall mixed types of device are encountered on 73.48% of all reads with subject eighteen experiencing the highest result of 96.43%, whilst user eleven contrasted this with only 25.37% of occasions.

The following section reflects upon these results and then establishes the basis for the next tranche of work.

#### **4.2.4 Discussion**

The preceding section examined the gathered data to establish the quantity and frequency that owned and known items were within detectable range during everyday life. Although some of the data was lacking in volume because of difficulties experienced by some volunteers, the outcome from the experiment has to be regarded as a success. The devices appear to have operated successfully and although anecdotally some users reported the experiment as a little restricting, none found it burdensome to the point where they abandoned participation. All have provided data that is contributory to the research and supportive of the project as a whole.

When analysed the quantities of recordings lay within the parameters indicative of a normal distribution with 100% of the data falling within three standard deviations of the mean. The saturation of observations certainly indicates that one or more objects were identified for the majority of individuals' waking hours, being detected on 97.84% of all attempts with infrastructure being found on 35.24% of occasions. 73.48% of all attempts detected a mixed range of items identifying at least two of the three categories; dumb, intelligent and infrastructure.

With two or more devices being detected on 87.68% of occasions the results certainly lead to the acceptance of the experimental hypothesis that significant numbers of devices are encountered to enable the Aura concept to function. Furthermore, it is certainly clear that an individual's Aura of devices could be built from a consistently diverse range of items.

The experiment was designed to additionally establish the relationship between dumb and intelligent items. It became apparent that inert items and possessions were observed more than three times as often as intelligent ones, with dumb devices being detected on 68.63% of all occasions. This significant figure suggests that these superficially lesser objects can contribute hugely if a means to incorporate them into an individual's Aura is found. If several items are consistently within detectable range at any given moment, it should be possible to use these to identify an individual. Couple this with the ability to recognise familiar locations and already it appears as if the basis for an adaptive response may be possible.

The plotted activity charts for weekdays and weekends further supported this theory, illustrating how the movement of an individual throughout the day results in a changing profile of detected items. Time spent at home and work could easily be distinguished in addition to visibly underlining the saturation of device detection. From these charts it was also possible to

identify how one user could also leverage the presence of someone else's devices. When time was spent in communal areas other subject's equipment was identified on a regular basis, suggesting that if harnessed this might further support locational information or strengthen the user's Aura.

In summary the experiment and analysis of the gathered data suggests that the concept of Aura is valid and provides reassurance of identity. The following section will build on this premise and outline how an individual's Aura can be used to build and adaptive and cooperative approach to authentication.

### ***4.3 Conclusion***

So far this chapter has defined an individual's Aura and how the undertaken experiment has confirmed its existence and quantified the diversity of the devices contained within. It has also demonstrated how people exist within their Aura during everyday life and how its profile adapts to change of location and contact with work colleagues or family members. This section will outline how this detail can be leveraged in the search for a novel approach to user authentication.

The concept of an Authentication Aura is two-phase. The first phase is designed to counteract the accepted fragility of Boolean point-of-entry security that once passed gives the user unfettered and consistent access to all applications, data and services that lie within the device being secured. Currently when a user successfully authenticates on a device the confidence that is established in the user's identity is 100% and remains so for the duration of their usage session. The concept aims to improve upon this by utilising a continuous authentication scheme that sets confidence in the user's identity based upon authentication method used, elapsed time and location.

The second phase of the Authentication Aura leverages the confidence gained from the surrounding Aura and associated devices. As established earlier, the user's Aura contains intelligent devices that are capable of calculating and maintaining their own Aura confidence level. Enabling them to communicate their current status will permit the host device to incorporate this confidence value into its own confidence assessment. Additionally, the regular presence of inert items and possessions is evident from the analysis that has been undertaken. These items can therefore also contribute towards the confidence calculation by incorporating them as tokens; the more there are, the more confident the host device should be that authenticated identity has not changed.

In summary an Authentication Aura is a cooperative and adaptive approach to mobile security that utilises surrounding possessions, devices and infrastructure to enhance user identity confidence against which apps and services with preset thresholds can either have activation and use permitted or denied.

There is one further requirement for the Authentication Aura to fulfil. It was observed earlier in this document how users carrying multiple electronic devices currently have the repeated arduous requirement to authenticate on each device during activation. If upon activation the Authentication Aura immediately polls the surrounding Aura and the confidence gained is sufficiently high it will be possible to remove the need for the user to authenticate. Immediate access to the device can be gained without the usual associated inconvenience.

Having now established the overarching concept of an Authentication Aura and the interesting potential it harbours the next chapter expands upon the ideology outlined above and examines in detail the elements that will be required to implement this novel approach to security on mobile devices.

---

## **Chapter 5**

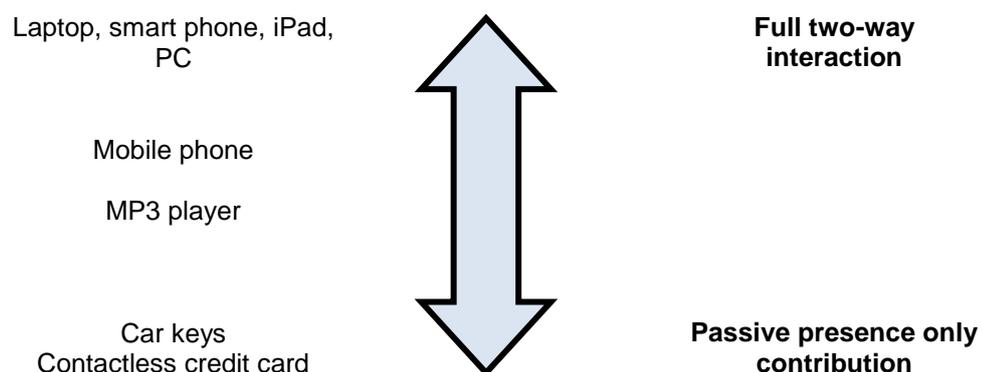
# **Elements of an Authentication Aura**

---

## 5. Elements of an Authentication Aura

---

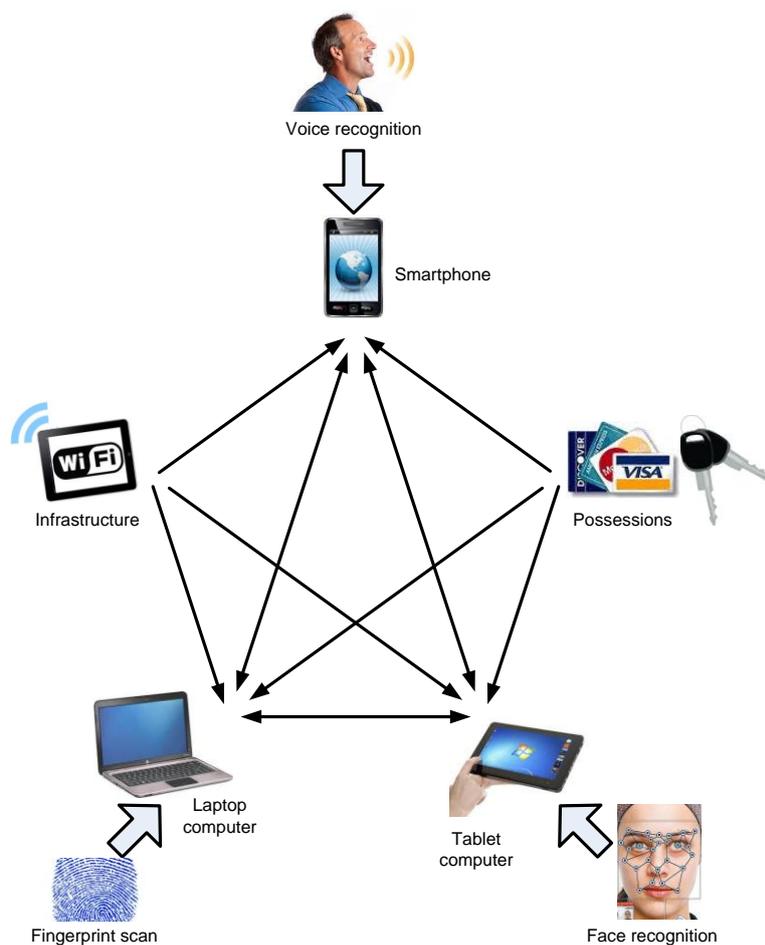
In current systems, each authentication measurement is treated as discrete and independent, and users may have to remember a variety of information and/or carry a variety of physical tokens with them in order to achieve authentication in different contexts (Tanvi et al., 2011). When considered from a holistic perspective, this can clearly be seen to be inconvenient, and potentially over-complex. The Authentication Aura introduced in the previous chapter proposes a distributed approach that can improve the situation by bringing together a range of authentication methods (e.g. based upon secret knowledge, physical tokens, and biometrics) that can operate across multiple devices and services within a user's personal area, their Aura. The intention is not to simply achieve a single sign-on, whereby authentication to one device automatically authenticates the user to all others for an unlimited period. Instead, by intelligently combining authentication measures from the different devices and techniques used within this network, the concept of an Authentication Aura can be established. When access to a new device or service is requested, the strength of the user's Aura will determine whether they will be granted access automatically, or be required to perform an explicit authentication. This strength will vary depending upon when the user last performed an authentication, and with which technique it was achieved (e.g. a measure obtained from a physiological biometric could well be weighted higher than that from a password) (AuthenticationWorld.com, 2006; Clarke and Furnell, 2007). This distributed and collaborative environment seeks to improve the level of authentication security and improve the convenience for users.



**Figure 5-1. Varying levels of device sophistication and consequent contribution to the Aura**

From the strength of the experiment results outlined in the previous chapter it indicates that the Authentication Aura should use intelligent, dumb devices and even innocuous possessions to contribute to the Aura and its function as shown in Figure 5-1. Intelligent devices are those

that have computational capabilities and able to interact with the user and one another, whilst dumb or inert possessions are those that do not currently possess this ability. For some intelligent devices it might be possible to undertake continuous authentication (such as voice recognition during telephone calls) to provide frequently reconfirmed identity details and a valuable confidence contribution, whilst others might simply act as tokens, their physical presence at a location being the only information of use. Figure 5-2 illustrates how the information might then be relayed amongst a group of commonly owned devices and where relevant, some of the authentication techniques that could be employed. Note that the three intelligent devices receive and provide information, whereas the possessions and infrastructure only act as providers.



**Figure 5-2. The potential inter-device relationship and authentication techniques**

This chapter builds upon this proposed concept of an Authentication Aura by examining in detail the elements required to implement this novel form of mobile device security, discussing the strengths and weaknesses of each and how practical the respective element of the approach is. It then concludes by summarising the findings and discussing the feasibility of implementation.

## **5.1 Inter-Device Trust**

One of the fundamental principles of an Authentication Aura is its ability to draw information from surrounding devices and infrastructure. To achieve this, a communication channel will have to be established and opened during operation, allowing information to be received and transmitted. With data being communicated between devices consideration needs to be given to trust and whether or not it has to be established prior to invoking the Authentication Aura or if trust can be learned by the participating items with suitable intelligence.

Superficially the latter option appears more desirable because no initial enrolment or human intervention would need to be undertaken, each device would autonomously learn. In this scenario however, to initially relay confidence between devices without trust would be meaningless. For instance, if device A authenticates person X and transmits this to device B which it has detected as being in near proximity, device B is now aware that device A is confident in the identity of its own user but does not possess intrinsic trust and knowledge of device A. Without prior trust and knowledge there are no means by which the devices can be assured that the identity of their own users is the same - they may simply be communicating with an item owned by an entirely different person who just happens to be nearby. It could be suggested that upon receipt of such knowledge from a nearby device, the user could be obtrusively informed of the receipt and polled to ascertain if the communicating equipment should be trusted. The counter argument is that this approach opens up the Authentication Aura to spoof communication and the potential for users to unwittingly accept communication from illicit devices by mistake. It is therefore clear that trust must be established between devices within the Aura as part of the initiation requirement.

An enrolment process similar to Bluetooth pairing will be necessary to distribute inter-device awareness and the relevant information to enable common identity of individuals to be undertaken. Once a new device has been introduced to an established piece of equipment, the knowledge of the established entity could be automatically shared and transposed onto the new arrival which in effect would limit the entire introduction process to a single action, reducing the burden for the user.

## **5.2 Functional Requirements**

There are a number of criteria that a functioning Authentication Aura will have to meet should any implementation be deemed a success. These requirements provide an understanding of the Authentication Aura's aims, what it will achieve and some of the expectations that a user will have. This section introduces these benchmarks and describes the rationale behind each one.

### 5.2.1 Non-intrusive

One of the key motivations for this research was the repeated intrusive nature of current authentication implementations which is exacerbated by individual's possessing multiple devices. Thus during the process of authentication and operation it is imperative that minimal intrusion is made upon the individual because safeguarding the user experience and quality of service is of primary importance (Ngoc, 2007). It is important to avoid asking direct questions of the user and prompting for responses which will impinge upon the flow of work being undertaken on the device at the time. As far as possible the techniques employed must operate imperceptibly in the background during normal situations and will only become visible if an authentication by the user is absolutely necessary and cannot be undertaken in any other way.

An obvious candidate to meet these criteria is non-intrusive biometric authentication which can be performed invisibly and continuously in the background whilst the user continues to interact with the device. With service access being restricted as confidence in the user's identity is eroded it can be implemented as required to re-establish maximum confidence. Intuitively the ability to invoke such an approach is dependent upon the target device and its capability to perform the necessary processing and data capture. Smart phones, tablets and laptops would clearly be able to meet this requirement utilising methods such as voice and facial recognition or even keystroke dynamics.

Standard	Description
ISO/IEC 24713-1:2008	Information technology -- Biometric profiles for interoperability and data interchange -- Part 1: Overview of biometric systems and biometric profiles
ISO/IEC 29164:2011	Information technology -- Biometrics -- Embedded BioAPI
ISO/IEC 29109-5:2014	Information technology -- Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 -- Part 5: Face image data

Source: ISO (nd)

**Table 5-1. The key ISO Biometric standards defined by ISO committee SC37**

To future proof the system and leverage the most advantage from new and emerging technology a universal and adaptive interface will be required that complies with the key ISO standards (ISO, nd) as shown above in Table 5-1 but will also be able to use less sophisticated traditional methods. This will provide a fully inclusive Authentication Aura that can utilise the greatest diversity of devices, ensuring the most benefit is gained from their presence.

### 5.2.2 Flexible metrics

The premise of the Authentication Aura is to protect the host device and the services it contains, whilst leveraging maximum advantage from familiar surroundings, devices and possessions alike. The experiment findings supported the inclusion of a wide and varied range of devices. To achieve this, parameterisation will facilitate an adaptive approach that incorporates this diversity at the lowest level but where appropriate has the scale to concurrently underpin sophisticated items.

The Authentication Aura will incorporate parameterisation at its core providing the ability to adjust settings and influence the way in which it operates. However, it is important that as default the system is set with restrictive parameters to implement strict initial security, protecting the device to a high degree without the need for user intervention. Any user should only consider making adjustments when they become comfortable with the concept and confident in their understanding of the influence of the parameters.

To maintain adaptability it is necessary to impart the Authentication Aura with the facility to restrict service access and application use on an item-by-item basis. At any given moment the Authentication Aura will possess a user identity confidence rating and restricting service and application access based on this rating will yield the desired control. Parameterising these access thresholds will enable bespoke control to be maintained and provide the required level of flexibility.

With devices in the Aura having varying perceived degrees of significance the flexibility to reflect this is also required. Introducing a ranking system that will enable a weighting to be assigned to a device will once again allow a common approach to cope with the diversity of equipment. Assigning a parameterised level to a device will then allow the system to adapt and deal with items on an individual basis.

Location of the user at any given time is also a key influence upon the Aura's performance. As discussed earlier the risk associated with locations is correlated with the familiarity of those surroundings and the perceived threat associated with being there. Flexibility can be introduced by assigning weightings to categories of location and then linking these to known static devices or infrastructure. This will equip the Authentication Aura with the ability to recognise where it is and under what level of response it should function.

With all the metrics listed above those that are deemed to be of a lesser threat or influence will be given a lower weighting, and those that are considered more of a threat and sensitive will conversely receive a higher factoring. Potentially these can be adjusted by the user although any user burden must be minimised which is achievable via the use of a strong set of

default values. If these rankings are then incorporated into the calculation of user identity confidence (see section 5.5) it will provide the owner with the ability to influence operation and adapt functionality.

### **5.2.3 Rigorous authentication**

The employed solution should operate with strict rigour when authenticating an individual and immediately reject detected impersonation whilst minimising false acceptance and rejection rates. As outlined in section 5.2.1 this will vary from device to device and the corresponding available methods of authentication. If a choice exists, the Authentication Aura should always invoke the strongest form of authentication available, not only to secure the host device but also as a contribution to the Aura as a whole. It must be the responsibility of any partaking device to add as much as possible to the collective, ensuring that all devices concurrently maintain the highest level of user identity confidence.

Different techniques will be allocated varying starting percentages of confidence meaning that when a user authenticates the Authentication Aura will not automatically set the identity confidence to 100% but to the parameterised level instead. Techniques such as iris or retina scanning will intuitively be allocated a very high percentage (if not 100%) because of their proven strength, whilst PIN authentication might only be given a 70% initial value. This will provide a mechanism through which the user can adjust the contribution to the Aura that a method makes and how it will effect ensuing confidence calculations.

Utilising parameterisation of authentication percentages and rank of authentication methods will yield the necessary information to meet these requirements further supporting the need for flexibility.

### **5.2.4 Supports multiple identities**

Multiple identities will need to be supported by the employed framework across a number of different platforms (Ngoc, 2007). With devices being shared amongst family, friends and work colleagues the ability to manage these with minimal intrusion is paramount. As an individual picks up and uses a device it is imperative that the Authentication Aura does not assume identity and immediately open itself up for use if suitable confidence can be gained from the local environment. Auras are not mutually exclusive with common devices likely to appear in more than one, especially in the home environment, and so without safeguards unwarranted access could be permitted by incorrect identification.

However, the Authentication Aura must allow a new user to create a profile and introduce devices personal to them once access to the device has been gained via standard authentication, and beyond this manage the multiple identities. Upon activation it will be

necessary to simultaneously assess multiple Auras to gauge if numerous matches exist and further more rigorous checks need to be made to ensure accurate identification is maintained.

### ***5.3 Influence of Location***

Location has a major influence and indeed is one of the cornerstones of the Authentication Aura as introduced earlier in the discussion of Flexible metrics in section 5.2.2. Recognising location via known infrastructure or static equipment will influence degradation of confidence and even parameterised thresholds for service activation and application use. Security invoked at home is intuitively less than that required when a device identifies itself as being in an entirely alien environment. Identity confidence should be eroded more slowly and levels at which authentication is required, lowered.

Additionally, people interact differently with technology in different environments (e.g. the usage of a laptop during working hours may be starkly different to its usage at home in the evening) and so the Authentication Aura will need to adapt and use appropriate authentication. Although the strict identity of an individual remains unaltered the perceived identity can be quite different for some biometric authentication methods such as keystroke analysis.

An advantage of knowing a person's location would be sufficient for applications to carry out predetermined actions in a given situation, such as muting a mobile phone whilst at the cinema or in a library. In these cases, the person's relationship or interaction with a place is more important than the physical location (Hazas et al., 2004). Although the determination of such actions could be considered burdensome, the Authentication Aura has the capability to meet this need if so desired.

The influence of location is coupled closely with the degradation of confidence. Section 5.5 expands upon this concept and explains in detail how the two Aura elements work in unison.

### ***5.4 Taxonomy of Device Interaction***

Exploring the taxonomy of device interaction will give an understanding of the relationships that need to be established in order to facilitate the implementation of an Authentication Aura. Figure 5-1 and Figure 5-2 already illustrated some of the types of interaction that will be experienced and indicates how both one way and two way communications will need to be accommodated.

Below are outlined each category of relationship and a discussion of scenarios where this interaction may occur. Each relationship is initiated by a user's device on which they have been

authenticated (either directly or by Aura assessment) and the target device with which the liaison is to be established.

#### **5.4.1 Own New or Un-trusted Device**

This inter-device relationship triggers the procedure of enrolment, discovery and introduction necessary for the new equipment to operate as part of the Aura. For instance, when a new mobile telephone is purchased by an individual, upon initiation, it will have no knowledge of its surroundings or kindred devices and equally the other pieces of equipment owned by the user will have no prior knowledge of the new item. Initially security will have to be set to the highest level by all devices in the security cooperative, even though some of them are familiar to each other. This is because in the worst-case scenario, following initial authentication the owner may have had all items stolen and the presence of a new device might indicate their removal.

Enrolling new devices into the Authentication Aura framework will require a phase of tentative introduction in addition to self user verification as soon as feasibly possible. During this pairing like process the individual devices must be satisfied with the authentication process on both items before the new entity can be confirmed as being a new member and extension to the Aura. Following this, ongoing operation would adopt the methodology outlined in the following subsection.

#### **5.4.2 Own Trusted and Established Device**

Within this relationship all devices are owned by an individual, with trust and knowledge of each other having already been ascertained. Typically this might be the relationship established between an individual's smart phone, personal computer and tablet. Each device is known to every other, and upon initiation there is a level of anticipation regarding the presence of the other devices that can contribute towards the Aura. With the inclusion of location recognition and the contribution from these devices the requirement to authenticate on a newly activated device might be negated. For instance, having logged onto a PC via fingerprint authentication and with the presence of a PIN enabled smart phone, activating the user's own tablet whilst at home might draw sufficient confidence from the two sensed and recognised pieces of equipment to facilitate access without need for further security assurances.

This taxonomy encompasses both intelligent and dumb devices although the relationship between an intelligent and a known dumb device is only one way as illustrated earlier in Figure 5-1. Enough detail will be held to recognise the inert equipment when encountered but

because of its incapability to converse it can only be used as a token, merely its presence contributing to the Aura assessment.

### **5.4.3 Alien New or Un-trusted Device**

A precursor to the taxonomy discussed below in subsection 5.4.4 and interaction with an alien<sup>13</sup> device is the enrolment process that must be undergone to introduce the assurance necessary for cooperative working. It is unlikely that this will be an entirely unobtrusive process; it will require some human intervention. Alien devices are generally used for less onerous tasks such as printers and refrigerators. This category of equipment, from the perspective of the user, can usually be regarded with complete confidence and act as tokens in contribution to the confidence calculation. Communicated information, in the majority, flows from the device within the Authentication Aura to the alien device; for example a printer only transmits job status information in the reverse direction. The printer is more intent on establishing whether or not it should accept the print request.

In general, alien devices will always remain external to the Aura and therefore recognition must be established by listening to the near vicinity, identifying networked devices and transmitting polled requests for identification. Once a list of present and currently unknown devices has been compiled it will then be a manual task for the user to review each and specify the appropriate interaction.

### **5.4.4 Alien Trusted and Established Device**

Some devices, even though they are deemed trustworthy, will always remain alien to the Authentication Aura and never accepted as part of it. However, in the future it may be possible for the alien device to utilise the confidence of identity established within the Aura for its own purposes, provided it is known to the Aura. An example of this might be the approach of an individual to a cash-point machine (ATM). Upon entry of the customer's cash card and associated PIN the electronic items held about the person could be polled by the ATM to identify themselves but in consequence the Aura would not expect the ATM to become a part of it. The ATM system would need to have prior knowledge of the items owned by the customer and be able to cross reference these against the user's cash card; it is not secure to unilaterally act upon the device identification because of the possibility of theft.

The Authentication Aura must be able to deal with such a scenario and respond accordingly. Devices will need to be allocated controls that govern their social promiscuity and identify the mode in which they will be expected to cooperate with encountered entities. It is essential

---

<sup>13</sup> In this context an alien device is one not exclusively owned by the user

that the method of secure identification that is synthesised will allow recognition of alien devices whilst protecting against spoofing attacks. Only with assurance that the nearby alien device is in fact what it purports to be will the Authentication Aura be confident enough to enter into appropriate negotiation.

#### **5.4.5 Shared Computational Capability**

A further subset of a user's own trusted and established devices (section 5.4.2) are those that are able to share computational capability. In some established relationships one device might be capable of capturing information that can potentially be used for authentication but because of computational restrictions be unable to process the information autonomously. If however the capturing device is able to transmit this information to another Aura member which has the capacity to process the data, the receiving device can undertake authentication on behalf of its colleague and either convey the outcome or use the result for the benefit of the Aura.

For example some MP3 music players have inbuilt cameras and Wi-Fi capability that will enable them to capture a facial image of the user but they are incapable of independently acting upon it. If it can transmit the image to another device within the Aura that can process this information, resultant successful analysis will provide authentication with a good confidence contribution.

To establish these symbiotic relationships additional parameters will be required to identify devices on either side of the affiliation, signifying those that can capture information and those that can process it. This identification process would have to be undertaken after any mutual trust or recognition has been established.

### ***5.5 Degradation of Confidence***

On the majority of personal devices, as an individual authenticates, the piece of equipment establishes a confidence in the user's identity. In most scenarios this is Boolean, in that the user is either believed to be whom they claim to be (they pass the authentication process) or they are not (they fail). As a consequence, the confidence in the user's identity is either set at total (100%) and universal application access granted, or it is none and the user is barred. One of the fundamental concepts of the Authentication Aura is the degradation of a user's identity confidence over time, with the associated restriction on service access as the tariff reduces. High confidence will permit the use of expensive applications and access to sensitive data, whilst reduced confidence can be used as a cue to block the use of these functions (Clarke, 2011 p. 180). Then when confidence erodes to a suitably low level, or a high level action is attempted with insufficient confidence, re-authentication of the user will be necessary to

ensure continuing availability of use. This proposal is similar in concept to an approach outlined by Clarke and Furnell (2007) and Furnell et al. (2008). The original IAMS and updated NICA frameworks discussed how eroding confidence could be used to shutdown the availability of applications until an intrusive specific authentication was required to enable the user to continue device use. Although the current work does not specifically develop its proposals based upon these publications, it does acknowledge the detail contained within and the similarity in approach. This section examines the degradation of confidence and how it will impact upon functionality of an Aura's devices.

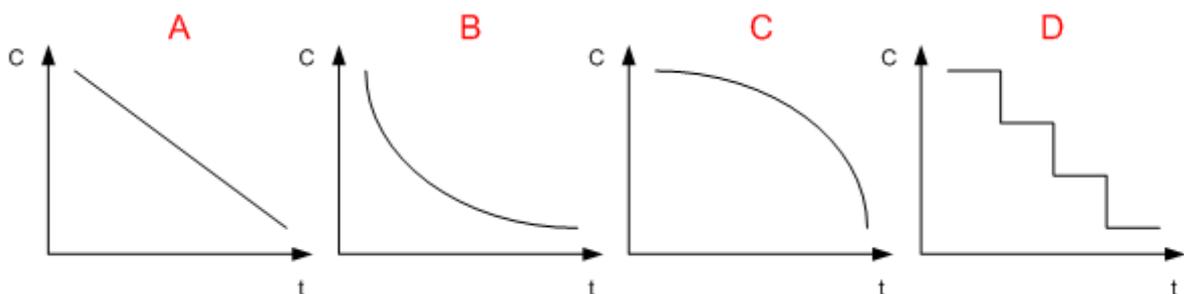
Initial assessment of confidence in the user's identity will be established by the Aura in one of two ways. Upon activation of a piece of intelligent equipment, the surrounding locale is polled for trusted and recognised devices to establish a confidence level. If recent and high level authentication has been performed on one or more nearby devices, the inherited confidence can be established and may well be sufficient to postpone intrusive authentication. If the contribution from the Aura devices is insufficient to achieve this state, the traditional second method is invoked and explicit authentication is required from the user to directly establish the confidence in their identity. Upon completion of either of these processes and with the confidence level set, the device will proceed to operate within the Aura framework.

The first fundamental influence upon confidence erosion is time, as time passes suspicion regarding the user's identity should increase. It is an inversely proportional relationship as captured below in Equation 5-1 which illustrates that as time ( $t$ ) increases ( $t$  approaches infinity) the core confidence ( $C$ ) of device  $x$  will tend to zero.

$$\lim_{t \rightarrow \infty} C_{x,t} = 0$$

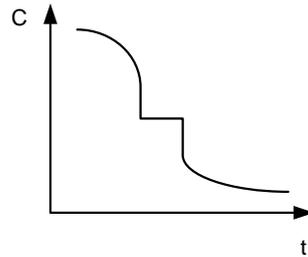
**Equation 5-1. Relationship between time and identity confidence**

Intuitively the erosion of confidence can take many forms from linear erosion, through curved, to stepped reductions as illustrated below in Figure 5-3; even a combination of more than one form of degradation as shown in Figure 5-4 might be appropriate in some situations.



**Figure 5-3. Graphs of varying approaches to confidence degradation over time**

Different approaches might be suited to different devices within the same Aura. For instance a high value device that holds sensitive information might require an initially rapid decrease in confidence which slows as time passes (graph B), whilst a lesser item of equipment could be suited to a slow linear reduction in identity confidence (graph A). It can also be argued that following strict authentication it is unlikely that within a short period of time the device would be lost or stolen; it is probable that it is being used and consequently in the user's control. To reflect this a degradation path should be chosen that erodes slowly to begin with but then gathers pace as more time passes as illustrated in graph C.



**Figure 5-4. A combination of confidence degradation approaches over time**

A further influence on the process which has already been referred to earlier in this chapter is location. There are two main types of location that any user will experience, those that are familiar and known, and those that are alien and unrecognised by the device. However a finer granularity can be introduced by dividing familiar locations into home and work; Table 5-2 summarises the categories of location and how they influence security.

Location	Threat	Description
Home	Low	Location most familiar to user and devices where security can be most relaxed. Multiple static inert devices present. Several users sharing the same device. Accessible infrastructure.
Work	Medium	Regular weekday time spent at this familiar location. Security can be slightly relaxed although device removal a possibility. Some shared device usage. Multiple familiar but un-owned devices present. Accessible infrastructure.
Alien	High	Unknown location, unlikely that any other familiar devices are present. Unknown inaccessible infrastructure.

**Table 5-2. Summary of locations**

Consequently home is where confidence should erode at its slowest, work at a medium rate but when in an alien location and the user is away from both work and home confidence must decrease at its most rapid as shown in Figure 5-5. It is evident that the influence of location must be incorporated into the degradation calculation in a way that will influence confidence accordingly.

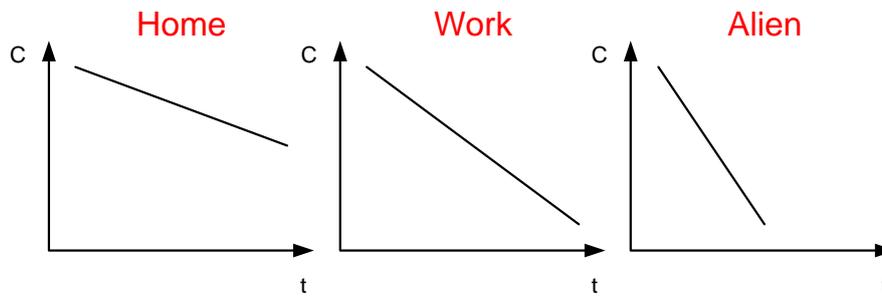


Figure 5-5. Confidence graphs illustrating the influence of location

It is important to highlight that when strict authentication is successfully performed by the user the level of confidence in identity, immediately afterwards, will not necessarily be set to 100% as a default. Previously in section 5.2.3 it was discussed how authentication techniques vary in rigour and strength, and how parameters will dictate the initial core confidence allocated following authentication. For instance Figure 5-6 shows how authentication methods with varying rigour will reduce the starting percentage of confidence and subsequently affect the rate of degradation even when the location of the user remains unaltered. An iris scan has the highest starting confidence value with slowest degradation because of its rigour and imparted security, voice recognition is awarded a lower initial confidence and a medium rate of erosion, whilst PIN authentication experiences the lowest starting value and steepest rate of decrease.

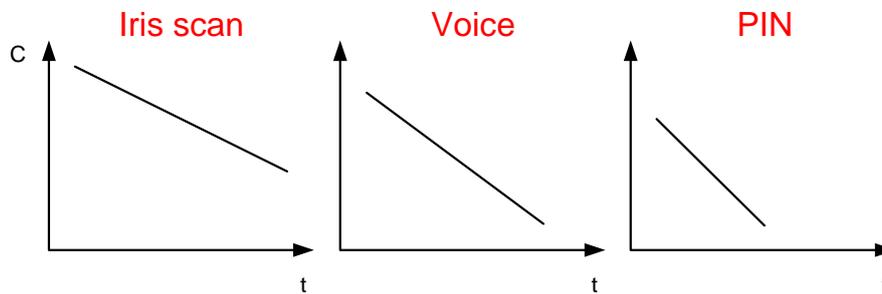


Figure 5-6. Confidence graphs illustrating the effect of different authentication methods

With consideration being given to all of these requirements it is possible to now summarise the core confidence calculation in the following equation.

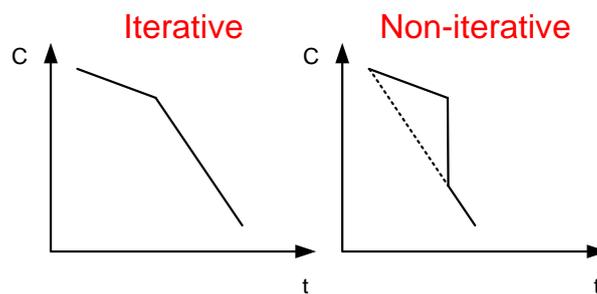
$$C_x = F(t_x, m_x, l)$$

Equation 5-2. The core confidence calculation equation

In Equation 5-2 it is noted that the core confidence of device  $x$  is a function dependent upon time since authentication on the device ( $t_x$ ), the method of authentication ( $m_x$ ) and the location ( $l$ ). Additionally because this confidence is a percentage the function will be bounded above at 100 and below at zero. A vital caveat to this function is that confidence erosion must be treated as an iterative process and not as a direct time calculation. This implies that when location is changed via the user physically moving the effect will be to alter the rate of

degradation from that point onwards to ensure that the Aura is still influenced by the time spent at the previous location. For instance when a user leaves home if a complete recalculation (non-iterative) took place it is likely that a huge dip in confidence would immediately be experienced, triggering service barring or a polled request for authentication artificially early.

Figure 5-7 below illustrates the comparison between the iterative and non-iterative approach described in the previous paragraph. The point at which the user leaves home is evidently clear but the iterative graph indicates how the influence of the time spent at home remains when compared with non-iterative degradation that exhibits the immediate significant drop in confidence.



**Figure 5-7. Comparison of iterative and non-iterative confidence calculation**

Within the Authentication Aura confidence erosion will be offset and potentially reversed by confidence gained from the user's personal Aura and so it is important to remember that although degradation is a fundamental process it is only one element of the entire approach. In the remainder of this chapter these other influences will be discussed and the overall form of the confidence equation introduced.

## **5.6 Information Policy**

It is imperative to establish a policy regarding the information that flows amongst the elements within an Authentication Aura which will control its effect and duration of validity. Information will be received by a device in response to a request for status updates, as unpolled detail from other Aura members or as identification of dumb devices and infrastructure. This section will examine these scenarios and discuss the length of time for which it can be regarded as significant.

When an intelligent device is activated and its Authentication Aura system launched the first process it will have to undertake is to ascertain what other devices are near, operational and prepared to cooperate. This will be achieved via transmission of a general request for status information to the local vicinity to engender replies from other Aura members. Those that are present and active will respond and their contribution to confidence assessed; the conveyed

detail will specify the last time of strict authentication and an indicator signifying the strength of the method used.

The same data should also be transmitted whenever strict authentication is performed upon any device capable of relaying the information. Although the authentication has occurred in isolation transmitting the detail will benefit the Aura as a whole, enabling interested receiving devices to gain the greatest advantage from the knowledge to maximise their own confidence assessment.

Intuitively it is unreasonable to treat the received information with the same significance as time passes. If a communication is received indicating that authentication has just been successfully passed on a device, at that moment it is extremely significant and should port an equally significant proportion of confidence to the receiver. However as time passes, without further status updates being received and although the contribution should still be counted, it will carry less significance. The Authentication Aura should address this situation in two ways; firstly any received contribution assessment will be degraded over time, and secondly at parameterised intervals all contributing devices must be polled to ascertain their continuing presence and their current status, ensuring that all information is as up to date as possible.

In a similar manner, inert devices and infrastructure that are acting as tokens and indicators of location will also be polled on a parameterised time interval to ensure they are still within the Aura's active vicinity. Implementing another user controlled parameter to dictate this time period not only complies with the requirement for flexible metrics (refer to section 5.2.2) but also gives the user control over the performance of the Authentication Aura. However, the presence of the token inert equipment is Boolean in contribution, it is either detected and adds to confidence, or it is undetected and considered absent. For this category of device the policy will be to include its existence when relevant without degradation over time, with the only influence being the user controlled significance rank. For instance detection of a contactless payment card might be deemed more significant than the presence of computationally incapable MP3 player.

$$C_i = F(t_i, m_i)$$

$$C_d = F(r_d)$$

**Equation 5-3. The contribution to confidence made by an intelligent device**      **Equation 5-4. The contribution to confidence made by an inert device**

Utilising this information policy enables the realisation that the confidence contributions made to the Authentication Aura by any individual intelligent device (*i*) (shown above in Equation 5-3) is a function of the time since successful authentication and the method used, and those

of inert/dumb devices ( $d$ ) (Equation 5-4) is a function of the user controlled device security rank ( $r$ ).

The equations shown above encapsulate the parameters to be used when formulating the confidence contributions of both inert and intelligent devices but only when simulation has been performed and analysis of performance observed will it be possible to establish the precise detail of each function.

## **5.7 Data communication**

As illustrated earlier in Figure 5-2 the Authentication Aura relies upon the communication of information between intelligent devices, and the sensing of infrastructure and inert devices. The concept of Aura is focussed upon the local vicinity that surrounds the user at any given moment and so it is across this area that communication must be enabled. With security being the primary focus, to minimise data leakage to eavesdropping equipment inter-device communication should only operate over a relatively short distance such as 3-4m. This will also ensure that should some equipment be surreptitiously removed it will quickly drop out of communicable range and its contribution to the Authentication Aura lost, reducing the confidence of the host device. With the development of technology a number of methods are now in-built and available for use; for instance NFC, RFID (NFC being a form of RFID), Bluetooth and Wi-Fi are all commonly resident in the modern smartphone and able to impart information (Baker, 2011; Bluetooth, 2014; RFID Journal, 2013). Dumb equipment and infrastructure however, are used as location identifiers and tokens but do not as a rule have a variety of options available; they are either detectable or not, and generally via a single communication channel. For example Internet access points are Wi-Fi enabled, contactless payment cards utilise NFC and car keys RFID. Although NFC is specifically designed to operate over a very short maximum distance of 4-5cm the underlying RFID technology has the ability to be detected over greater distances which qualifies it as a usable candidate (NFC Forum, 2014; Rapid NFC, 2013).

To get full advantage from the local vicinity it is vital that the Authentication Aura will have to adapt and possess the potential to use all of these methods as required. It will simultaneously be required to monitor all channels and transmit responses or requests appropriately.

The vast majority of inter-device communication will consist of short individual text strings that contain details of performed authentications or Authentication Aura generated messages. However, as previously outlined there will be a requirement to pass captured biometric samples for analysis from one device to another. These are much larger blocks of data and because of their sensitive nature must be appropriately secured. Utilising a long-term

symmetric key which could be exchanged between devices when their initial trust is established, from which short-term symmetric session keys are generated to encrypt the biometric sample that has been captured prior to transmission (Xiao et al., 2013). Pre-encoding the data sample in this way will secure it and ensure that if captured by an alien device it will remain protected.

To achieve the required data communication Bluetooth has the greatest suitability because of its minimal footprint, wide availability, resistance to interference, low power usage and overall flexibility (Ang, 2008). Taking devices through the pairing process during setup will inherently introduce a level of inter-device trust and knowledge, providing confident communication and an immediate degree of security. The element of the Authentication Aura that manages communication however will require inbuilt flexibility to utilise a variety of the methods outlined above and adapt as required.

## 5.8 Summary

This chapter has introduced the core functional requirements and elements of an Authentication Aura upon which a detailed framework can be built. It has highlighted the need for the transfer of information relating to location, time since authentication and the method used between trusted devices, and how this combined with the presence of other detected possessions can be used to calculate a positive confidence contribution. In contrast it has also examined the erosion of identity confidence and general functions for its calculation have been proposed. Although without simulation it is not possible to precisely define the specific functions that will be employed in any of the listed elements it is imperative to understand how they relate to one another. As such, the distinct constituents can now be combined and the formula for the calculation of identity confidence visualised.

$$C_x = \left[ F_1(t_x, m_x, l) + \left( \sum_{i=1}^n F_2(t_i, m_i) \right) + \left[ \left( \sum_{d=1}^p F_3(r_d) \right) \right]_{\min 0}^{\max a} \right]_{\min 0}^{\max 100}$$

**Equation 5-5. Combined identity confidence equation**

In Equation 5-5:

$x$  signifies the user device on which the confidence  $C$  is being calculated and  $C$  is bounded within the range 0.0 to 100.0 inclusively.

Function  $F_1$  calculates the amount of core confidence held by the host device  $x$ , using the time ( $t$ ) since authentication was carried out on the given device ( $x$ ),  $m$  the method of authentication that was used and the location ( $l$ ) of the user.

$n$  represents the number of intelligent devices and  $p$  the number of dumb that constitute the current active Aura.

Function  $F_2$  yields the contribution to confidence that each intelligent Aura member ( $i = 1..n$ ) makes to the receiving device  $x$ . This function utilises the time ( $t$ ) since authentication was undertaken on the contributing device ( $i$ ) and the method used ( $m$ ).

The confidence contribution assessment of dumb and inert items to the receiving device  $x$  is calculated by function  $F_3$ . Each of these Aura members' ( $d = 1..p$ ) addition is simply based upon their rank ( $r$ ), a numeric indicator used to represent their significance. The total inert device contribution is bounded at a parameterised upper limit  $a$  to block excessive influence being gained from this element of the Aura.

The following chapter will now build upon these concepts and detail a framework which will administer and control an Authentication Aura, providing a route to simulation and further analysis. All of the core elements introduced will form the fundamental premise for the framework and enable it to be developed in a focussed and controlled manner, whilst precisely addressing any of the outstanding issues.

---

## **Chapter 6**

# **Authentication Aura Framework**

---

## 6. Authentication Aura Framework

---

Now that the supporting principals have been ratified by the experimental results and the core elements introduced in the previous chapter it is necessary to establish a framework within which a functioning Authentication Aura can be constructed. The framework must enable a member device to identify its current locale, recognise and communicate with the infrastructure and other devices contained in it, and interpret this information to formulate a confidence coefficient of user identity. This figure can then be used as a user adjustable security control to either permit or deny service and application usage upon the host device, enhancing the security of the device and benefitting the user with an increased assuredness of its integrity should it be lost or stolen, or when operating in an unfamiliar environment.

A fundamental principle of the Authentication Aura is its capability to function for a user with a single device without contribution from external influences, or grow into a collaborative network of trusted devices, further supported by possessions and infrastructure. The member devices can be intelligent with the ability to perform independent computation and communication such as tablet computers or smartphones, or dumb with merely the ability to be detected, for instance car keys or contactless credit cards. Hence the framework and resultant product must be able to adapt to changing environments, a variety of devices, and the arrival and disappearance of member items at random intervals during operation. It is a fundamental principle that the Aura will be gregarious and include as many devices as possible. This requirement will maximise the influence that can be obtained from the Aura members and provide the greatest security assurance for the owner when using multiple devices. Further to this, to provide an additional benefit, some intelligent devices will be able to provide an authentication service to other less capable pieces of equipment. That is, a laptop could undertake voice recognition on behalf of a basic mobile phone that is capable of capturing a voice sample but lacks the processing power necessary to perform the analysis and authentication. By capturing the sample and transferring it to the laptop for analysis, it would be able to undertake a higher level of authentication than would otherwise be possible. To ensure data integrity it is vital that this process be performed in compliance with the ISO standards for biometric information interchange highlighted earlier in Source: ISO (nd)

Table 5-1; that is standard ISO/IEC 24713-1:2008 (ISO, nd) which specifies details of how the data should be exchanged between devices and the precautions that should be taken to ensure data integrity and protect its security.

Finally, it is paramount that the framework design produces agents with small footprints, enabling them to be deployed upon the greatest range of devices, whilst providing a level of sophistication that will administer the Authentication Aura effectively. To achieve this it is imperative that any resultant design be focussed and efficient, with size being kept to a minimum.

This chapter will explore in detail the components of the framework, how each functions and the interoperability that is necessary to achieve the requirements above. Initially a diagram is presented to provide an overarching understanding of the framework with an associated outline of the components and their role in its operation, which is then supplemented by a more detailed investigation and explanation of the specific function of each.

### 6.1 Anatomy

A diagrammatic view of the framework is shown below in Figure 6-1 which outlines the elements and interconnectivity that has to be incorporated into the design. The diagram divides the internal structure of the agent into two discrete groups, the data and the processes. The data is intuitively a key element in the design of a functioning Aura agent with the data tables and the information stored within dictating the flexibility of the Authentication Aura to adapt and its ultimate capability. The processes collectively form the agent and are the logical blocks that undertake data processing, initiate internal and external communication, and provide the agent with the sophistication required to establish and manage the user's Aura.

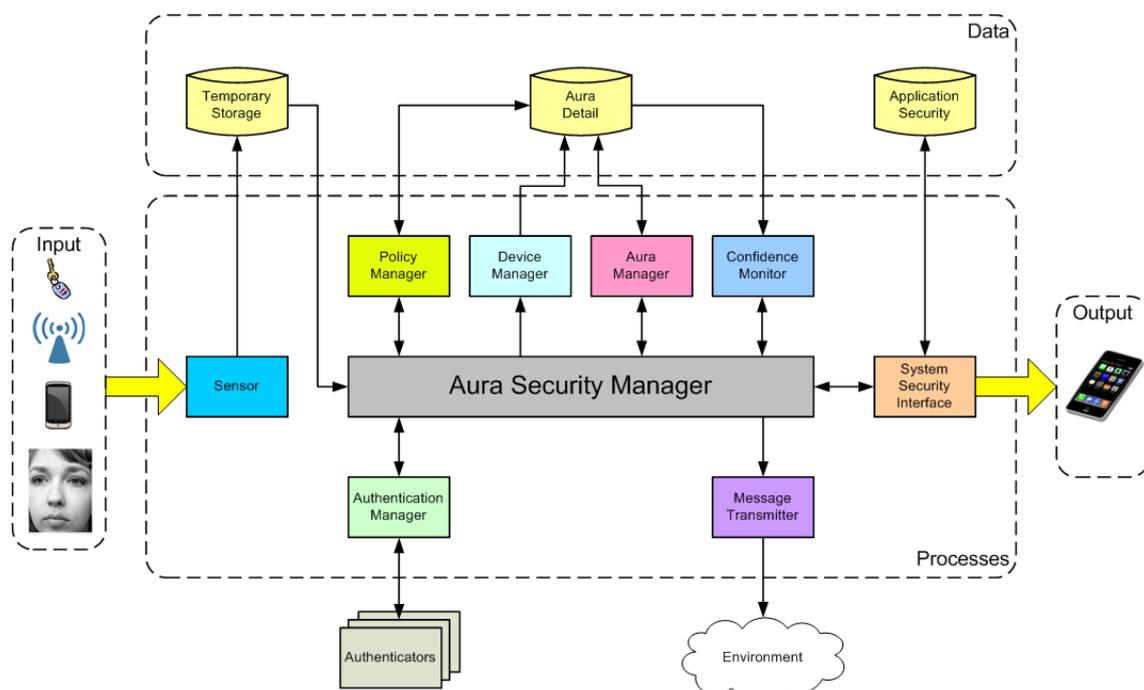


Figure 6-1. Authentication Aura implementation framework

The framework diagram illustrates the presence of three distinct databases, Temporary Storage, Aura Detail and Application Security. Although in implementation it is probable that the agent will contain a single database with multiple tables, to facilitate clarity and for the purposes of this thesis the tables have been grouped into these three disparate types. Table 6-1 below outlines the data tables contained in each of the three groups to provide an understanding of the information that will be held.

Database group	Data table	Description
Temporary storage	Message cache	Stores received messages from other Aura members in preparation for processing.
	Authentication sample	Holds data samples supplied by other Aura member devices that require authentication e.g. a voice sample.
Aura detail	System parameters	Controls the parameters and variables required by the system to function. These are both default and user amended values.
	Location	This table will hold the locations at which devices can be found. Initially it will default to Home, Work and Away but will be user extensible.
	Device	Stores the records of trusted devices that can become members of the Aura.
	Aura	This key table holds the details of the current Aura and the status of the member devices.
Application security	System security	A table of thresholds used to control the confidence level at which application invocation and service activation is denied.

**Table 6-1. Database structure**

For further clarity Figure 6-1 presents a separation between the databases and the processes. However, in reality each is inextricably linked with the other and thus precise details of the data tables will be explained in conjunction with their controlling processes. Firstly though, it is appropriate to introduce the required processes and provide an insight into the function of each.

The information necessary to operate the Authentication Aura is drawn from the surrounding environment, be this sensed infrastructure, tokens or communication from other active Aura members within communicable distance. Figure 6-1 illustrates a representative mixed sample of data sources, showing items such as keys, Wi-Fi access points and electronic devices passing information into the agent via the Sensor. It is important to reiterate that some of these items (e.g. keys) may not be intelligent and possess the ability to communicate; rather their mere

presence is sensed and used as a contribution<sup>14</sup>. The information obtained from each can vary greatly, from indication of presence to complex biometric data samples for analysis. The Sensor will react appropriately to the type of data, collate the received detail and place it into a Temporary Storage database for later processing.

The Aura Security Manager (ASM) is the core processing unit of the framework. It utilises the information held within the Temporary Storage invoking appropriate processing procedures as required. Upon installation the ASM directs the user to define system parameters and tailor the system to their specific requirements; this process is administered by the Policy Manager. When the system is activated the Policy Manager is also called to initiate operational parameters and thresholds in preparation for ongoing functioning.

When captured data samples are passed to a sophisticated device for analysis and authentication by a less capable device, the ASM uses the Authentication Manager to undertake this process. Dependent upon the category of data sample the Authentication Manager will utilise external Authenticators to perform the relevant processing. For instance, if a fingerprint image scan was captured and supplied the Authentication Manager would pass the data to a fingerprint authenticator for analysis, whilst if it were a voice sample an alternate but appropriate authenticator would be called. The Authentication Manager will then obtain the verification result and inform the ASM accordingly.

The Device Manager administers data pertaining to known devices that are trusted by the host device. Upon initial recognition of a new device the ASM invokes the Device Manager to create a relevant record in the Aura database. Once the record exists and the device recognised at a future date, the Device Manager will be used to supply the ASM with its relevant details to be used as required.

Administration of the Aura, the devices currently active within it and necessary information requests are all undertaken and generated by the Aura Manager sub-process. This process will operate under the direction of the ASM, updating the database with the latest details as devices arrive and depart, location changes and communications are received. Then as status updates from other Aura members are needed, the Aura Manager will communicate the request back to the ASM for processing.

When an information request is received by the ASM it uses the Message Transmitter to perform the practicalities of compiling and sending the message to the relevant device. This

---

<sup>14</sup> The research experiment detailed in Chapter 4 produced results that overwhelmingly supported the inclusion of these inert devices into the Authentication Aura's design.

removes the ASM from the burden of having to interface directly with the appropriate communication channel and provides a degree of flexibility that will allow the Authentication Aura framework to be deployed on as many types of device as possible.

The Confidence Monitor will continually assess the information held within the Aura database and based upon the time since last authentication of the host and other member devices, the current location, and the status of member devices, will calculate the security confidence coefficient. This value will then be passed from the ASM to the System Security Interface which will communicate directly with the device's operating system, intercepting requests for application and service usage, blocking those which have been defined as requiring a higher confidence level than that which is currently experienced. If a request is blocked the user will be given the option to authenticate themselves in order to raise their identity confidence and if passed the request be will be reassessed and invoked if appropriate.

Now that an overview of the framework has been established the remainder of this chapter will undertake a thorough and detailed investigation into the functions and roles of each of the elements, providing a complete understanding of the logic to be employed and the intricacies of an operational Aura.

## **6.2 *Sensor***

The Sensor provides the communication gateway into the Aura from the local surroundings, receiving all messages that are of concern to the device, sensing token (dumb) equipment, and monitoring the environment for networks and infrastructure that can be used to recognise the current location. To ensure that all messages are received and equipment sensed, the Sensor will have to continually monitor all channels through which communications can be received, dependent upon the device and its associated sophistication. A number of communication channels are available such as Bluetooth, Wi-Fi networks and local area networks as discussed in section 5.7 but because of security provided by its limited operational range and the inherent security from the pairing process, the primary channel for communication will be Bluetooth. However, as Near Field Communication (NFC) and even RFID become more prevalent on laptops, smartphones and other mobile equipment, the potential to sense possessions such as contactless credit cards and keys will evolve. These tokens will respond to a polled request from a master device, a role which can be fulfilled by a suitably enabled piece of equipment on a regular basis providing a key element to the Authentication Aura as the research experiment proved. Interfaces to each of these communication channels will need to be incorporated into the Aura agent providing the means for the Sensor to monitor the local environment effectively.

As a module the Sensor is standalone, continuous and does not have any direct communication with any other processes. It analyses the information it receives or gathers, parses it and then depending upon the type of information places it into one of two temporary storage data tables, Message Cache or Authentication Sample. Two data tables are required because of the very different nature of the two categories of communication; messages are short and carry a small amount of detail, whilst authentication sample requests will potentially contain large amounts of data for processing. Separating the two tables will enable the data to be handled more efficiently and result in faster processing.

As temporary storage the function of these data tables is to temporarily store information in preparation of processing by the Aura agent for a brief period of time. As transmitted data is received, identified and verified by the Sensor it is inserted into one of the two tables. Each table is distinct, unrelated to the other and acts as a short-term holding repository. Upon opening or closing the device any remaining data will be cleared and the appropriate table left empty.

It should be noted, when data tables are introduced, alongside the title the suggested name is shown in brackets, i.e. when the agent software is developed it is suggested that the 'System parameters' table be created as 'param' and this is then carried through the design by prefixing each of the columns with the corresponding table name. For instance, 'param\_key' is the key field for the table 'param' ensuring consistency and clarity throughout.

### **6.2.1 Message Cache data table (cache)**

The Message cache data table is used to hold all received inter-device communications that have either been generated by an intelligent Aura member or detection of an item of equipment that is acting as a token. It is a repository that aides processing speed whilst ensuring that all messages are recorded without any being lost. As each appropriate message is received by the Sensor a new row is appended to the table and remains until it is parsed and used by the ASM.

Each data row will hold up to nine distinct columns as illustrated in Table 6-2 below. The key field cache\_key is the primary index field that dictates the order in which the messages are received. It is an incremental integer automatically allocated during row insertion by the database engine and can be reset upon initial activation of the device. Although cache\_key indicates the order of receipt, cache\_received maintains the precise internal date and time at which the message was detected. When a communication is processed and the row created, the receiving device's internal clock value is allocated to this column on table update.

During any information receipt or sensing of infrastructure and tokens, the identity code of the technology or broadcasting device will be detected. This unique identifier is held in the `cache_device` field of the message cache data table to aid subsequent processing. For known and familiar devices this can be used to rapidly identify them accurately, dictating how the received message will be handled; for alien or unknown devices it can be used to start building familiarity.

Field name	Description	Type	Length	Details	Example
cache_key	Key field	Integer	n/a	Auto increment	1
cache_received	Date and time received	Date	20	Date and time in internal format at which the message was received by the device	15824937301
cache_device	Source device identity code	Text	50	Character string used to identify device. i.e. machine identity code or similar	00037A964637
cache_message_type	Character	Text	1	Single character that indicates the type of message that was received and cached e.g. A (Aura message), I (infrastructure sensed), T (Token/dumb device), U (unknown – although this should not be used)	A
cache_message_command	Message command	Text	3	The message command	MSI
cache_message_identity	Device identity	Text	50	Character string used to identify the target device. i.e. machine identity code or similar	A785H6575G46
cache_message_detail_1	Message detail #1	Text	50	First detail field. Is dependent upon command	19:32:48
cache_message_detail_2	Message detail #2	Text	50	Second detail field. Is dependent upon command	5
cache_message_detail_3	Message detail #3	Text	50	Third detail field. Is dependent upon command	00037A964637

Table 6-2. Message cache data table definition

Field name	Description	Type	Length	Details	Example
auth_sample_key	Key field	Integer	n/a	Auto increment	7
auth_device	Source of authentication sample	Text	50	Character string used to identify device. i.e. machine identity code or similar	00037A964637
auth_sample_type	Type of sample	Text	5	Indicator used to identify the sample type that has been transmitted for authentication e.g. FR (facial recognition), V (voice), FP (fingerprint) etc.	V
auth_sample_received	Date and time received	Date	20	Date and time in internal format at which the authentication sample was received by the device	6389543390
auth_sample_encryption_key	Authentication sample encryption key	Text	50	Public encryption key allowing the authentication data to be deciphered	1456383683
auth_sample_data	Authentication sample data	Blob	n/a	Encrypted	QE+yg)05sbQ/@...

Table 6-3. Authentication sample data table definition

As the Sensor receives communication the command string will indicate the type of message detail received. Rather than wasting this knowledge a single character is allocated to the `cache_message_type` column that can be utilised by the ASM to immediately categorise the type of message, aiding the processing speed. For example, 'A' will indicate an Aura message from another device whilst 'I' the sensing of infrastructure and 'T' a token. With the Sensor hearing all but with limited processing capability, it is imperative that a catch-all be utilised in scenarios where the source and message type cannot be readily identified, the character 'U' (unknown) is reserved for this purpose.

When a message is received from another Aura member, it will contain a short text string that identifies its function enabling the appropriate action to be taken. The format of the command string is detailed in section 6.2.3 and will be held within the `cache_message_command` field.

`cache_message_identity` is used to hold the identity string contained within the message. Finally three columns have been allocated to store the remaining detail associated with the received message. These may or may not be filled with data dependent upon the type of communication that has been received.

### 6.2.2 Authentication Sample data table (auth)

In some instances, devices that are active members of the Authentication Aura will be able to capture user details that can be used to authenticate identity but will be unable to perform the process independently. For example, a low-end tablet computer is capable of capturing a user's facial image or voice sample but may not have sufficient storage available to host the application and processing capability necessary to undertake authentication via facial recognition. With an active Authentication Aura enabled laptop within communicable range it is possible to securely transmit the encrypted image or sound file to the laptop for remote validation. In this scenario the Authentication sample data table as illustrated by Table 6-3 will be utilised by the receiving laptop to store the transmitted data prior to processing. In short, it is a holding table for identity data samples sent by other devices that require validation.

This temporary data table is smaller in design but will potentially store much larger items of data. Each row of the table will consist of six columns `auth_sample_key`, `auth_device`, `auth_sample_type`, `auth_sample_received`, `auth_sample_encryption_key` and `auth_sample_data`.

The primary key field (`auth_sample_key`) will be used to control the order of population within the table, enabling the ASM and the Authentication Manager to process received requests for authentication process in the correct order. Although the `auth_sample_received` column

dictates the exact date and time of receipt, being the internal clock value of the authenticating device.

Each item of equipment that communicates an authentication request will supply its identity, sample type and sample data (encrypted where appropriate, for instance in the use of biometric feature capture). The `auth_device` column will be used to track the device from which the detail was transmitted, storing the unique device identity number. This field will then be used to direct the outcome communication appropriately upon completion of the validation procedure.

`auth_sample_type` is used to annotate the type of detail that has been received. It is intuitively important that the authentication process clearly understands what variety of data sample is waiting to be processed, enabling it to perform the appropriate analysis. It has been designed as an uppercase character string that will be easily recognisable. For example, 'FR' will indicate a facial recognition, 'FP' a fingerprint, whilst 'V' will specify a data sample for voice recognition.

As intimated above, transmitted data that requires authentication is likely to be biometric in nature. As such and because of non-repudiation issues it is imperative that any undertaken transmission be as highly secured as possible and encrypted. The Sensor process will receive the transmitted data sample and place it in this table in raw form, it will not attempt to decipher the sample in any way. By inserting any relevant supplied encryption key into `auth_sample_encryption_key` it will enable processes later in the authentication route to manipulate the data and utilise appropriate external modules to ascertain the validity of the sample.

The `auth_sample_data` is an unbounded blob of storage that holds the encrypted biometric sample ready for validation to be performed.

### **6.2.3 Message identification and format**

A message will be received during the operation of the Authentication Aura in reply to a request for information, as a targeted call for information, to pass a data sample for authentication or a general announcement from another Aura member. The first three of these are precisely aimed at the receiving host whilst the fourth is not but must be dealt with accordingly; these transmissions will be received via the configured communication channels.

Each received message will be securely transmitted, and structured in such a way as to allow easy parsing and quick identification of the message type. All messages will consist of a command block separated by an underscore from a device identity, followed by none, one or

more items of detail, each of which is preceded by an underscore. The message format is shown below in Figure 6-2.

**command\_device identity{\_detail}\***

**Figure 6-2. Generic message structure**

Each command string will be comprised of exactly three alphabetic uppercase characters and which can be parsed easily using the underscore to identify the message type. Using the same technique the process will then extract the device identity, a string of characters of undefined length. As introduced above, some messages will be specifically targeted at the receiving device whilst others are purely generic. Although precise message logic and interaction is discussed in section 6.7, it is imperative to briefly introduce the entire message vocabulary to gain an understanding of how each type can be recognised. Table 6-4 illustrates an exhaustive list of Aura messages, a brief description, the category of each indicating the data table into which it will be placed, and the type.

Message code	Description	Category	Type
ARR	Authentication Request Reply	Message	Targeted Reply
ARQ	Authentication ReQuest	Authentication	Targeted Request
AUT	AUThenticated	Message	Announcement
AYT	Are You There	Message	Targeted Request
IAH	I Am Here	Message	Announcement
ISH	I am Still Here	Message	Targeted Reply
MSI	My Status Is	Message	Announcement
PEN	PENding authentication	Message	Targeted Reply
WIT	Who Is There	Message	General Request
WYS	What is Your Status	Message	Targeted Request

**Table 6-4. Message acronyms**

The Sensor module is only interested in processing significant messages, and then to distinguish between the ones containing captured detail being passed for authentication and those that are not. The first category is identified by the command string 'ARQ' (Authentication ReQuest) and is specifically targeted to the receiving device; this will be placed into the Authentication Sample data table if it qualifies on both command and device identity. The second category which will be placed into Message Cache is marginally more complicated to parse. If the message type is an announcement or a general request then it is accepted,

otherwise it has to be specifically targeted and the identities matched. With knowledge of the full vocabulary available, the Sensor will easily be able to filter out irrelevant communication.

#### **6.2.4 Intelligent device monitoring**

All available communication channels will be simultaneously monitored for messages from other intelligent devices that are active within the Aura. The Sensor will parse these communications in accordance with the semantics described in section 6.2.3 above and store them in the appropriate temporary data table. Implementing this rapid processing and storage will enable the Sensor to focus its operation on surveilling the communication channels, ensuring that all messages are received and none are missed.

#### **6.2.5 Token device monitoring**

Token or dumb devices and equipment (those that are unable to authenticate) can still positively contribute to the Aura as previously established. The Sensor process is responsible for the detection of these items and the recording of their presence. With NFC becoming more common, personal items such as contactless credit cards, car ignition keys and even cars themselves will all become detectable by portable devices.

With this capability a device operating the Authentication Aura will be able to regularly poll these items and store their corresponding presence in the Message Cache, in preparation for processing by the ASM. Recording the observed time, identity and token indicator (setting `cache_message_type` to 'T') will provide the ASM with the information it requires.

#### **6.2.6 Infrastructure monitoring**

The final role of the Sensor process is to monitor the infrastructure within the local environment and then for each item identified, to write a pseudo message record into the Message Cache to register the information. This will be achieved by monitoring the device's network interface, gauging the present equipment to ascertain Wi-Fi points, networked servers and other significant equipment (e.g. a networked printer or even a networked CCTV camera). These messages will be used by the ASM to identify familiar locations which will in turn affect the user identity confidence calculation.

#### **6.2.7 Sensor logic**

Figure 6-3 below illustrates the logic of the Sensor process in diagrammatic form, showing the control flow within the module, the decisions that are taken and the points at which data is written to the database. It encompasses all of the three monitoring roles discussed previously and indicates how messages, detected tokens and infrastructure will be allocated to the appropriate cache database.

The logic takes two main routes; the first when a message has been received, and the second when none was detected. When no message has been received the Sensor loops through all infrastructure and token device channels, detecting which are visible and for each entering a pseudo message into the Message Cache data table.

When a message is received the Sensor checks if it is of concern to the receiving device. A message is of concern when it is either a generic request for information or an announcement, or targeted at the specific device; both these scenarios are detailed within the message acronyms shown in Table 6-4. If the message is not of concern it is dropped, no further action is taken and the Sensor continues with its processing. If these checks are passed and the message is deemed significant, one further decision is taken to ascertain if the receipt is a request to undertake authentication of a captured biometric data sample (message command ARQ) or another command. If the message is biometric data the detail is written into the Authentication Sample table to await processing, otherwise an entry is added to the Message Cache table. Processing then continues.

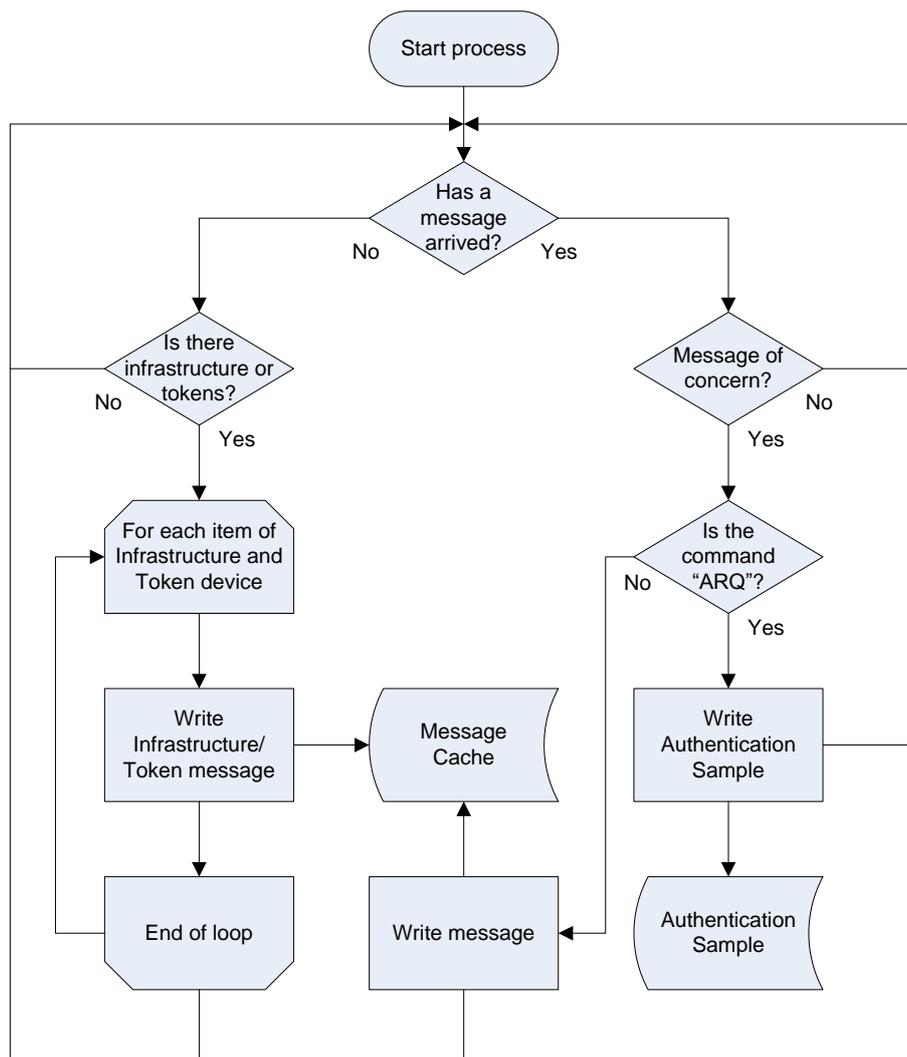


Figure 6-3. Sensor process flowchart

It should be noted that the process operates continuously and in isolation. During the entire operation of the Aura the Sensor will gather the appropriate information and persist in the population of the data tables, only the ASM will remove records as it processes each in turn or when the device is shutdown.

### **6.3 Authentication Manager**

The Authentication Manager is utilised in two ways within the Authentication Aura framework. Firstly, it undertakes the authentication of the current user as required within the regular working of the framework and secondly as an agent performing authentication on behalf of another less capable device.

When the current user attempts to access an application or system process and their current identity confidence is below the parameterised level required to activate the function, the ASM intervenes and requests the user to undergo authentication. In this instance the ASM will call the Authentication Manager to trigger an authentication and the Authentication Manager in turn will interface to an authenticator which is external to the framework. This could be a process as simple as a password or equally a request to provide a fingerprint scan. The available methods are entirely dependent upon the device being used and its inherent sophistication, with any necessary parameterisation being requested and captured during system installation and initiation. Each method will be assigned a tariff of robustness in the range one to five indicating its perceived security by the user. For instance a fingerprint scan would be considered very robust and given a high tariff of four or five, whilst a password is deemed less secure and would potentially only be allocated a tariff of one or two. When authentication is performed successfully upon a user the utilised method's associated tariff will be returned to the ASM for use in the identity confidence calculation as described in Equation 5-5 on page 97. This will provide the user with a degree of control, adjustability and influence over the confidence degradation process.

In an intelligent and sophisticated device there is a secondary role which can be performed by the Authentication Manager; the processing of identity data samples which are passed to the host device for authentication. The data is received from the ASM as it processes the samples held in the Authentication Sample data table as described earlier in section 6.2.2. As already established data passed to intelligent devices capable of undertaking the necessary authentication processes will be biometric in nature and require correspondingly capable external authenticators. The Authentication Manager will interface with the appropriate authenticators, establish the validity of the data sample and report back to the ASM.

Interfaces to the external biometric authenticators will be compliant with the internationally accepted standards of the ISO Committee SC37 which are available on their website, providing a degree of future resilience and allow expansion of the available authentication methods (ISO, nd).

#### 6.4 Message Transmitter

Intuitively the Message Transmitter process is the gateway from the ASM to the outside local environment. Through this process messages are issued as requests for information from other specific Aura members or those that are present but not currently active, and as replies to requests for information. The ASM will supply the Message Transmitter with a variable representing the category of message to be sent and any other required detail, which will then be processed and transmitted accordingly.

At this juncture it is important to further expand upon the messages that are used within a functioning Aura agent and the information that they provide. The vocabulary of the Aura has already been introduced in Table 6-4 on page 111, alongside a brief description of generic message syntax. However, a fuller exploration of this must now be made in order to gain an understanding of how the Message Transmitter will operate; each element of the vocabulary is described in Table 6-5.

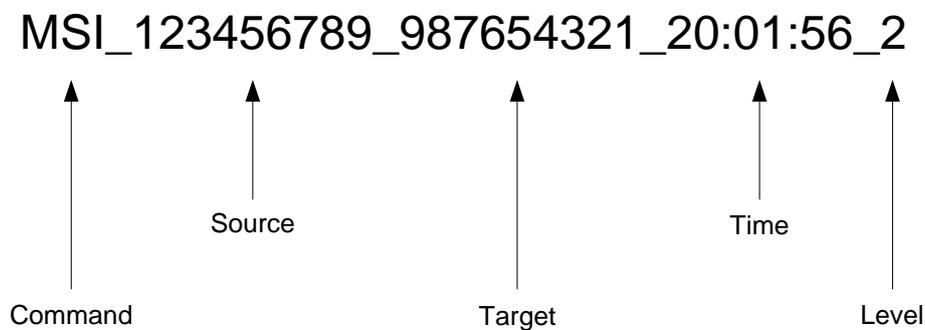
Message code	Description	Syntax
ARR	Authentication Request Reply	ARR_X_Y_success
ARQ	Authentication ReQuest	ARQ_X_Y_data type_blob
AUT	AUThenticated	AUT_X_X_last authentication_level
AYT	Are You There	AYT_X_Y
IAH	I Am Here	IAH_X_X
ISH	I am Still Here	ISH_X_Y
MSI	My Status Is	MSI_X_Y_last authentication_level
PEN	PENding authentication	PEN_X_Y
WIT	Who Is There	WIT_X_X
WYS	What is Your Status	WYS_X_Y

**Table 6-5. Vocabulary syntax and transmitted detail**

In the table above; X represents the device identity of the transmitting device and Y the target device, last\_authentication holds the time at which the last authentication was successfully performed, level conveys the authentication robustness, success is a Boolean indicator used to

pass the success of an authentication, data type specifies the type of data being supplied for authentication (e.g. voice sample) and blob is the data sample to be authenticated.

When invoked by the ASM between one and four arguments will be passed to the Message Transmitter which will then construct the message in the correct format and then transmit it via an appropriate communication channel. The source device identity will not be passed as a parameter by the ASM; it will be readily available to the Message Transmitter and as such can be inserted as required. For ease of processing a consistent three field message header has been designed containing the message code and two device identities. This will make it easy during the parsing process but in order to fulfil this, in some cases (for instance WIT, an untargeted request) it has been necessary to repeat the transmitting device identity. For further clarity Figure 6-4 below shows the format of a typical message.



**Figure 6-4. Example of a My Status Is (MSI) message**

The logic associated with the transmit-receive cycle and how this interacts with the Aura is detailed in sections 6.7.3 and 6.7.4.

## **6.5 Policy Manager**

The Policy Manager process controls the creation, maintenance and allocation of the system parameters and locations required to operate the Authentication Aura. When the system is initially activated the ASM will launch the Policy Manager to prompt the user through the allocation of values to the core parameters which are then stored in the Parameters data table. During regular operation of the Aura the Policy Manager process will be required to establish parameter values, reading them from the database and assigning their values to the corresponding variables. These will be held in working memory and used by the ASM and other processes.

### **6.5.1 System parameters**

Upon activation of the system for the first time the user will be presented with a data entry screen displaying the various parameters and their default values, enabling them to make

changes as required. Detailed explanations and associated annotations will be provided for those users who may not fully understand the terms and operational effect that each of the parameters has. Additionally, by presenting the user with this interface it will reinforce its existence to them, allowing them to return at a later date to make appropriate adjustments as and when their comprehension has improved. Upon saving the information, each value will be written in turn to the Parameters data table overwriting any previously stored entry.

There are a number of core system parameters that have been identified at this time which need to be set to enable Authentication Aura operation. In the following paragraphs each of the parameters will be described in turn and a default value for each suggested. These empirical values have been drawn from the undertaken experiment, experience gained during the data analysis and the application of them being a sensible starting position. These values will require thorough evaluation and variations tested to ascertain the full impact of alteration. They are liable to change.

The first system parameter is `authThreshold` and will be used to hold the confidence value at which re-authentication of a user is triggered, should the Authentication Aura's user identity confidence fall below this threshold value. Setting the default value to 20.0 will initially provide the system with a broad window of operation without being too punitive upon the user. The time it will take the system to reduce to this cut off will directly correspond to location, time since authentication and the contribution of confidence gained from other Aura devices.

At specified periods the Authentication Aura will poll the local vicinity for devices and to check if existing Aura members are still within communicable range and active. The variable `auraCheckSecs` will be used to store a value that dictates how often (in seconds) this process is undertaken. At this point-in-time setting the default value to two minutes (120) will provide a reasonable starting point for further investigation. The lower this threshold is set, the quicker the Authentication Aura will respond to changes in location and make up of the active devices in the Aura, leading to a rapid shift in confidence should movement be detected. However, it is worth noting that the more frequent the locale is polled, the greater the power consumption within the device, and so it is imperative that a balance between these two aspects is identified.

Confidence erosion as previously discussed is another key element of an Authentication Aura's operation. Rather than always degrading the confidence in the user's identity second by second or even in conjunction with `auraCheckSecs` it is proposed that this time frame be separately parameterised to provide another granularity of control. To this end the cycle rate will be dictated by `auraDegradeSecs` and will specify in seconds how often the host device's

confidence is reappraised; an initial value for this parameter prior to simulated evaluation is 60 seconds. Once again this value will control the quantity of messages generated by the agent and the amount of continuous processing, helping to prolong battery life in a mobile device.

Operating in conjunction with the above parameter, `periodDegradation` is used to control the amount by which the core confidence in the user's identity is reduced during each iteration of the Authentication Aura. The previous chapter extensively investigated degradation of confidence and illustrated how it could take many forms. As a starting point it is sensible to utilise a straight line degradation prior to further analysis and thus setting this to a value of  $t*2$  will achieve this. This implies that each cycle (default every minute) will erode the core confidence by a value of two, meaning that it will take the Authentication Aura 40 minutes to erode confidence from the maximum value of 100 as shown in Equation 5-5 to the default re-authentication value of 20 held in `authThreshold`. The `periodDegradation` parameter will specify the degradation equation to be applied and will require restriction to a number of options unless a full evaluation and parsing routine is written and applied during validation testing and operation.

During initial operation the Authentication Aura agent will have to go through a period of learning in which it builds its relationship with other devices. `learningMode` is a Boolean variable that will flag this state as either 'true' or 'false' and although initially set to the former, it can be disabled by the user at any time when they are satisfied with the system's operation. When this parameter is set to 'true', as communication is received from an unknown device or the agent finds itself in an unrecognised locale, the system will prompt the user to establish the relevant relationship. This is achieved by entering and saving the appropriate information in the Device data table as outlined in section 6.6.1.

The Authentication Aura agent will continually monitor the communication channels for both targeted and general messages from other active devices. However, if a message is generated by the agent it is necessary to employ a threshold to dictate for how long the system waits for a reply until it presumes the target device is currently dormant. The user amendable `messageTimeout` parameter will hold this value in seconds and control the patience that is exhibited by the agent. Specifying a low value will have the potential effect of blocking contributing devices prematurely whilst too high a value will falsely preserve their contribution to confidence and so it is imperative that a balance is struck. Initially a default value of 30 seconds is proposed although simulation and further analysis is likely to alter this viewpoint.

Coupled with the above parameter is `inactiveTimeout`. This value is used to specify how long a device can remain out of active contact until a message re-establishing its status and details is

required. The stored value will be in seconds although it is suggested that several minutes should be the default, for instance 300 or five minutes. As the agent cycles through it will evaluate each of its known and active devices to assess the last time of communication. If this time exceeds the threshold a message enquiring about the status of the device will be sent and if no reply received, it will be assumed that the device has been removed or deactivated and subsequently deleted from the active Aura. For more detail about this process refer to section 6.7.3.

In the summary of the previous chapter the generalised confidence equation was introduced; Equation 5-5. In this equation the total contribution that can be made by all the token and dumb devices was bounded at a maximum level by variable  $\alpha$ . This value will be specified by the parameter `maxTokenContribution` and with an initial default value of 20 will prevent excessive influence being exerted. The undertaken experiment indicated that these inert pieces of equipment were regularly detected in large numbers and so the potential for bias is clearly evident without the implementation of this threshold.

Extending the concept of confidence contribution and to ensure that the amount of influence is user controllable, the base contributory amounts for each intelligent and dumb device requires parameterisation. Consequentially `intelligentContribution` and `tokenContribution` are proposed to carry these values throughout the system and will be utilised where appropriate. At this time it is suggested that initial values prior to simulation and testing should be 20 and 1 respectively.

The final parameter which has been identified is the default security threshold for application or service activation within the host device, `appSecurityDefault`. During early operation of the agent apps and services will be invoked which will require the user to specify the confidence level at which they are prepared to allow the activation to proceed. This process detailed in section 6.10 will be initially onerous but nonetheless key to the concept of an Authentication Aura. To aid this task `appSecurityDefault` will be used as a default security setting for each newly discovered device and will be a slider controlled numeric value between zero (no confidence) and 100 (total confidence). It is proposed to initially set this value arbitrarily at 80.

### **6.5.2 System parameters data table (param)**

Having introduced the system parameters in the previous section it is necessary to discuss how the information will be stored. Although it would be possible to use a data table with a single row that would contain the parameter values within a set number of columns, constructing generic storage which has a separate row for each of the values ensures future proofing and easy system expansion or alteration. To this end, the System Parameters data table shown

below (Table 6-6) has been designed with only three columns. The key field (param\_key) will not serve any significant role in the table but has been included for completeness, param\_field\_name will be used to store the variable name of the parameter held within each of the particular table rows, and param\_field\_value the corresponding value.

param_key	param_field_name	param_field_value
3	authThreshold	20
6	inactiveTimeout	300

**Table 6-6. Extract from the System parameter data table**

During system start up the Policy Manager will be invoked by the ASM to initiate the respective parameters. To achieve this, the process will proceed to loop through each row within the table and by evaluating the param\_field\_name allocate the respective value.

### 6.5.3 Location data table (location)

An additional function of the Policy Manager is to provide an interface through which the user can administer the Location data table. It has already been established how vital the current location of the device is when administering the user's Authentication Aura and their associated identity confidence. During the discussion in the previous chapter that investigated the importance of location (see section 5.3) it was proposed that the system defaulted to using three locations 'Home, 'Work' and 'Away'; this table is employed to hold details of these locations with associated security parameters.

Table 6-8 on page 121 illustrates the design of the Location data table and indicates that similar to the system parameters table it consists of only three columns location\_key, location\_name and location\_multiplier. Defining the storage in this way provides the opportunity to extend the discussed defaults (Home, Work and Away) with the inclusion of additional locations with varying security profiles at a later date. For instance, a user might create an entry for a friend's house, a location in which they want their Aura to operate differently and this approach allows the easy incorporation of this new locale.

Field name	Description	Type	Length	Details	Example
param_key	Key field	Integer	n/a	Auto increment	2
param_field_name	Parameter field name	Text	30	Name of the parameter	authThreshold
param_field_value	Parameter field value	Text	20	Value of the parameter – un-typed to allow flexibility. Therefore validated during input.	15.0

Table 6-7. System parameter data table definition

Field name	Description	Type	Length	Details	Example
location_key	Key field	Integer	n/a	Auto increment	1
location_name	Name	Text	30	Allows the user to describe or name the location	Home
location_multiplier	Multiplier	Float	3	Number in range 1..10 which signifies how secure the environment is regarded to be	2.5

Table 6-8. Location data table definition

Upon system installation the data table will be populated with three rows and as such will appear as shown below in Table 6-9.

<b>location_key</b>	<b>location_name</b>	<b>location_multiplier</b>
1	Home	2.5
2	Work	5
3	Away	10

**Table 6-9. Example of the Location data table at system installation**

The default values contained in the column `location_multiplier` have been drawn from the investigatory experiments discussed previously and are used in the calculation of the confidence coefficient as illustrated in Equation 5-5. It reflects the ease that a user feels when operating their device in a particular location; the lower the value, the more at ease the user is and the lower the perceived security risk. Manipulation of these values affects the rate of decay of the confidence over time, which in turn will alter the length of time that particular services and applications remain available to use.

It could be argued that the data within this table is another set of parameters and as such should be held within Parameters. However, in order to support processing performance and maintain the degree of flexibility necessary to future proof, it has been deemed prudent to separate this table to stand in its own right.

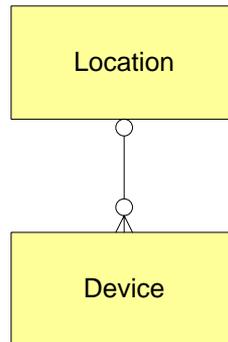
## **6.6 Device Manager**

The Device Manager process fulfils two roles within the administration of the Authentication Aura: firstly, when the learning mode parameter is set (see section 6.5.1) it will act to populate the Device data table with newly discovered items of equipment, and secondly it will provide an interface via which the user can manually update, annotate and maintain existing device records which are already held. In this instance it is worth introducing the structure of the main data table used by this process first, so an understanding can be imparted prior to the explanation of the process' intricacies.

### **6.6.1 Device data table (device)**

The known devices data table (`device`) is a key element in the successful functioning of the Authentication Aura agent. It is used to store and hold the details of all pieces of trusted electronic equipment that can operate within an active Aura and controls which devices will be able to contribute to the confidence calculation. Each row of the table consists of nine columns as shown in Table 6-10 on page 124. Although `device_key` is the table key, `device_id` will be the primary search field. The `device_id` column will store the unique identification code of each

individual piece of equipment, providing a look-up route via which the appropriate record can be retrieved as communication is received. This field is read only and cannot be entered or amended by the user.



**Figure 6-5. Relationship between the device and location data tables**

As Figure 6-5 above indicates there is a non-compulsory parent-child relationship that exists between entries in the Device table and locations because each Device may or may not be statically resident in a single particular Location.

The implication of this is that each Location may have one, several or no devices located within it, and any one can therefore be used to identify that locale. To achieve this device\_location\_key is used to maintain the link when it exists by holding the corresponding value of the associated location. In the event that the device is mobile and may therefore move between different locations, this field will be left blank.

The device\_name column is a freeform text field that permits the user to annotate the device record with a personally meaningful description. This data is used for no other purpose than information display and an aide memoir.

device\_block is a Boolean flag that allows the user to withdraw a device from contributing to the Aura. For completeness, deletion of records from this table is not permitted and so providing a means by which devices can be barred is clearly necessary. The default for this field is false and so unless altered each newly recognised device will immediately become part of the active Aura once the record has been saved.

Field name	Description	Type	Length	Details	Example
device_key	Key field	Integer	n/a	Auto increment	1
device_id	Unique identity code	Text	50	Character string used to identify device. i.e. machine identity code or similar	00037A964637
device_location_key	Location key field	Integer	5	Provides the child parent relationship with the Location data table	2
device_name	Name	Text	30	Device name or description that reminds the user which device is which	Work mobile phone
device_block	Block device	Boolean	1	A field that provides the user with the ability of blocking a device from being an active member of the aura. Default value 'False'	False
device_type	Type	Text	1	Indicates if the item of equipment is a device 'D', Infrastructure 'I' or Other 'O'	D
device_intelligence	Intelligence	Text	1	Differentiates between devices that are Intelligent and can authenticate (I) and those that are dumb and cannot (D)	I
device_rank	Rank	Integer	1	Range 1..9. An integer that indicates how significant the contribution that any device gives to the overall aura confidence.	5
device_owned	Owned	Boolean	1	Specifies if the item of the equipment is owned or whether it belongs to a colleague or acquaintance.	True

Table 6-10. Device data table definition

It is necessary to be able to distinguish between items of infrastructure, intelligent devices and dumb pieces of equipment. This is achieved by the use of two fields, `device_type` and `device_intelligence`. The first is set to 'D' to indicate a device, 'I' which will identify an item of infrastructure or 'O' for other. Although 'O' will not be used often it has been included to provide a catchall for items of equipment that the user feels does not fit the description of being a device or infrastructure. For devices, the second field (`device_intelligence`) will hold 'I' for intelligent devices and 'D' for those that cannot authenticate and are therefore regarded as being dumb. Items that have been specified as 'other' will always be treated as dumb and therefore unable to authenticate.

`device_rank` is used to control a device's contribution. This integer value in the range between one and nine indicates which devices have high significance and will contribute more to the confidence calculation. One will indicate devices that are highly significant and therefore contribute most, whilst nine is reserved for equipment that has the least significance. Rather than presenting the user with a numeric value which is potentially confusing, it is likely that during development a graphical slider is utilised to mask the underlying numeric tariff.

The final column, `device_owned`, is a Boolean field that specifies whether or not the detected device belongs to the user or if it is the property of a colleague or acquaintance. Only intelligent devices that are owned can dynamically contribute to the Aura, those that belong to other people can only be utilised as tokens.

### 6.6.2 Device discovery and validation

By monitoring the Message Cache the ASM will identify equipment detected for the first time in the current session and pass each of these for validation to the Device Manager process. If the Aura is operating in learning mode and an unknown device or piece of infrastructure is identified, a prompt alerting the user to the presence of this newly discovered item will be issued and the user placed in data entry mode on the device information screen. Upon display of this data entry form the appropriately system populated `device_id` will be shown and the user will then be able to fill the remaining information and save the record when complete.

If however the device is already present within the Device data table the Processor Manager will locate the appropriate record, check to confirm that the `device_block` flag is set to false and report its findings back to the ASM. For completeness and clarity a flowchart outlining the sequence of these events is shown in Figure 6-6 below.

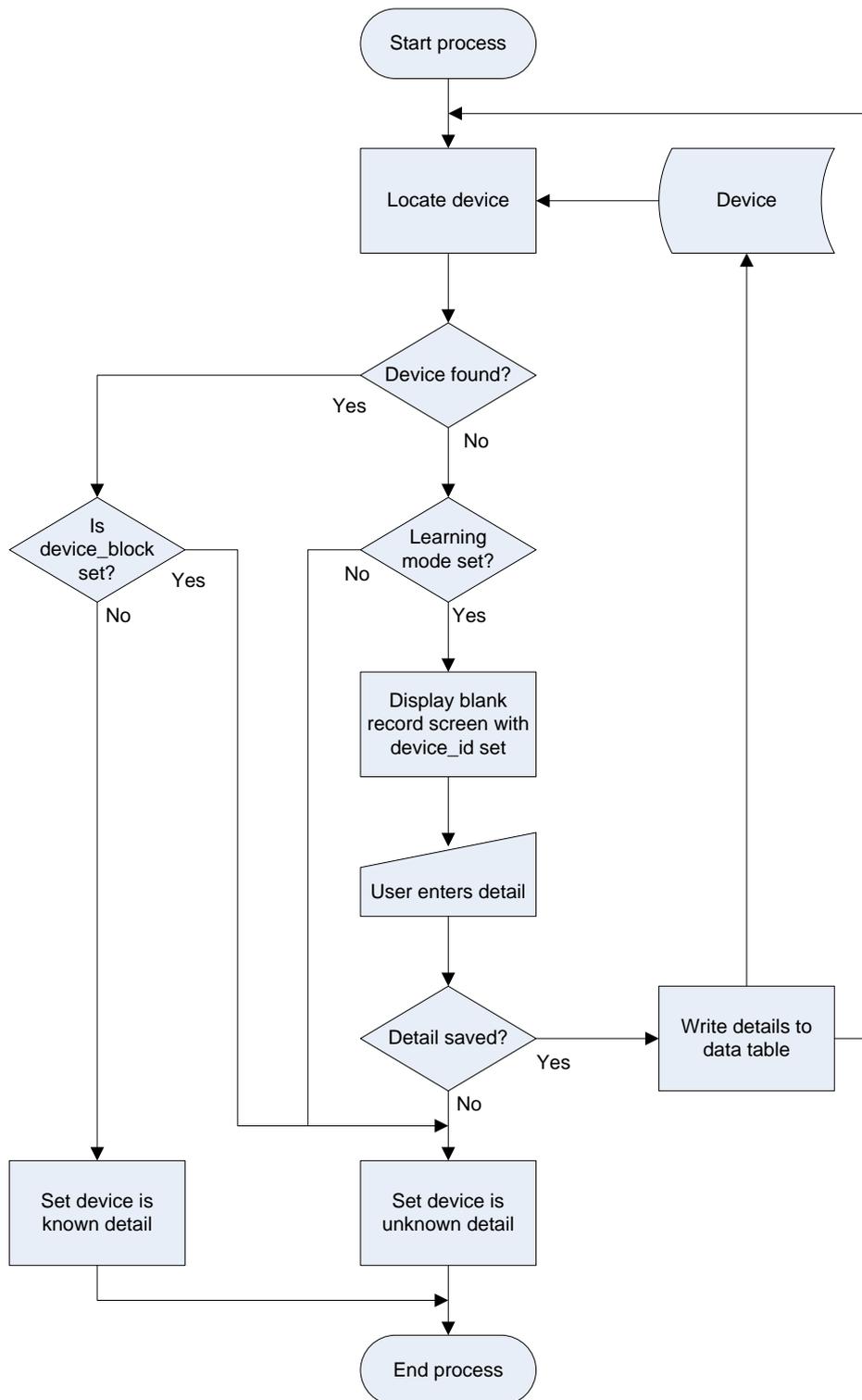


Figure 6-6. Device Manager flowchart

### 6.6.3 Device maintenance

It is important to note that the user will be able to gain direct access to a list of devices and then to the device detail screen to amend information held or for instance set the device\_block indicator. This will be achieved via a system administration function within the Device Manager.

## 6.7 *Aura Manager*

The Aura Manager is one of the most intricate processes and administers the Aura data table in which the details of all devices currently active within the Aura are held. In unison these rows will provide the detail necessary to calculate the current device's status and provide the information upon which the Confidence Monitor (detailed in section 6.8) operates.

Two functions are incorporated in this process: to update and maintain the Aura members' status from messages that the ASM gathers from the Message Cache and passes on to the Aura Manager, and to compile a list of messages that need to be generated and transmitted. However, before the logic of these two functions is fully detailed the structure of the Aura data table will be described.

### 6.7.1 **Aura data table (aura)**

Forming the core of the agent's operating potential, the Aura data table is also temporary storage (non-permanent - created and held in memory during runtime) and is used to hold the details of all devices that have been detected during the current session. It provides all the information required to perform the intricate calculation of the Aura's confidence contribution, as well as maintaining details of messages sent to and received from other Aura devices. It represents the active Aura.

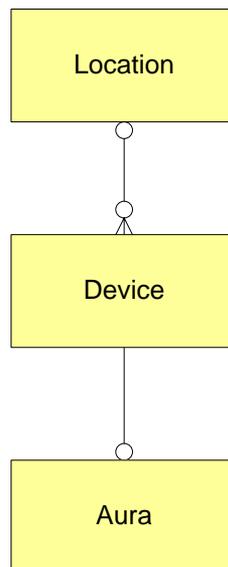
The columns contained within the Aura data table are shown in Table 6-11. `aura_key` is the key field and will be automatically incremented upon creation of a new record. It has been included in the data table design for completeness and will not actively be used within the Authentication Aura Agent's operation.

There is a relationship between this table and the Device data table, although it is more restricted than the previously discussed relationship between Location and Device; in this instance every Aura record must be linked to a specific Device record but not every device will be present in the active Aura (illustrated by Figure 6-7). As such, `aura_device_key` is used to store the key field value of the Device table and therefore establishing a one-to-one relationship between the two. That is, each and every entry in Aura must be linked to a recognised and active (`device_blocked` is false) device.

Ongoing communication between devices and information requests need to be tracked which is achieved by the use of the `aura_status` column. This is a five character text field which holds a short code signifying the current relationship between the agent and any of the devices within the Aura. A full status state diagram is shown later in section 6.7.4 which follows a detailed discussion of each valid command and how the status of the target device is affected.

Field name	Description	Type	Length	Details	Example
aura_key	Key field	Integer	n/a	Auto increment	1
aura_device_key	Device key	Integer	5	Field that provides a join to the Device table.	7
aura_status	Status	Text	5	Status of the device within the aura which is used to manage communication and control which actions have taken place. Passive devices hold status of 'dumb'.	ayt
aura_last_authenticated	Last authentication	Date	20	Date and time in internal format of the last authentication performed by the device. For passive devices this field will remain empty.	17684936632
aura_authentication_level	Authentication level	Integer	1	Indicator in range 1..5 which signifies how secure the method of authentication was.	3
aura_rank	Rank	Integer	1	Range 1..9. An integer that indicates how significant the contribution that the device gives to the overall aura confidence.	8
aura_last_update	Last update	Date	20	Date and time in internal format of the last time an aura member had an alteration made to its details.	23467363535

Table 6-11. Temporary Aura data table definition



**Figure 6-7. Relationship between the location, device and aura data tables**

The next three columns of this data table are used to record the information transferred between devices during the communication process. `aura_last_authenticated` is utilised to store the date and time that the member device last carried out an authentication process and is held in an internal clock format.

In addition to the date and time, `aura_authentication_level` will indicate how secure the authentication process was. This is specified by an integer in the range between one and five, one being the most secure and five the least; this will be directly supplied from the transmitting device during communication.

`aura_rank` is the penultimate column in the aura data table and is once again an integer in the range one to nine. This data field is used to indicate how significant the communicating agent is, the lower the value the more significant the device is deemed to be. There are some instances when some entries in this data table will be made for dumb entities incapable of data communication. For example, in the case of items such as a contactless credit card which can be sensed and indeed whose presence is potentially highly significant, will carry a low `aura_rank` tariff but will be unable to communicate this fact. All devices where `device_intelligence` is set to 'D' will operate in this way.

The final field in the aura table is `aura_last_update` which is used to store the date and time that any Aura member's details were updated by the system. This information is used to ascertain when devices have become inactive or left the Aura and so it plays a vital role in the agent's operation.

### 6.7.2 Received messages

The message lexicon was detailed earlier in Table 6-4 and all but the ARR (Authentication Request Reply) and ARQ (Authentication ReQuest) receipts will be processed by the Aura Manager; these two specific messages will be dealt with appropriately by the ASM and subsequently the Authentication Manager, in isolation.

When communication is received from a device, the Aura Manager splits the message into its constituent parts and then checks to ascertain if the communicating device is already present and active in the Aura. If it is present, the appropriate row within the data table is updated with the details received and when appropriate a reply message will be invoked. However if it is not present, its trust is established by the Device Manager via its existence in the Device data table (as discussed previously in section 6.6) and upon successful location, a record is then appended to the Aura record set. If the device is unfound and therefore not trusted, the message will simply be ignored.

### 6.7.3 Message processing

This section will describe the precise logical sequence invoked by each of the messages in turn. Some are incorporated with others as they are an automated reply response and so will be dealt with under a single heading. Each of the following diagrams illustrates a flowchart that occurs across two devices and the communication channel. The source device transmits ONE message via the syntax shown in the communication channel and the target device then either accepts this message type from ANY device or FILTERs only the messages specifically targeted at it. Processes on the target device then update the Aura table appropriately and generate responses when required.

#### 6.7.3.1 *Authenticated (AUT)*

This message is transmitted from a device immediately following the successful completion of an authentication by the user.

AUT is untargeted and should therefore be collected and processed by any listening device. If the source is unknown it should be added to the current aura membership list with a status of 'new'. All relevant authentication details should then be applied to the source's Aura record, be it new or an existing Aura member.

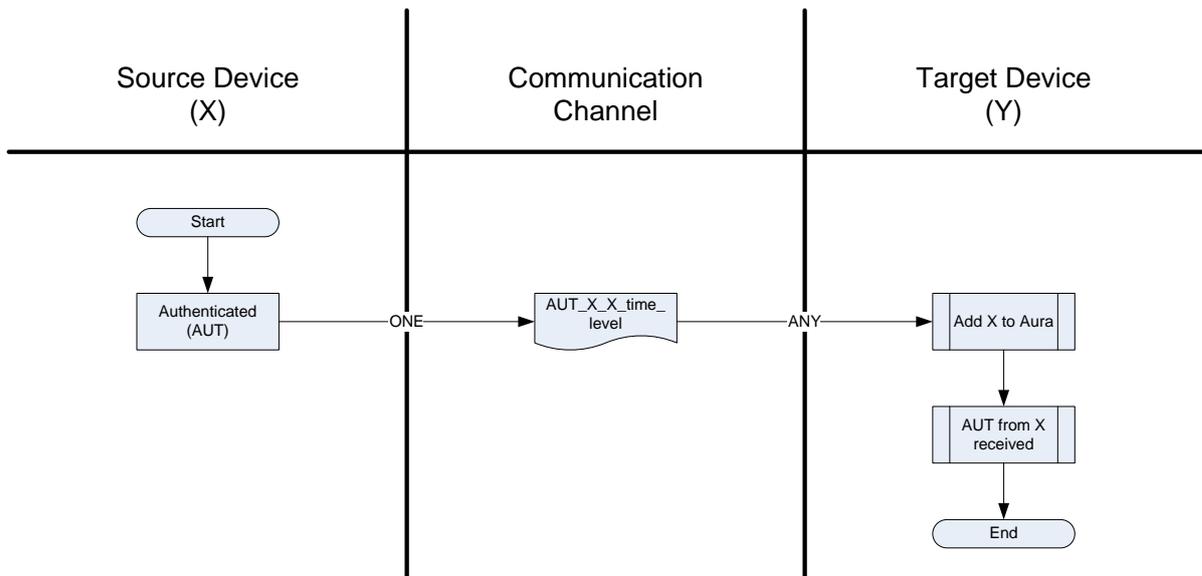


Figure 6-8. Authenticated message syntax and effect (AUT)

6.7.3.2 Are You There (AYT) and I am Still Here (ISH)

When an aura member has not been in communication with a device for a period of time an AYT message may be issued to establish whether or not the target is still present and active. AYT is targeted specifically at an existing aura member. After it is sent a reply is always expected from the target. If one is not received the target should be flagged by the sender as having left its Aura.

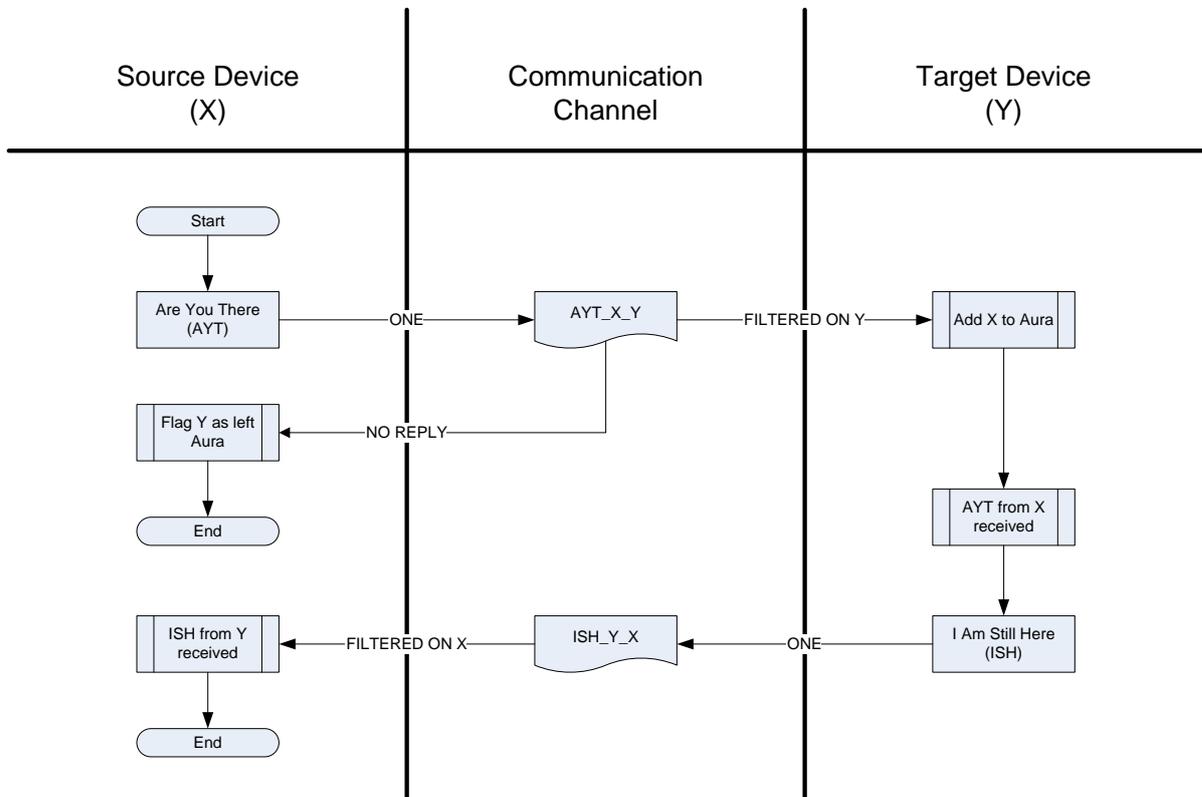


Figure 6-9. Are You There message syntax and effect (AYT)

Any listening device should only pay attention to AYT messages directed specifically at them i.e. when a device receives an AYT it should filter out and discard those where the target identity does not match its own identity. Upon legitimate receipt, the receiver will add the source to its Aura with a status of 'new' (if appropriate) and then issue an 'I am Still Here' reply. This will then be appropriately interpreted by the corresponding receiving device.

### 6.7.3.3 I Am Here (IAH)

An IAH message is transmitted when a device is first activated or in response to a WIT request. IAH is also untargeted and should be collected by any listening device. Upon receipt, if unknown by the receiving device, the sender is added to the current aura membership list with a status of 'new'.

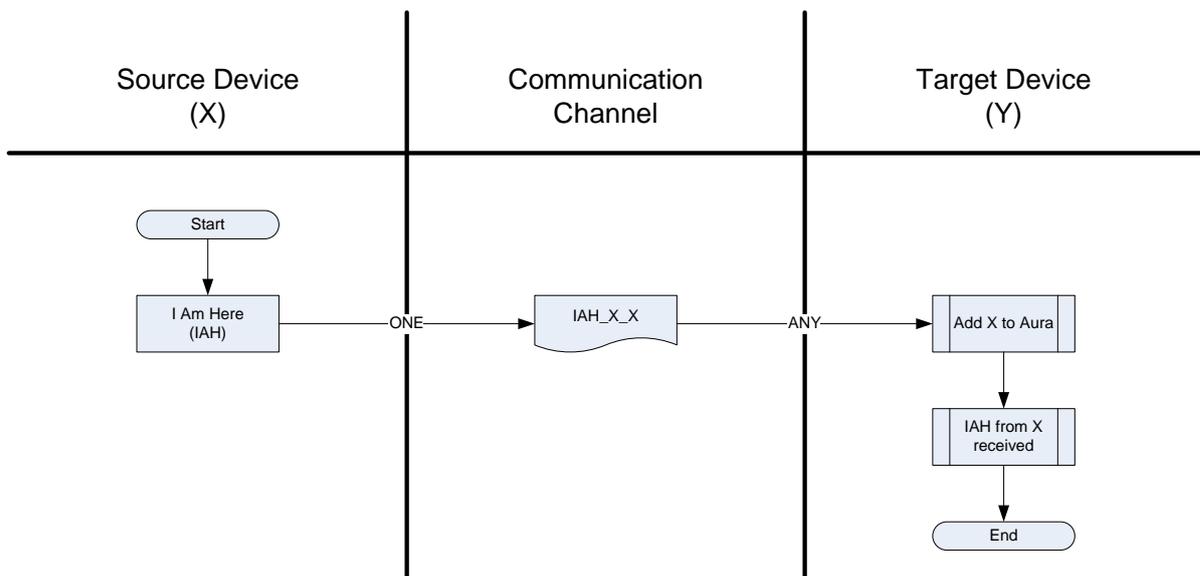


Figure 6-10. I Am Here message syntax and effect (IAH)

### 6.7.3.4 Who Is There (WIT)

Upon activation an untargeted WIT message is issued to any devices that may be listening to establish which Aura members are active and within communicable range. A WIT message is untargeted and should therefore be received and duly processed by any listening devices. Upon receiving a WIT request it should firstly add the source device's identity to its Aura membership if it is absent and then reply by issuing an 'I Am Here' (IAH) reply. IAH is an untargeted response and will then be handled appropriately as shown previously in Figure 6-10.

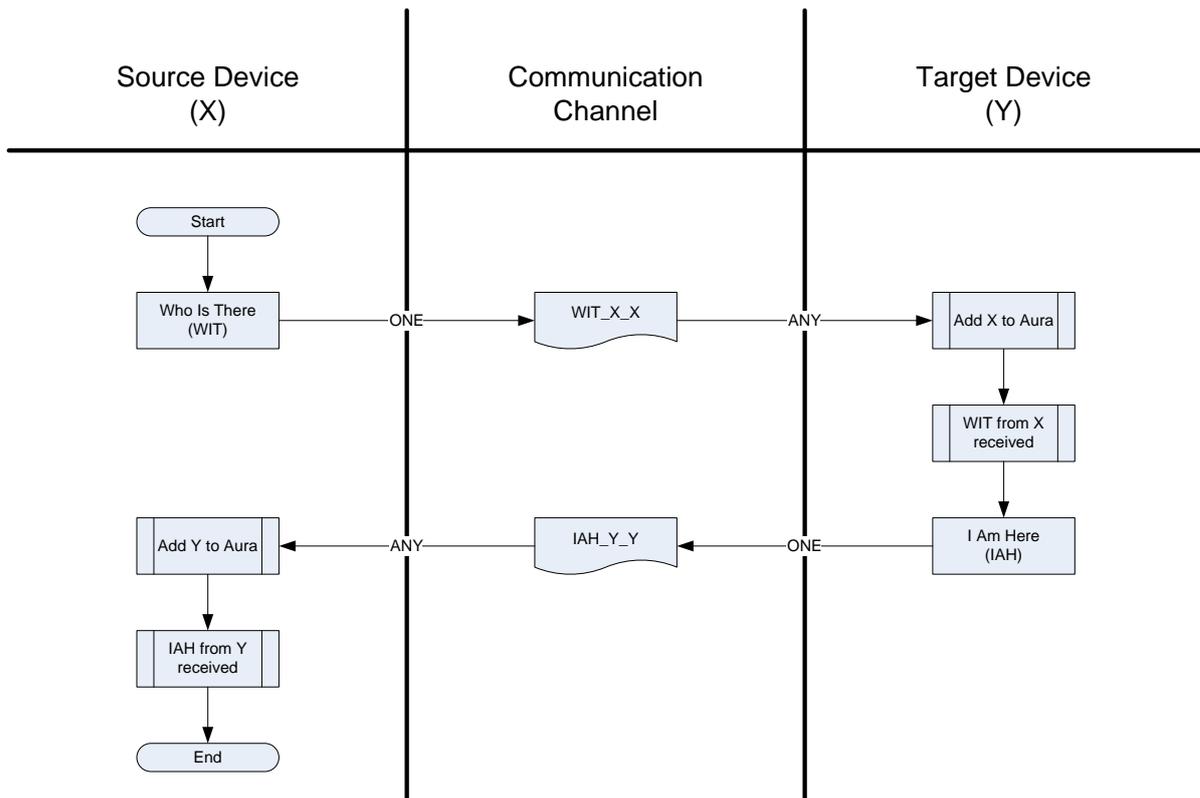


Figure 6-11. Who Is There message syntax and effect (WIT)

#### 6.7.3.5 What is Your Status (WYS), My Status Is (MSI) and PENDING (PEN)

The WYS message is the most complicated that is utilised by the ASM. It is issued when the system needs to acquire the current status of an existing active Aura member. Thus, it is a targeted message that without a timely response (governed by the messageTimeout parameter – see section 6.5.1) will be interpreted as indicating that the corresponding device has become inactive or left the aura.

Upon receiving a WYS an agent will initially update its Aura to reflect the presence of the source. Following this process, it will react differently depending if it has authenticated its user or not. If the current user is authenticated a MSI reply is issued containing details of the last authentication. However, if the user has not currently been authenticated a message indicating this pending status (PEN) will be transmitted instead. With confidence being drawn from Aura members, it is possible that a device may be operating legitimately without having specifically confirmed the user's identity via authentication. As such, the PEN message relays this status allowing the receiving device to utilise it as a token rather than an intelligent contributor.

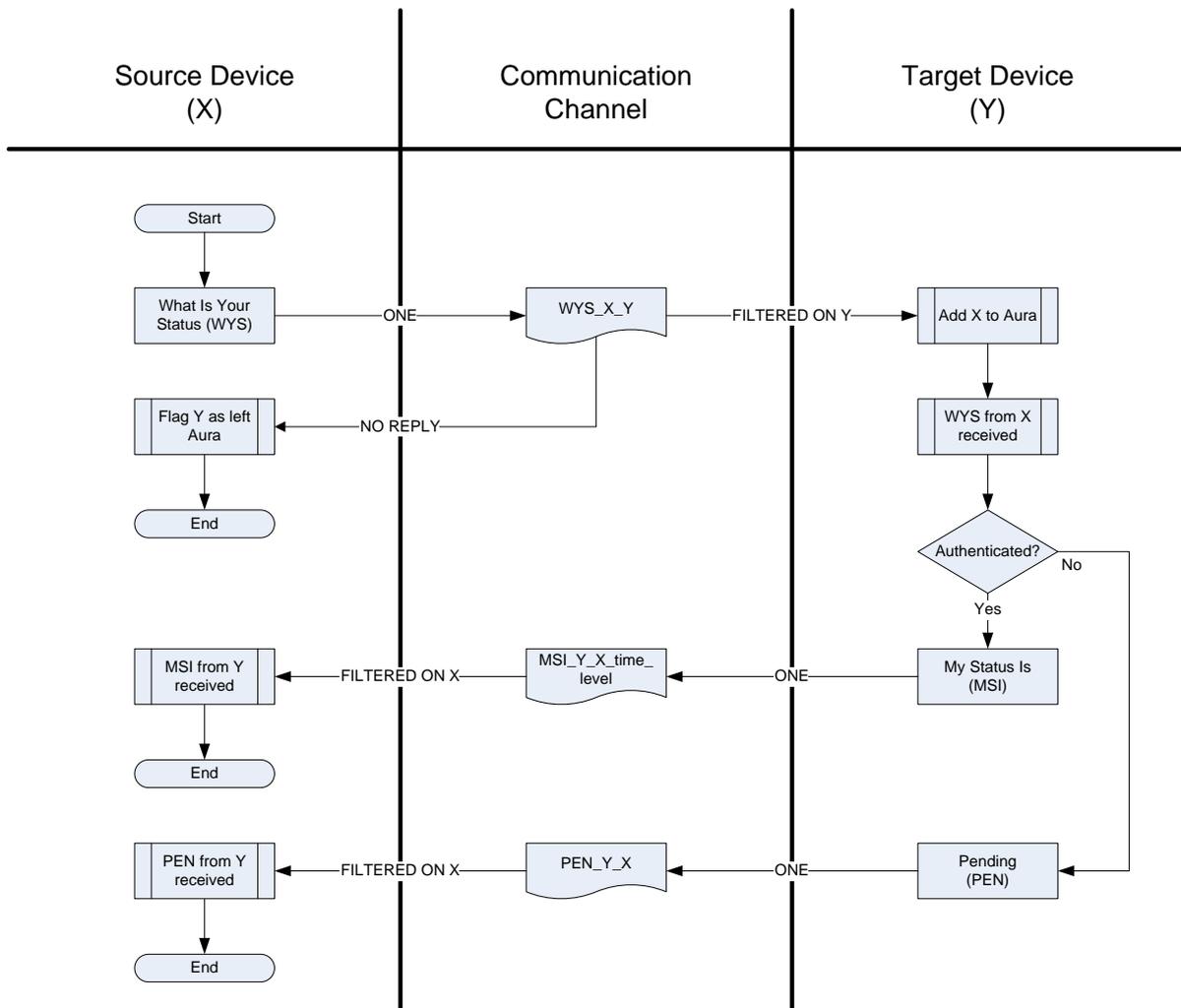
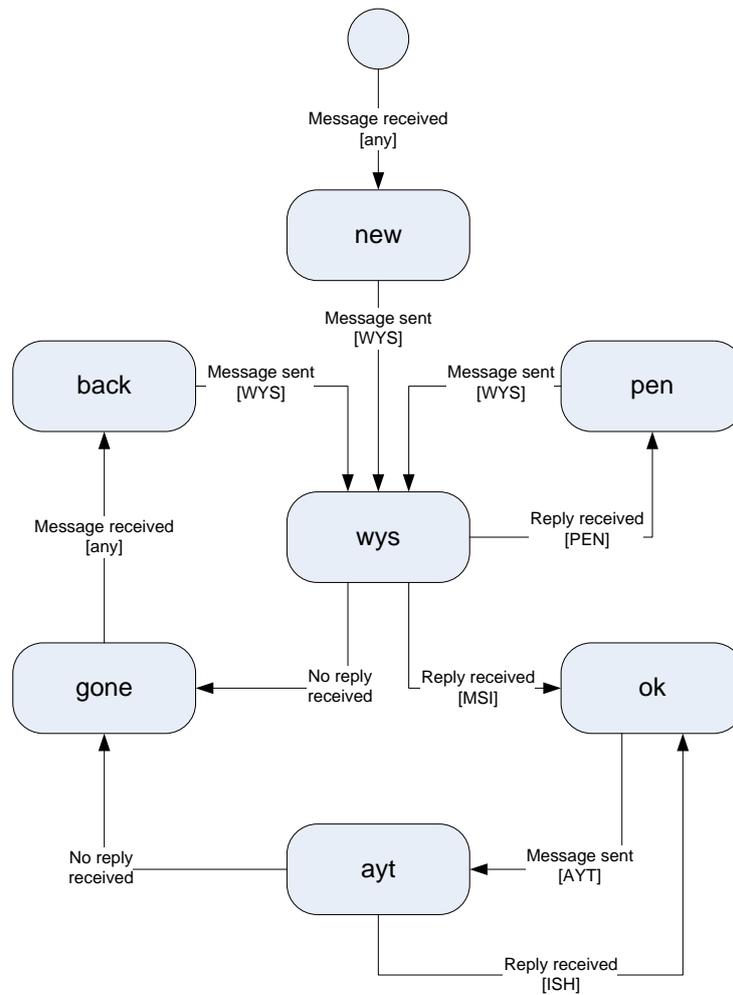


Figure 6-12. What Is Your Status message syntax and effect (WYS)

#### 6.7.4 Member status

As intelligent members of the Aura communicate with each other the status of each will be amended within the Aura table to reflect received messages or requests that have been made. In Figure 6-13 below, the state chart graphically illustrates how the status of the Aura members change during the agent's operation, summarising the effect of the messages discussed above.

In this diagram the associated message that triggers each change in status is encapsulated in square parentheses '[' ]' below the action description, i.e. the status of an Aura member is altered from 'new' to 'wys' when a WYS message is transmitted to that particular member. With the Aura table being temporary, when the host device is activated the system commences with an empty Aura and polls the listening community to establish which known and trusted devices are near and active. When a reply is received and a device is detected it becomes part of the Aura and constantly remains so until the host is switched off. This is illustrated by the diagram being closed, without any exit points.



**Figure 6-13. Aura member status state chart**

When communication fails between devices the status is set to 'gone' indicating the target is no longer active, however during operation the Aura agent will periodically re-poll these devices, enabling them to become active again if they return within range.

### 6.7.5 Generated messages

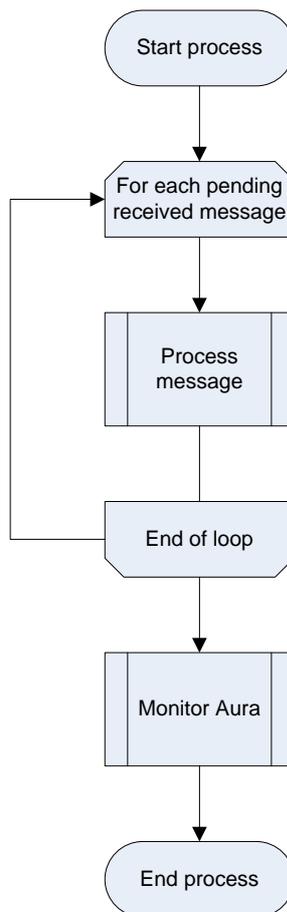
During regular processing checks will be performed to maintain the Aura's membership and ensure the continuing presence and activity of devices. This repetitive housekeeping will be undertaken by the Aura Manager and where appropriate a list of required messages to ascertain the current situation will be generated. Additionally as demonstrated above, some messages require an immediate reply and so these will also be appended to the list in readiness.

At the end of processing the Aura Manager will return the list to the ASM where the requests will each be processed and passed to the Message Transmitter for dispatch.

### 6.7.6 Aura Manager logic

The previous sections have introduced the syntax of the messages utilised to relay information between Aura members, how one message can trigger a response and the members' status categories that are held within the Aura table.

To gain a more complete understanding of the logic used within the Aura Manager comprehensive flowcharts have been formulated to diagrammatically show how each message is processed, the generation of response messages and how the details within the Aura table are maintained. The highest level of these is shown below in Figure 6-14.

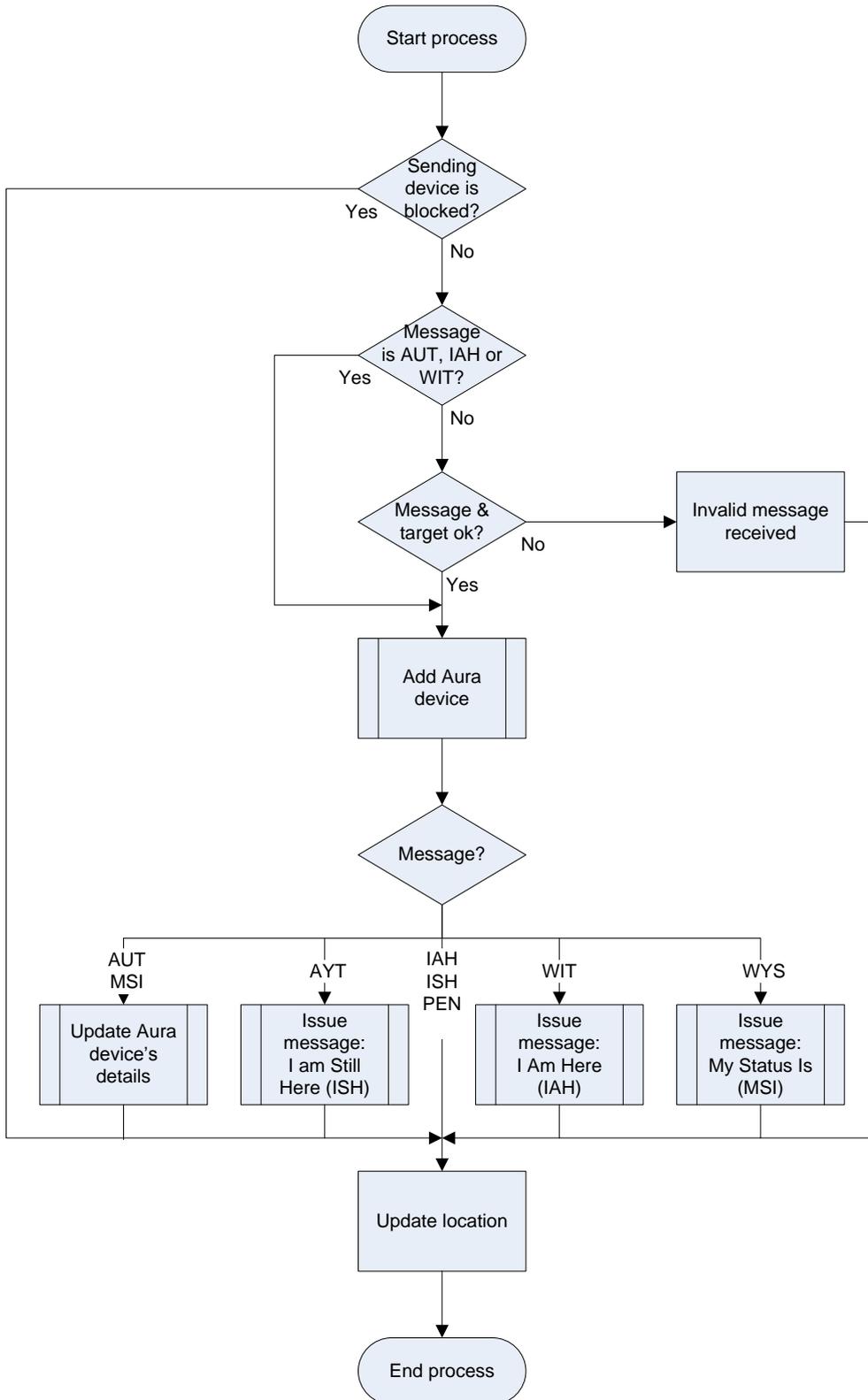


**Figure 6-14. Aura Manager operational overview**

As messages are received by the Sensor they are parsed, filtered and placed into the Message Cache data table for processing. When the Aura Manager is invoked by the ASM it deals with each message in turn, passing it through a Process Message sub-process which updates relevant information and generates any required responses. Upon the finalisation of message processing the Monitor Aura function is called perform any required housekeeping. The by-product of this function is the production of a compiled list of transmission requests which are then returned to the ASM for action.

### 6.7.6.1 Process Message sub-process

The flowchart for this procedure is shown below in Figure 6-15.



**Figure 6-15. Process Message sub-process flowchart**

The first step the sub-system takes is to validate that the transmitting device is known to the host by being present in the Device database and active by having the associated device\_block

flag set to false. The next step is to validate the code of the message received and where appropriate check that it has been targeted at the host device. If the message fails this validation it is deemed to be spurious and simply discarded. Once these tests have been passed a further sub-process (Add Aura device) is called which updates the status of the device within the maintained Aura table, explained in detail in the next section.

For messages AYT, WIT and WYS a transmission message is generated and added to the list to be returned to the ASM; for AUT and MSI the sending device's authentication detail and status in the Aura data table are updated, otherwise no action is taken.

Finally, as the messages are processed the current location of the device is monitored and updated. Upon activation of the sub-process the location is set to a default of the Location record with the highest location\_multiplier value, that is, the least secure and un-trusted location. As each message is processed and a device recognised, the procedure identifies the device with the lowest associated location\_multiplier value and sets the associated memory held variable accordingly. This variable will then be used in the calculation of the host device's confidence.

#### **6.7.6.2 Add Aura Device sub-process**

The Add Aura Device sub-process is invoked frequently throughout the system to ensure the aura membership is accurately maintained. The flowchart for this process is illustrated in Figure 6-16.

When activated the unique identity of the communicating device is passed as a single parameter to the routine. This value is then checked to ascertain if it is already present in the Aura data table. If it not present and therefore a new device, the routine appends a row to the data table, sets aura\_status to 'new' and allocates the current date and time to aura\_last\_update. Conversely, if the identity is found to exist, the procedure checks various statuses or if the device is dumb, and depending upon current values, it makes the appropriate amendments. If a change is made at any point aura\_last\_update is appropriately updated.

#### **6.7.6.3 Issue Message sub-process**

This sub-process as shown in Figure 6-17 is reasonably short when compared with some of the other discussed processes.

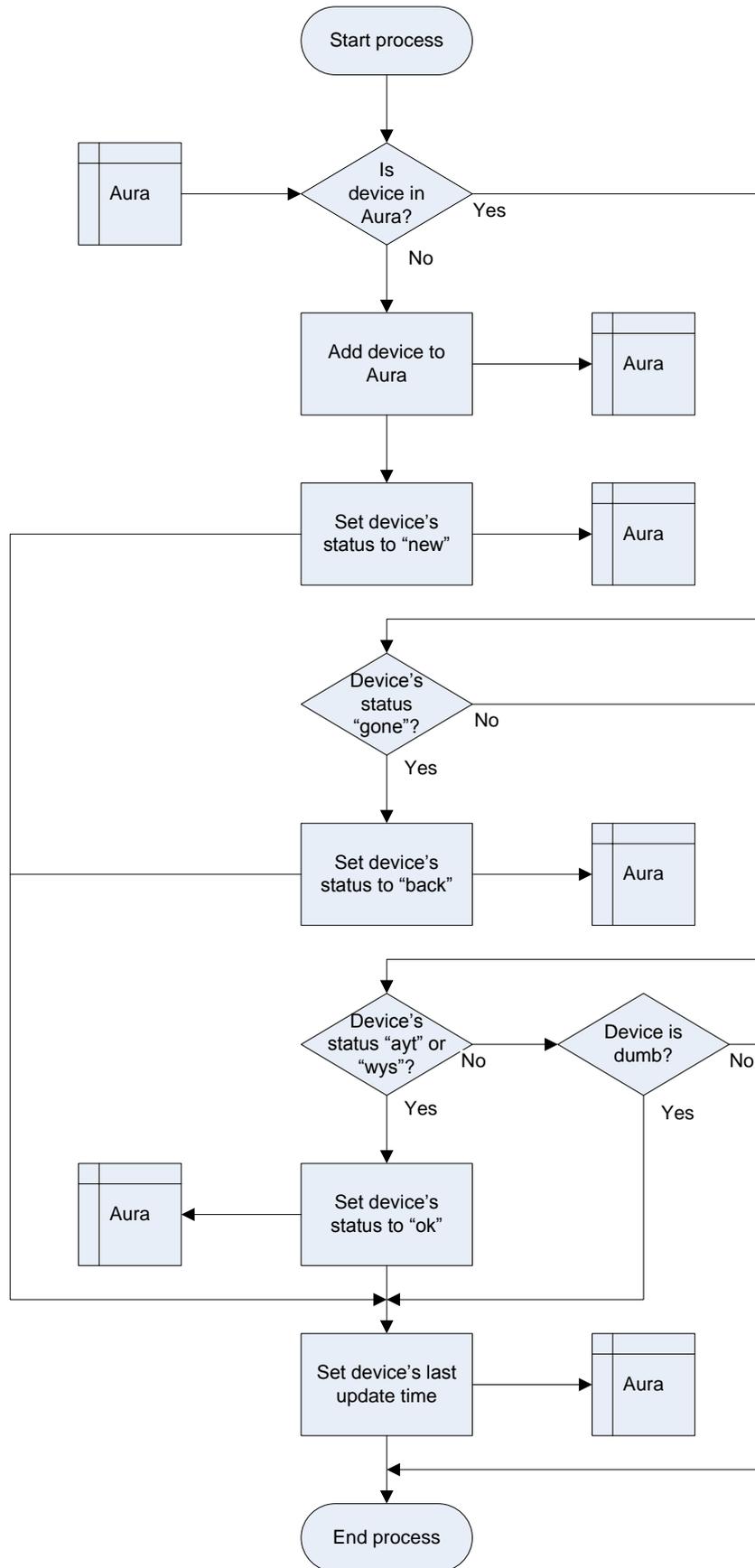
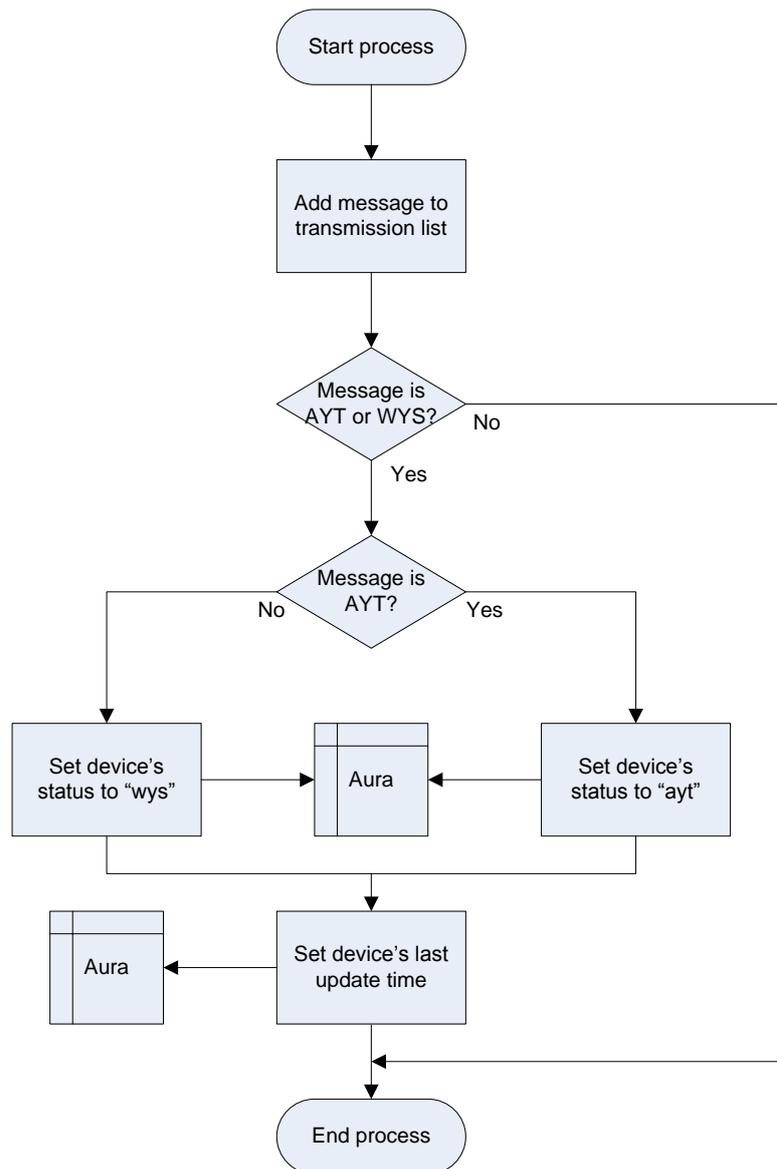


Figure 6-16. Add Device sub-process flowchart



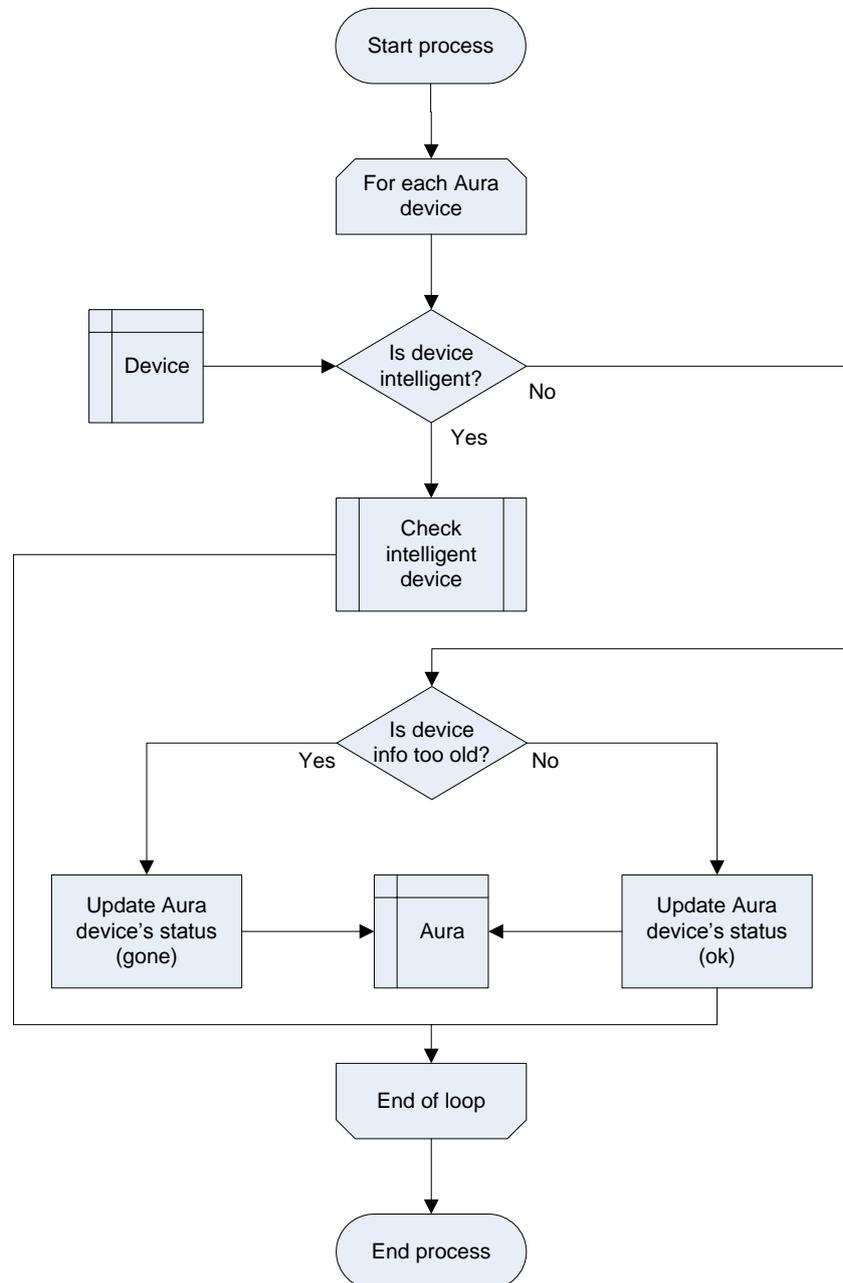
**Figure 6-17. Issue Message sub-process flowchart**

When it is called the appropriate message request is added to the maintained list in preparation for transmission. If the message is either 'AYT' or 'WYS' the aura\_status column is set to reflect the appropriate message and aura\_last\_update is updated with the current date and time value. If however the message is not one of these two, the sub-process simply passes control back to the calling routine without taking any further action.

#### **6.7.6.4 Monitor Aura sub-process and Check Intelligent Device sub-process**

In these two interlinked sub-processes, parameterised values are used to assess when an Aura device's details have remained unchanged for a significant period of time, and when a request for information has been sent and the reply is overdue. Within the Monitor Aura sub-process the system loops through the Aura table and firstly checks if each device is intelligent or not. If the device is intelligent a further subroutine (Check Intelligent Device) is called, otherwise for dumb devices the length of time since it was last observed (aura\_last\_update) will be assessed

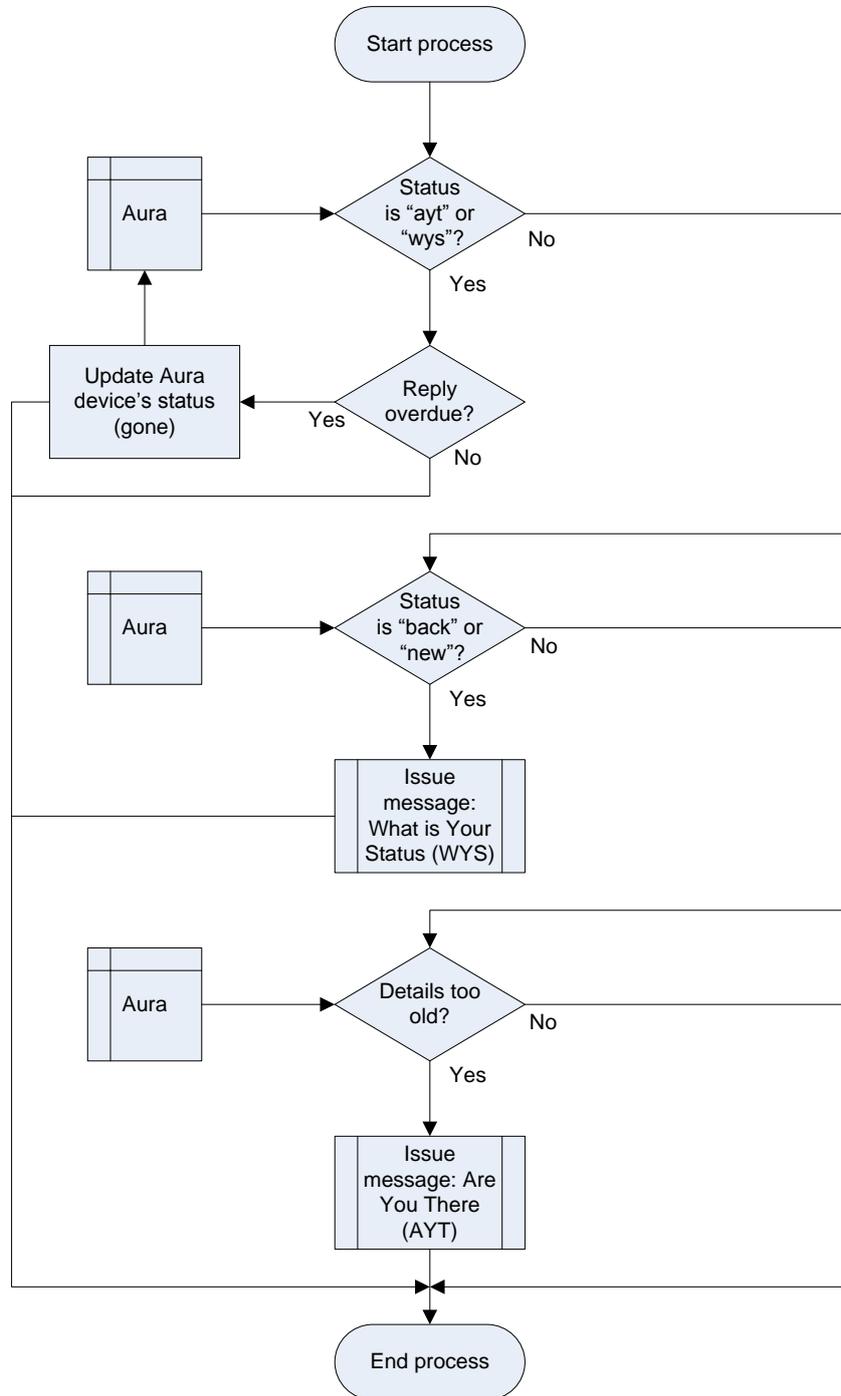
to ascertain if it is still significant. This is achieved by comparing the time between `aura_last_update` and the current time with the parameterised threshold `inactiveTimeout`. If the difference is greater than the threshold the status of the dumb devices is marked as 'gone', if not it is set to 'ok' and the device continues to contribute (summarised as "Is device info too old?" in the flowchart below).



**Figure 6-18. Monitor Aura sub-process**

The treatment of intelligent devices in Check Intelligent Device is more complex as shown below in Figure 6-19. The procedure initially validates the device's status (`aura_status`) to decide whether or not a request for information has been sent and a reply is due. In this scenario the status will either be 'ayt' or 'wys'. If a reply is expected but it is overdue (the

difference between `aura_last_update` and the current time, compared with a parameterised threshold) the Aura device is assumed to have left the Aura and thus the status is set accordingly to 'gone'. However, if the reply is deemed not to be overdue the table row is left unaltered.



**Figure 6-19. Check intelligent device sub-process**

If a reply is not expected the system then checks to see if the device is either a new member of the Aura or it has recently returned and become active once again (`aura_status` will either be 'new' or 'back'). If either of these two criteria is met the process needs to gather the current

---

authentication details from the device, and so a What is Your Status (WYS) message is issued to engender a reply with the required information. Accordingly `aura_status` will then be set to 'wys'.

Conversely, if a reply is not expected, the routine verifies the amount of time since the table row was last updated, to determine if the device should be contacted to confirm it is still active and within communicable range. If this is the case, an Are You There (AYT) message is issued.

## **6.8 Confidence Monitor**

When authentication is completed by the user on the host device, a core confidence level is set and remains unaltered until the Confidence Monitor procedure is called by the ASM at intervals dictated by `auraDegradeSecs`. The initial step the routine takes is to reduce the core confidence based on the authentication method, location and time since authentication was undertaken in accordance with the confidence equations outlined in chapter 5.8.

It then continues by examining each active device within the Aura and totals the amount of confidence that each category (intelligent and dumb) contributes. If a smart device is encountered that has a status indicating that it is pending an authentication ('pen') or has been sent a request for information ('ayt' or 'wys'), then it is treated as being a dumb device. That is, merely its presence will be treated as being significant and it will contribute a percentage toward the confidence based upon `device_rank` rather than the full active intelligent contribution. As discussed earlier in this chapter, intelligent devices will contribute an unlimited amount of confidence, whilst dumb devices will be capped at a threshold value in accordance with Equation 5-5. The specifics of this process are illustrated in Figure 6-20. Once the user's identity confidence has been calculated control is passed back to the ASM where it is used during service activation to establish if re-authentication should be triggered.

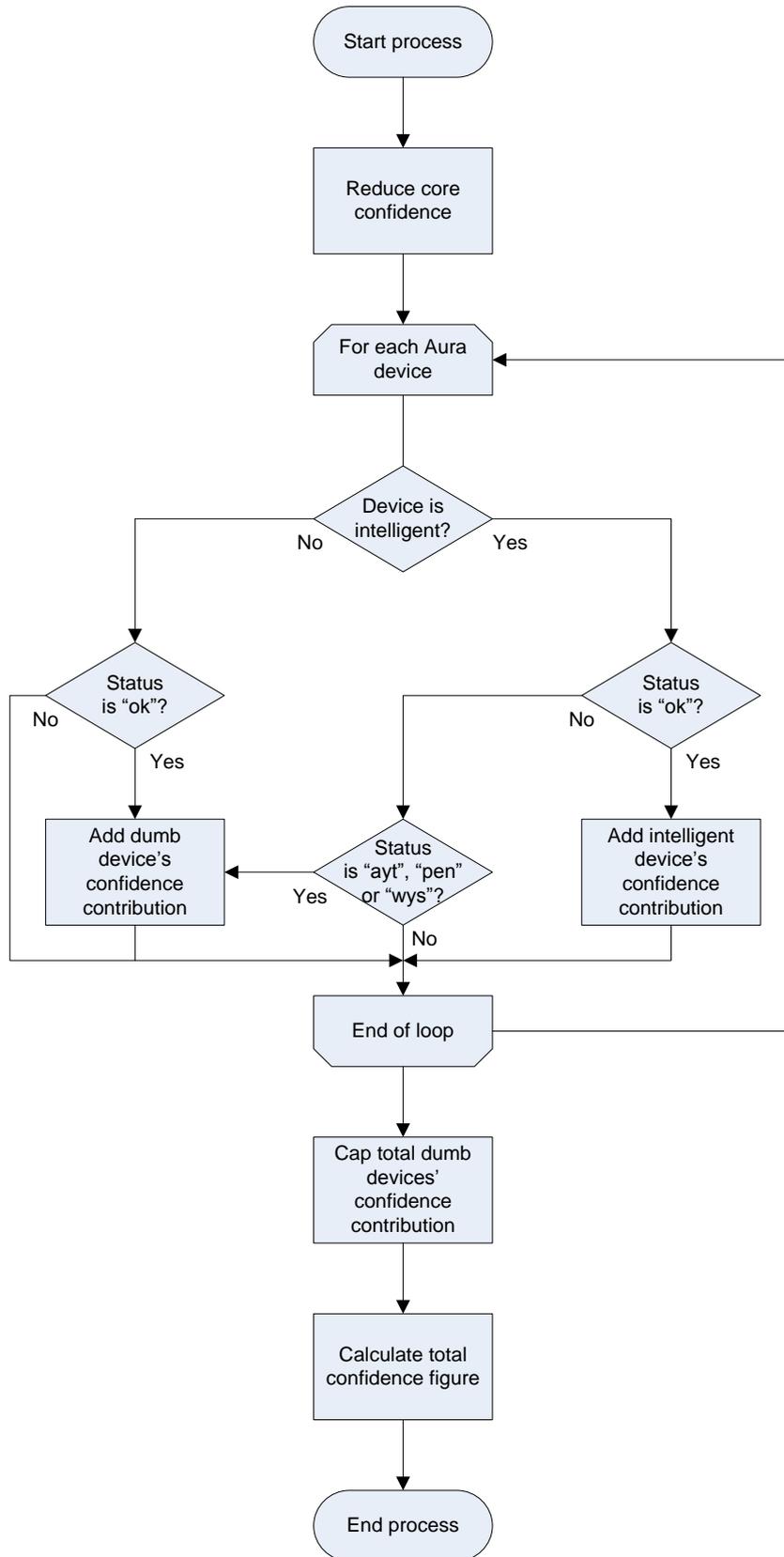
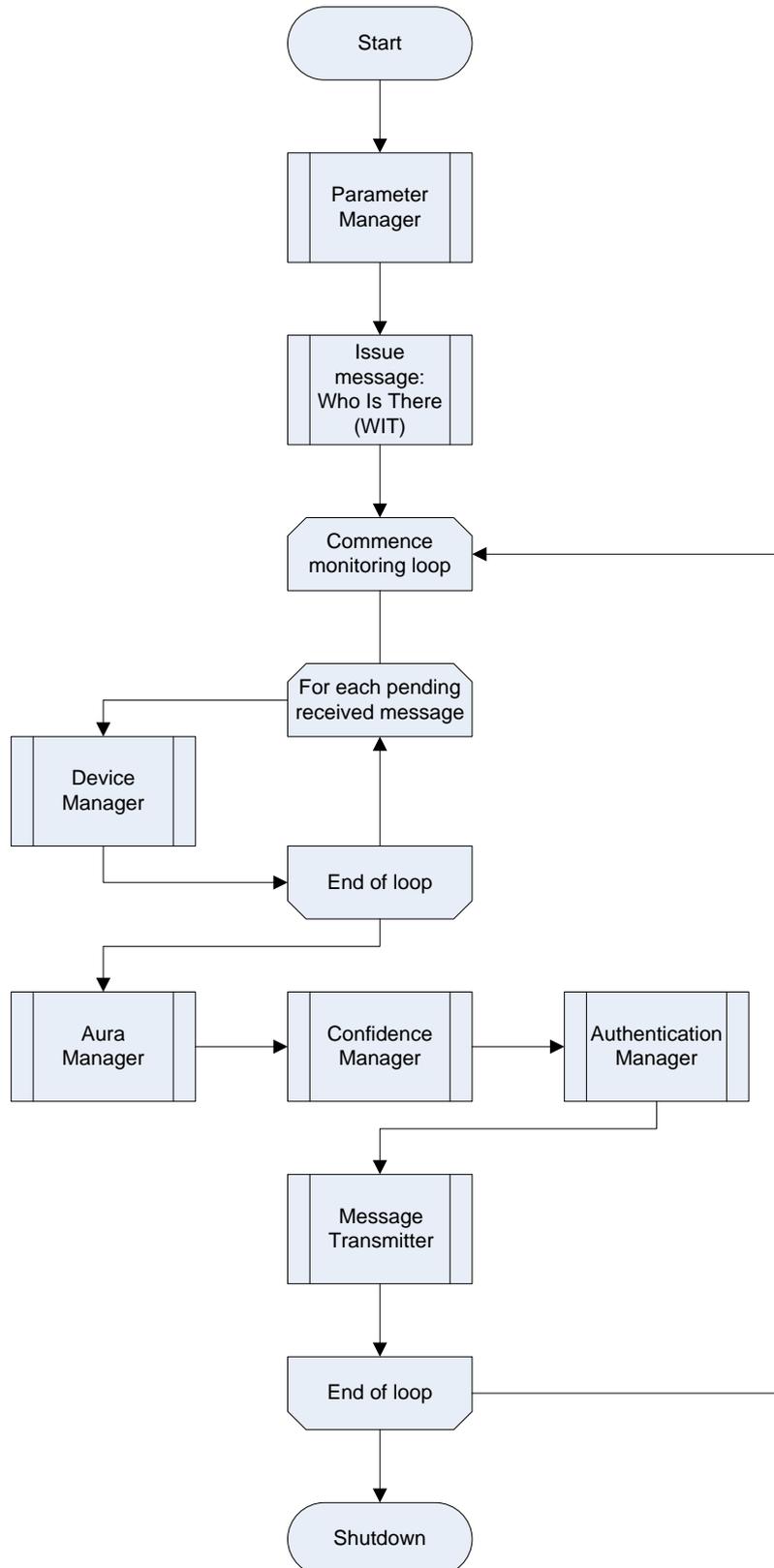


Figure 6-20. Confidence Monitor flowchart

## 6.9 Aura Security Manager (ASM)



**Figure 6-21. Aura Security Manager flowchart**

The ASM is the module which is at the heart of the Authentication Aura framework, administering the system and activating the other processes as required (refer to Figure 6-21 above). Upon initiation of the system the ASM firstly calls the Policy Manager to set the

required variable values or steer the user into the parameter definition screens. It then issues a Who Is There (WIT) message which serves two purposes: to poll the local environment to ascertain which devices are nearby and active, and to announce that this host device is now active and willing to participate in an Authentication Aura.

The routine then proceeds into a continuous monitoring loop which will remain active until the device is shut down. The first step in this loop is to monitor and filter any messages that have been received via the Sensor and placed in the message cache. As each message is superficially examined, the transmitting device is validated by the Device Manager (see section 6.6). Once the message list has been filtered those that are Aura specific are passed to the Aura Manager for processing, authentication requests are temporarily withheld.

When the Aura Manager has completed its process the ASM then passes control to the Confidence Manager to calculate the specific user confidence level. The Authentication Manager is then invoked to process any authentication request messages (ARQ) that have been received from other Aura members, and to undertake authentication of the user if the calculated confidence level falls below the re-authenticate threshold. Finally, any messages that have been compiled for transmission are passed to the Message Transmitter where they are dispatched. At this point the ASM returns to the starting point and recommences its monitoring and processing calls to the various subroutines.

## ***6.10 System Security Interface***

The System Security Interface is the process that gives the Authentication Aura concept its power. This routine will eavesdrop on internal system process calls and application initiation within the device, and check the current user identity confidence against a table of thresholds (System Security data table) to ascertain if a particular action should be allowed to occur. Before the intricacies are discussed, an explanation of the associated table structure will be given.

### **6.10.1 System Security data table (security)**

Centric to the Authentication Aura concept is the ability of the system to intercept application initiation and system processes, and validate these against set confidence thresholds prior to allowing their use. To achieve this, a data table of thresholds needs to be created and stored, against which the current user identity confidence can be compared during activation of an application or service; the System Security table fulfils this role.

This is standalone and has no relationship with any other data table and as the structure in Table 6-12 on page 148 indicates, a relatively small data table consisting of only four columns

of information. The primary key field, `security_key`, is administered by the system and incremented automatically upon creation of a new record.

When a process is intercepted there will be an associated identifying code (Process Identity or PID in abbreviation) that will be used to select the appropriate threshold. When a new application is identified this code will be held in the `security_application_code` data field.

To enable the system administrator to easily remember which threshold applies to which application, `security_application_name` is used to store a meaningful description of the process in question although it will be possible to pre-populate this from internal system information. It is free format and will accept whatever text the user types.

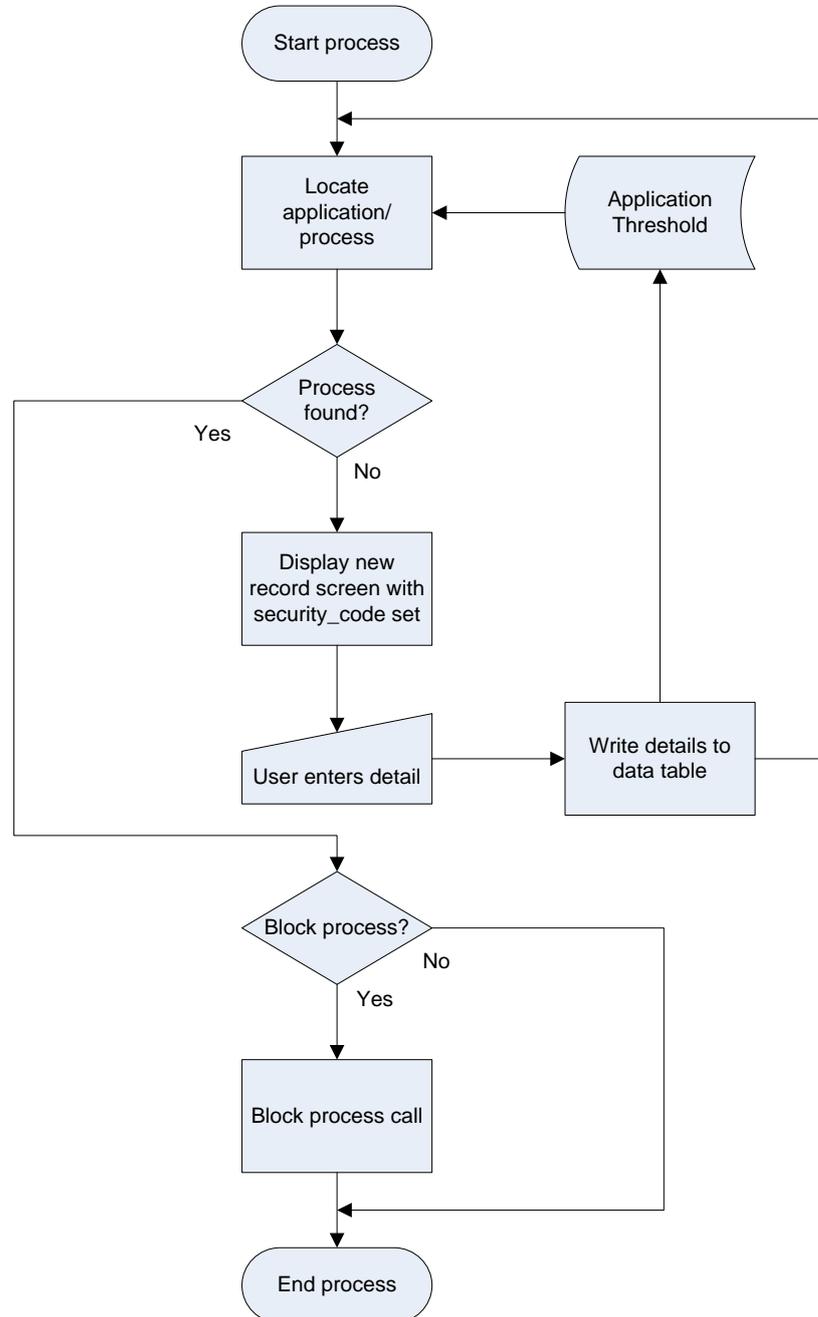
The final but all-important column is `security_threshold`. This is a numeric field which will accept data entry to two decimal places and stores the minimum value at which the corresponding application or system process will be allowed to operate. The figure contained within, will be bounded between 0 and 100 but these are the only constraints placed upon the administrator. To enable a more intuitive user interface the entry of this value will be made via a visual on-screen slider ranging from extremely high risk to low risk and to ease the initially onerous task the value will be defaulted to the parameter `appSecurityDefault`.

Field name	Description	Type	Length	Details	Example
security_key	Key field	Integer	n/a	Auto increment	1
security_application_code	Code	Text	20	Contains the code of the application or system process	SMS
security_application_name	Name	Text	30	Application name or description that enables the user to provide a meaningful reminder of which application this threshold relates to	Text messaging
security_threshold	Threshold	Float	6	A threshold which the confidence must exceed before the associated application or system process is allowed to run	25.00

**Table 6-12. System Security data table definition**

### 6.10.2 System Security Interface logic

When an application is activated the System Security Interface is called and passed the code of the process that is about to function. A search of this code is then undertaken in the System Security table (security\_application\_code field) but if this fails the operator is then prompted to create an appropriate description and threshold record for future use.



**Figure 6-22. System Security Interface flowchart**

The procedure then continues to compare the current user identity confidence against the threshold (either found or freshly entered) and then blocks the process call if the figure is below this value, permitting the activity in all other circumstances. A diagrammatic representation of this is shown in Figure 6-22 above.

### ***6.11 Summary***

In this chapter a detailed description of the Authentication Aura framework has been presented, outlining the processes, data and communication that dovetail together to form a functioning agent. Although the anatomical diagram initially presented the databases and processes as disparate elements it should now be clear that the two are intrinsically coupled. The process logic and messages created by and exchanged between devices has been explored in depth providing an understanding of how a functioning Authentication Aura will operate.

Segmenting the design into elements with limited but focussed responsibility will enable the production of an efficient agent, with the ability to be maintained easily and incorporating an element of inbuilt expandability. The specifics detailed within the chapter and the approach taken will allow an evaluation and subsequent performance assessment to be undertaken in the following chapter. Simulating operation of the Authentication Aura will enable the confidence calculation equation to be refined and in addition the proposed parameter values to be assessed.

Beyond the simulation this framework offers a route to the production of a fully operational prototype which can be installed upon a device and assessed within a real world environment. The detail specified within this chapter offers the logic and data structures necessary to achieve this, whilst maintaining the route to development of a novel, focussed, efficient and robustly secure approach to device security.

---

## **Chapter 7**

# **Evaluation of an Authentication Aura**

---

## 7. Evaluation of an Authentication Aura

---

In the previous chapters the conceptual elements of an Authentication Aura have been introduced and detailed to provide a thorough understanding of the framework and its fundamental principles. The undertaken experiment established that within a user's local environment detected equipment and infrastructure provided information that can be leveraged to boost user identity confidence and potentially offer enhanced security. With the processes to achieve this having now been detailed it is necessary to evaluate the approach and investigate if it does indeed have the capability to fulfil its aims and requirements.

Using the data gathered during the experiment and feeding parameter variations into the confidence equation introduced previously, mathematical simulations have been run and analysed to ascertain the effects of adjusting rates of confidence erosion, thresholds and timings upon the need to re-authenticate. The results will be compared against proposed benchmark situations to test the efficacy of this new approach to user authentication and establish if a reduction in user inconvenience is forthcoming, and even if the goal of removing the need to authenticate altogether is attainable.

Before the simulation and evaluation can be performed it is necessary to review the confidence equation introduced in section 5.8 and define initial forms of the three functions contained within it so the analysis can commence. As such the earlier proposed equation is reproduced below in Equation 7-1.

$$C_x = \left[ F_1(t_x, m_x, l) + \left( \sum_{i=1}^n F_2(t_i, m_i) \right) + \left[ \left( \sum_{d=1}^p F_3(r_d) \right) \right]_{\min 0}^{\max a} \right]_{\min 0}^{\max 100}$$

**Equation 7-1. Combined identity confidence equation**

Function  $F_1$  calculates the core confidence of the user's identity based on three arguments, the time since authentication was performed, the method of authentication used and the current location. This calculation must additionally incorporate the erosion of certainty in the user's identity since the last authentication was made on the host device  $x$ , the centre of the Aura.

Traditionally, when a user successfully authenticates on a mobile device the perceived confidence in their identity is 100% and remains so until the device is deactivated or a screen lock is invoked. As the Authentication Aura requires rigour tariffs to be assigned to every available method of authentication it is proposed to use this value to vary the starting user identity confidence, reflecting the method used. Hence, an average method (security rank of three e.g. a mixed case alphanumeric password of more than eight characters) might be

allocated a starting value of 80% whilst a more secure method will approach 100%, and it is from these levels that erosion will commence. As proposed in section 5.5 an iterative approach to erosion should be used to maintain the history of location, so that when a user moves between environments an excessively large fluctuation in this value will not be instantaneously experienced. An initial proposal for the function to calculate this at each time interval is:

$$\text{core confidence} = \text{core confidence} - ((\text{degradation}_t - \text{degradation}_{t-1}) \times \text{location})$$

**Equation 7-2. Core confidence calculation**

The system parameters *auraDegradeSecs* and *periodDegradation* described in section 6.5.1 will respectively dictate the time periods between recalculation, and the quantity of confidence erosion applied for each time segment (*degradation*). Every *auraDegradeSecs* the Confidence Monitor (see section 6.8) will be invoked by the ASM, with the number of time iterations since authentication *t* being calculated as illustrated below in Equation 7-3.

$$t = \frac{\text{current time} - \text{time of last authentication}}{\text{auraDegradeSecs}}$$

**Equation 7-3. Calculation of the current time iteration**

By calculating *t* in this manner as opposed to using the precise time difference will smooth out the effect of altering *auraDegradeSecs*; for instance, if an erosion of 1 confidence point every minute was required and *auraDegradeSecs* was set to 60 seconds, *periodDegradation* would need to be specified as *t/60*. If the user subsequently wanted to reduce the amount of processing their device was performing and changed *auraDegradeSecs* to 120 seconds they would correspondingly have to alter *periodDegradation* to *t/120*. Utilising the approach in Equation 7-3 dictates that on both occasions only a single time iteration has passed and thus for each situation *periodDegradation* would be set as *t* (one point reduction for each iteration – a straight line erosion).

*Core confidence* is further influenced by the location multiplier (*location*), an argument that is set dependent upon the device's current operational environment, initially home, work or away. Simulation will further explore values for these but it should be noted that home is where the device is likely to be safest (a low value), work is next and then away is the environment in which the device is at greatest risk (high). To enable simulation to commence respective values of 2.5, 5 and 10 are proposed meaning that when at home erosion will be half as fast as at work but four times slower than when the user is in an alien environment. Selecting these values as opposed to 1, 2 and 4 will allow scope for greater adjustment in either direction.

Additionally, it should be noted that the calculation of *core confidence* is unbounded and can even become negative, and if authentication has not yet been performed on the device it will be set to zero.

Function  $F_2$  encapsulates the contribution made by each intelligent device within the Aura and is based upon the method of authentication last performed on that member device and the time since the authentication was performed. It is important to highlight that the contribution of such devices cannot be based upon their current overall confidence because they are members of the Aura, and as such will be calculating their own value inclusive of a contribution from the host device. If this were done, a ping-pong effect would be created as values were traded back and forth, falsely elevating the confidence of each participating device; thus each intelligent device will contribute the same parameterised amount *intelligentContribution*. As such function  $F_2$  is proposed as follows:

$$\textit{intelligent device contribution} = \frac{(\textit{intelligentContribution} \times \textit{authentication method})}{\textit{time since authentication}}$$

**Equation 7-4. Intelligent device contribution**

For the sake of discussion, *intelligentContribution* might be set to a value of 20% and *authentication method* in the range one to five. An *authentication method* of value five would indicate an extremely secure and robust (resistant to circumvention) method of authentication and one the least secure method possible. *Time since authentication* is not a strict time such as the number of seconds or minutes but an iteration multiplier based upon the time and *auraDegradeSecs* as used in the calculation of *core confidence*. For example if *auraDegradeSecs* was set to 120 seconds this would be the number of two minute intervals since authentication. Thus for an authentication method of three (an averagely secure method) that was performed 18 minutes ago (9 two minute periods) and providing the device has been continuously present in communicable range, the confidence contribution would be  $((20 \times 3) / 9) = 6.66\%$ . Adjusting the parameter *intelligentContribution* will of course correspondingly alter the amount of contribution made by each intelligent device.

Dumb pieces of equipment that are unable to authenticate or communicate with other members of the Aura will simply act as tokens and contribute confidence by their presence. The amount by which they contribute is simply dependent upon their rank, an allocated value between one and ten, the higher the rank the greater the security significance of the item. For example in the experiment detailed in chapter 4.2 one subject's wallet was often detected yet hidden and potentially quite secure, so it is conceivable that this item would be allocated a rank of eight or nine, whilst the meeting table they encountered was far less personal and

would therefore be ranked at a much lower level, perhaps two. As an initial starting point the proposed equation for the contribution of the inert devices is:

$$\textit{token device contribution} = \textit{tokenContribution} \times \textit{rank}$$

**Equation 7-5. Dumb device contribution**

Within Equation 7-5 the static parameter *tokenContribution* provides the basis of the calculation and so to get a balance between the token devices and the intelligent ones it is proposed to allocate a value such as 1.5% to *tokenContribution*. Thus a significant item (wallet) with a rank of 8 when detected would consistently add 12% to the Authentication Aura's confidence total. As outlined earlier, the sum of all of the contributions from dumb devices will have an upper bound threshold (the parameter *maxTokenContribution*) applied to ensure confidence is not maintained at an artificially high level by a large number of these devices that can easily be purloined by an impostor. If for instance an upper bound of 30% were applied, in the above example it would require three such items to be concurrently detected to maintain this maximum contribution.

When intelligent devices are present but have not been through an authentication process it is proposed that they will be treated as dumb devices. Without authentication they would be incapable of making a contribution and so, by treating them in this way, at least their detected presence will be used positively.

### **7.1 Authentication Aura Simulation**

Now that initial proposals have been made to assess the effectiveness of the outlined Authentication Aura and to model the aforementioned formulae to understand the impact of the parameters upon authentication security analysis of the observed experimental data is required. This analysis has been undertaken by simulating the Authentication Aura using an initial set of proposed parameters and then adjusting them to ascertain the effect both statistically and visually. The hypothesis for the simulation is that a significant reduction in the number of intrusive authentications will be observed when simulating an Authentication Aura in comparison to a PIN based benchmark solution. The details of how the simulation was performed will now be outlined in the following sub-sections.

A script has been written in a mathematical modelling system that utilised the captured data and calculated a confidence based upon the detected presence of equipment and infrastructure; this is listed in Appendix B. With the script being consecutively run for all users and the sheer volume of data involved it was decided to simulate the user's day between 8am and midnight at ten minute intervals. This approach enabled legible graphs to be plotted illustrating the confidence level at each time interval.

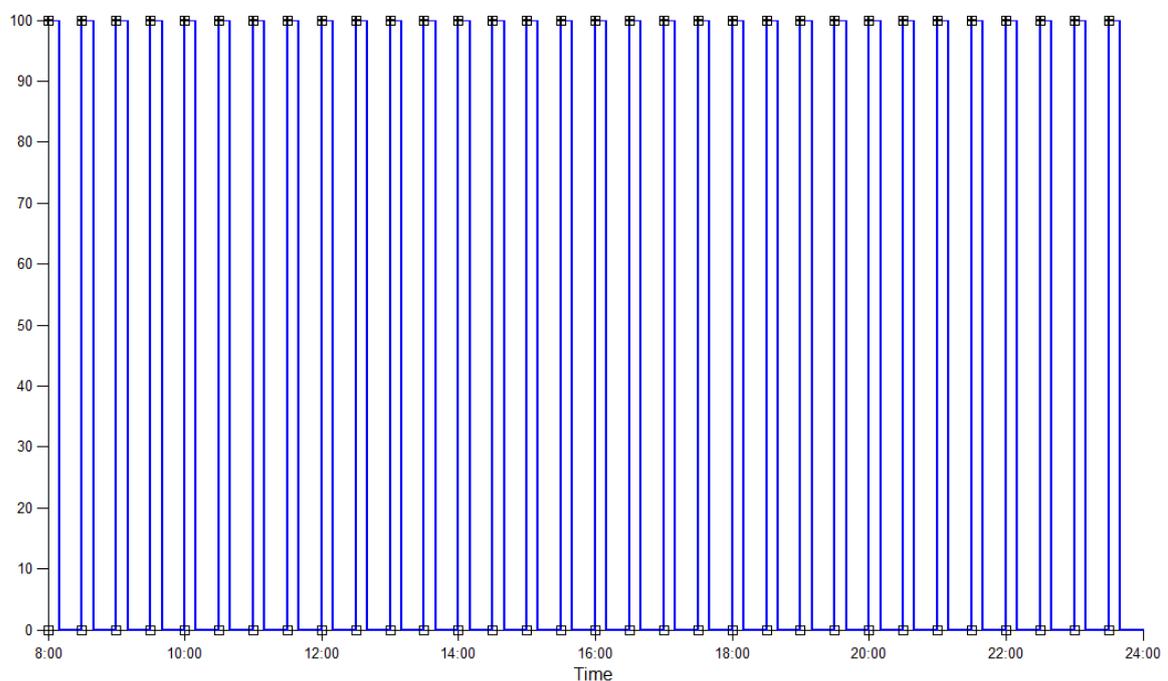
The calculated confidence value is based upon all the observed information and so the host device for which the confidence relates, should be regarded as a non-existent virtual item of equipment upon which the Authentication Aura is centred; that is, a device additional to the observed Aura, the role played by the PDA listening devices in the experiment. To maintain an accurate simulation, during the operation of the script the Authentication Aura confidence was calculated for each of the observed devices with the parameters being universally applied. Thus all intelligent devices had identical thresholds and allocated tokenContribution values which would not necessarily be true in the real world.

With the experiment being run concurrently for groups of five individuals it was vital that any simulation script was written to reflect this. During the operation of the script (listed in Appendix B), once the individual for whom the simulation was being run was ascertained the appropriate tag cross-reference file and then all tag data for the subject was read in and held in memory. As the tag observation data was imported it was filtered to exclude readings prior to 8am and combined into ten minute slots. Thus for each user an array of 96 ten minute slots (16 hours with 6 slots per hour), for every one of the possible 75 tags, across a fourteen day period was populated with an indicator when the appropriate tag was detected. Using the list of cross-reference values enabled the script to identify which of the possible 75 tags each row of detection information related to and provided details of the corresponding device. Consequently the array from which the simulation was run was three dimensional for each user (day, time, tag) and consisted of 14 x 96 x 75 or 100,800 cells.

The cross-reference file holds details of the tag reference, label (1..75), owner, location (home, work, mobile), description, type (device, infrastructure, other), category (intelligent or dumb), rank (1..10), can authenticate (yes or no). Hence the array constructed from this file was two dimensional and consisted of 75 rows with nine columns in each row.

The simulation then processes each timeslot in turn, identifying the devices that were detected, and from this builds and maintains an Aura (as detailed in section 6.7.1) for the subject; from this data the confidence calculation is then made. Authentication of the user's identity plays a vital role during confidence calculation and so within the simulation it has been necessary to make some assumptions regarding this process. When an intelligent device that can authenticate is newly detected, authentication upon that device is assumed to have just occurred and then confidence eroded from that point onwards. When authentication is required on any device it is assumed that the process is successful and performed via an averagely secure method, a security tariff of three. From this cyclic calculation of confidence and assumed authentications the appropriate statistics are gathered to record the number of required intrusive user interventions and draw the corresponding graphical representations.

As a baseline comparison, Figure 7-1 illustrates the performance expected from a mobile device employing current PIN based protection, with a ten minute screen lock and an assumption of access being required every thirty minutes. Thirty minute usage is based upon a review of the author's own interaction with a mobile device during a five day period. Although this is not considered heavy usage (with, for example, Woolaston, (2014) indicating that some extreme users access their devices over 200 times a day), it was decided to use the 30 minute frequency as a starting point. Using this access frequency implies that any screen lock of less time makes no difference to the baseline frequency of required re-authentication, and this generous value was selected to gauge the initial efficacy of the Authentication Aura. It should be noted, at the moment the screen lock is invoked the host device assumes the identity of the user to be valid, a well documented weakness of this approach to security (Muncaster and Turk, 2006).



**Figure 7-1. Control plot of user identity confidence on a device with a 10 minute screen lock**

In this and all succeeding plots the y-axis represents the percentage of identity confidence, with the time of day being plotted along the x-axis. Additionally, plus (+) symbols have been overlaid to indicate the point at which access to the device was made and squares have been used to show the points when the user was required to authenticate. Each authentication is represented by two squares, the lower indicates the time and confidence at which authentication was invoked whilst the upper illustrates the confidence allocated immediately after the assumed successful authentication. It should be noted that in several situations and especially in Figure 7-1, a plus and a square co-exist at the same point in time (along the top of the graph) and have consequently been plotted one on top of the other.

From this control plot and with the assumptions detailed earlier it is clear that this simulation indicates that the user would be required to undergo an authentication process 32 times during the 16 hour period from 8am until midnight. Also, employing a traditional Boolean approach to security, when authentication is passed confidence is set to 100% and remains unchanged until the screen lock is invoked and confidence drops to 0%. This gives the graph the box-wave appearance that is exhibited in the diagram.

Variable	Value	Reason for selection
Authentication method tariff	3	Median tariff value
Re-authentication threshold	20%	Low risk service being accessed
Device access frequency	30 minutes	Based on author's observed usage
Time segment for confidence calculation	10 minutes	Clarity of graph production and dictated by large data volume
Location multipliers: home, work, away	2.5, 5, 10	Initial weights, will be adjusted during simulation
Intelligent device contribution factor	20%	Set at this low figure to restrict the influence of these devices
Dumb device contribution factor	1.5%	Selected a low value to limit the influence of insignificant inert items
Cumulative dumb device upper bound	30%	Set at this value to permit usage of a low tariff app
Period degradation	$t \times 2$	Selected to ensure erosion to 0 within 20 minutes when in an alien location.

**Table 7-1. List of parameter values used in the simulation**

The simulation parameter values introduced earlier are summarised in Table 7-1 and in-line with the benchmark above it was assumed that the user attempted to access a low risk, low tariff application (e.g. texting on a mobile phone) once every thirty minutes. This application is deemed to be available at a confidence level at or above 20%. If the confidence level was below the 20% threshold at point of operation authentication was assumed to be requested and successfully completed with an average level three method, establishing the associated initial confidence of 80%. It should be noted that in reality this figure would vary upon differing authentication techniques being invoked.

The period degradation multiplier ( $t \times 2$ ) will invoke straight line erosion with the only influence on its rate being the location multiplier; without the inclusion of location it would take the system 30 time segments (300 minutes) to erode confidence from a starting point of 80% to the re-authentication threshold of 20%. If this Authentication Aura baseline is simulated both at home and away the resultant graphs are shown below in Figure 7-2 and Figure 7-3.

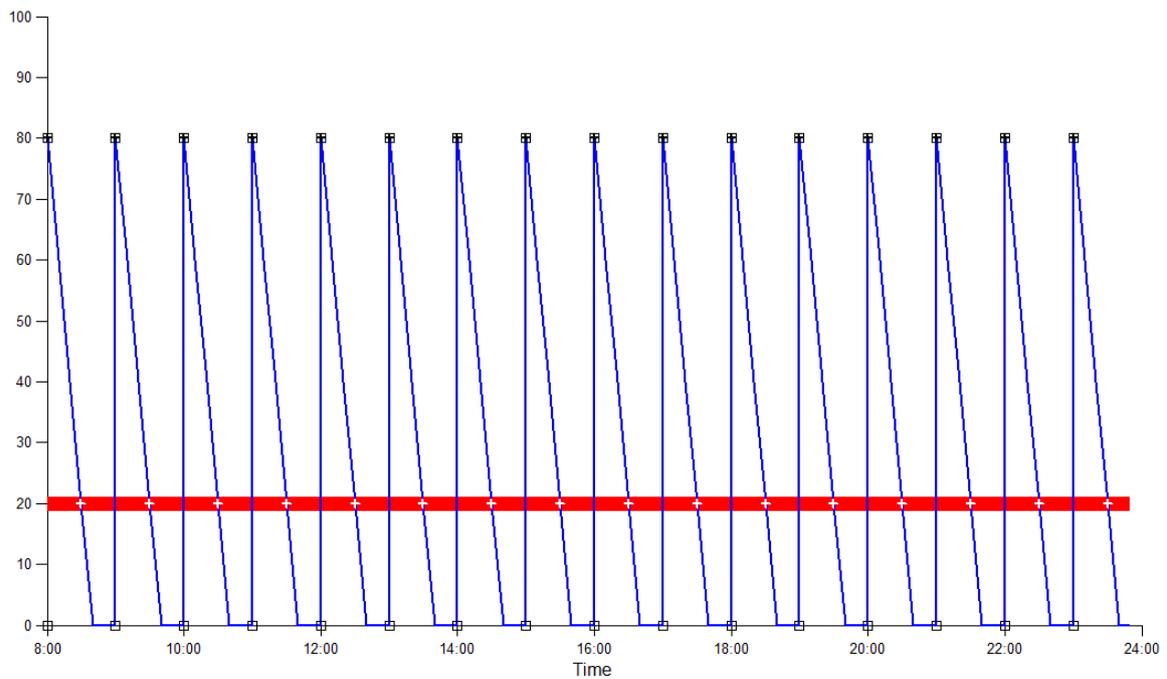


Figure 7-2. Degrading confidence whilst away from home

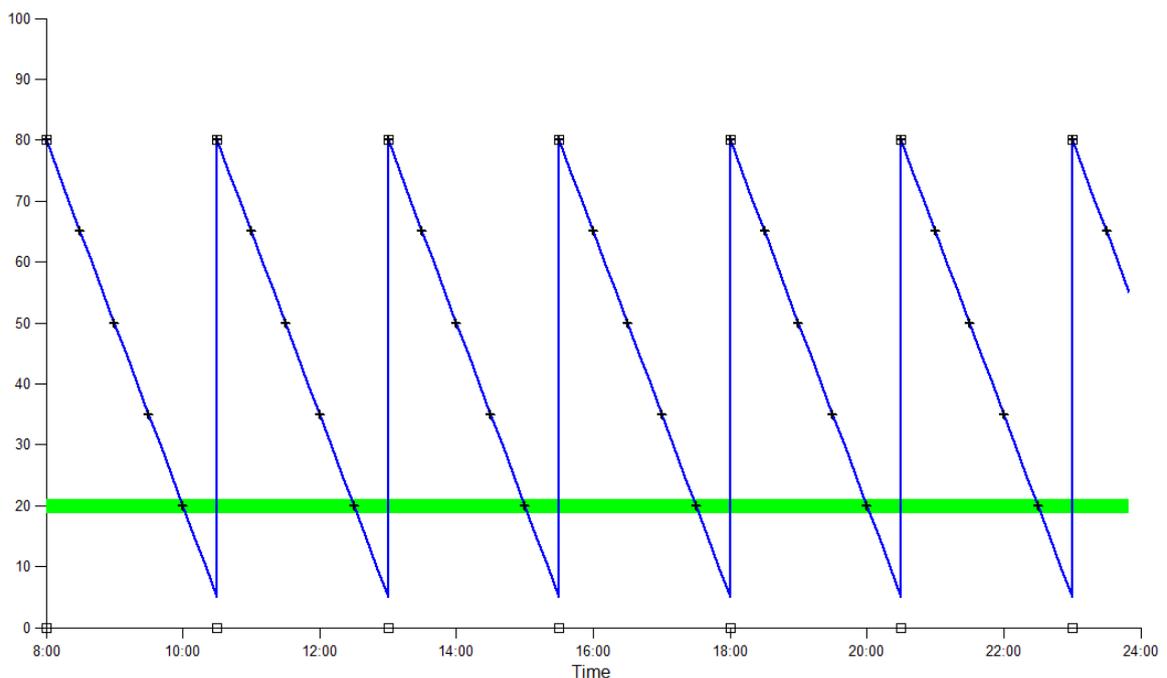


Figure 7-3. Degrading confidence whilst at home

To aid interpretation the graphs also include the re-authentication threshold which is drawn in a colour dependent upon the user's location (home is green, red away and work would be amber). When service access is attempted at a confidence level below this value re-authentication is demanded and assumed successful, and thus without any external Aura influence, in Figure 7-2 the confidence degrades at a rate of 20% for every ten minute period after authentication. Thus it takes 30 minutes to degrade from the authentication level of 80% to 20% and 40 minutes to drop below the access cut-off value. As a result, in this test simulation authentication is required every sixty minutes at alternate service activations,

leading to the 16 authentications exhibited by this default graph between 8am and the 12pm cut-off. In direct comparison when at home for the entirety of the day Figure 7-3 requires only seven re-authentications during the same 14 hour period.

As a further introductory comparison if a single user (subject 3) is examined for a single day (day 9<sup>15</sup> - the second Tuesday), it is first necessary to allocate ranking values for the items they specified on their experiment participation device list. The values used are shown below in Table 7-2 and have been allocated based upon the anecdotal evidence observed in the experiment.

Equipment	Rank	Equipment	Rank	Equipment	Rank
Wallet	8	Car (Home)	7	Bag	6
Fridge	6	Microscope	5	MP3	4
Locker	4	Coat	6	PC	5
Bed clock	6	Fax	1	Car (Work)	5
Laptop (Work)	4	WiFi (Home)	5	Mobile (Work)	5

**Table 7-2. Subject 3's tagged equipment and associated rankings**

Utilising these values and running the simulation for the user the graph illustrated in Figure 7-5 is produced. For completeness and to aid discussion the corresponding diagram in Figure 7-4 has been reproduced in-line, highlighting when the various items of equipment were detected throughout the identical timeframe.

Immediately it is noticeable that the detected devices provide the necessary information to ascertain the location of the user at any given time. Although close examination also reveals that shared resources, items tagged by other experiment subjects, have also been detected; that is, colleague's office, reception and meeting table. For security purposes the default location is away but this graph indicates the extended periods that are spent both at home and in a work environment. Interestingly, as discussed previously, upon activation of the core device initial authentication is delayed for a period of time. Although initially the Aura only contributes approximately 24%, a level at which operation of many services should be restricted, it is a level at which the first simulated access can function and is a good indicator of the influence that can be harnessed. This influence is further illustrated by the confidence rising above the parameterised 80% level immediately upon each authentication.

<sup>15</sup> All users' data was labelled with a day number based on 1=first Monday of experiment, ... ,6=first Saturday, 7=first Sunday, ... , 12=second Friday etc.

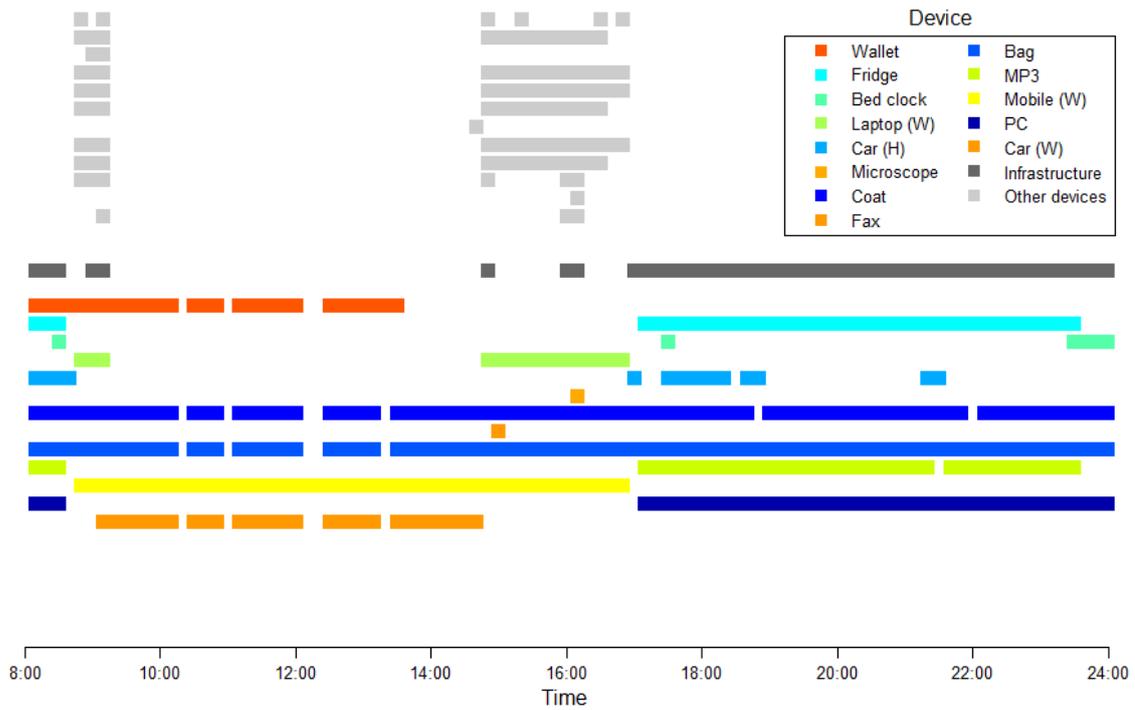


Figure 7-4. Subject 3's devices detected during the day selected for simulation (day 9)

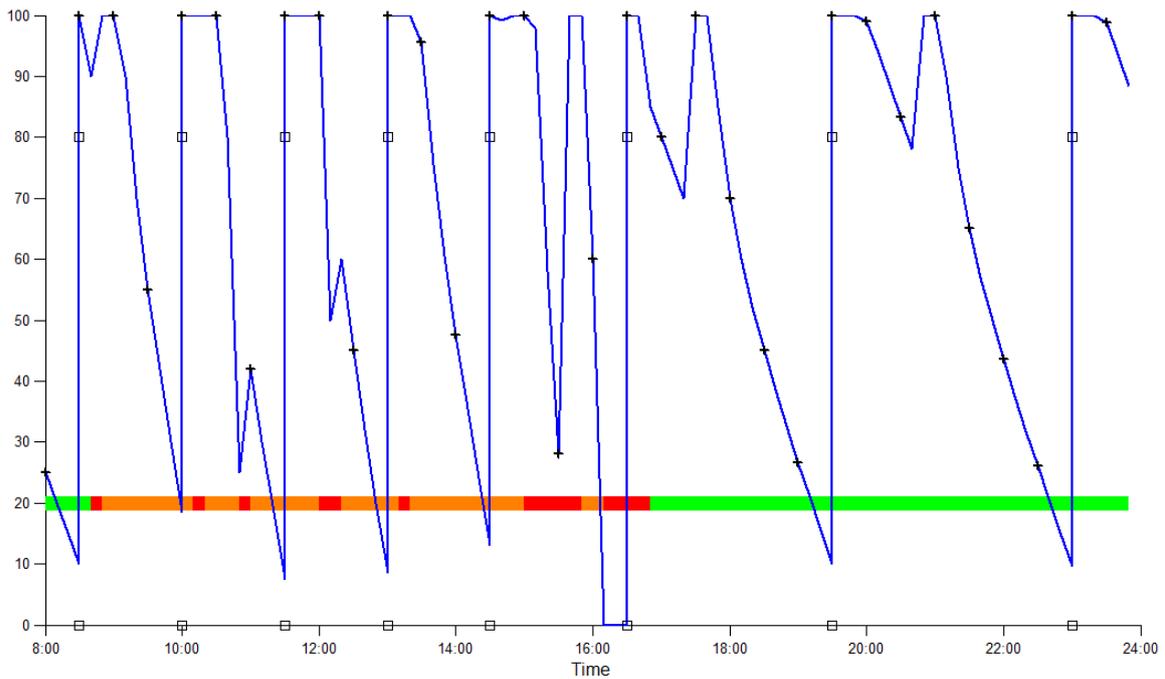
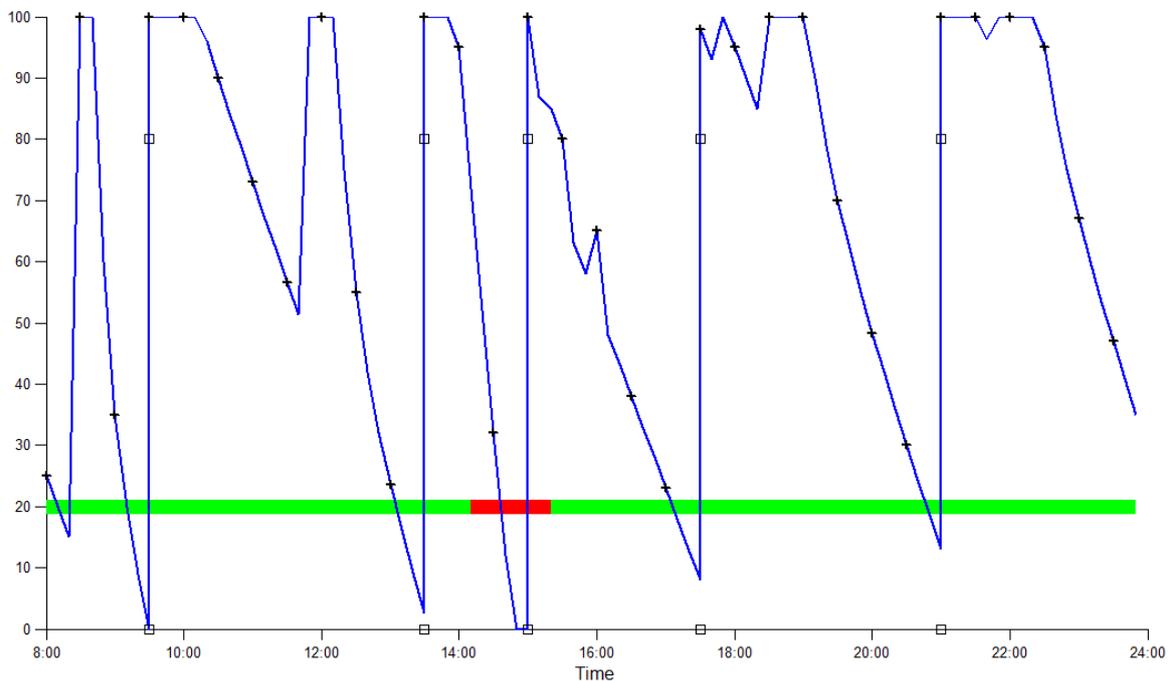


Figure 7-5. Simulated Authentication Aura results for subject 3 on the same day

Location of the user and the core device clearly affects the rate of decline in confidence; with the user returning home just before 5pm during the evening beyond this point the gradient of the plot significantly reduces, reflecting the relaxation of degradation expressed within the confidence equation. At approximately 5.40pm the user moves within detectable proximity of their PC, MP3 and fridge and the added assurance these token devices reverses the confidence erosion, reflected by a spike in the graph at this point. This further supports the applicability of the Authentication Aura's approach and with the future expected to provide us with greater

numbers of detectable devices, the potential for security leverage is only likely to increase. Overall the number of authentications across the 14 hours of utilised experimental data for this user on the simulated day is reduced to 8, 25.0% of the baseline 32.



**Figure 7-6. A comparative user's weekend Authentication Aura profile (user 9, day 14)**

For comparison purposes, Figure 7-6 illustrates a different user's simulated weekend day activity based upon their own specific devices and personal items but using identical parameters and thresholds. From this it is clear to see that apart from an hour in the early afternoon the user spent their entire day at home. In this location the Aura is most relaxed with degradation at its slowest. During the plotted 14 hours only 5 authentications are required, only 16% of the baseline 32. The home reference graph Figure 7-3 suggests that without the Aura's influence re-authentication will be expected every 2.5 hours. In the weekend graph however, this period extends to as much as four hours between 9.30am and 1.30pm as the detected devices maintain the confidence at an operable level. There are seven points during the day at which the confidence is capped and then sustained at its maximum level of 100%. Additional contributions from the Aura push the confidence from the simulated authentication threshold of 80% to above the 100% for over 60 minutes before the erosion finally reduces the level back below the cap.

Alteration of the simulated parameters of course influences the performance of the core confidence calculation. If subject three is re-examined for the same day as illustrated earlier but the value of the intelligent device contribution is varied, Figure 7-7-Figure 7-11 indicate the affect of the parameter adjustment. It should be noted that Figure 7-8 is identical to Figure 7-5 but has been replicated here for clarity.

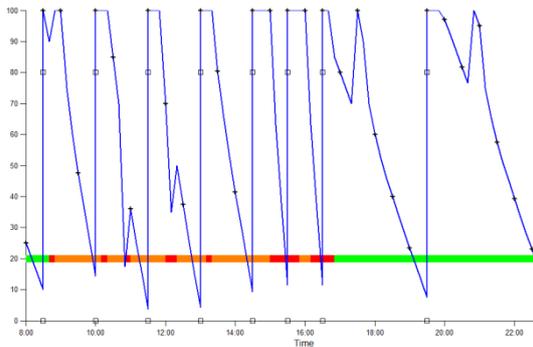


Figure 7-7. Intelligent device contribution 10

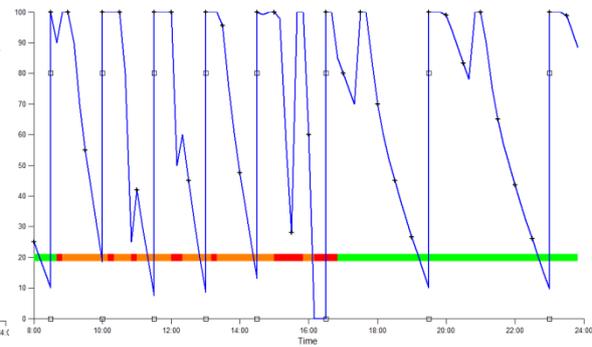


Figure 7-8. Intelligent device contribution 20

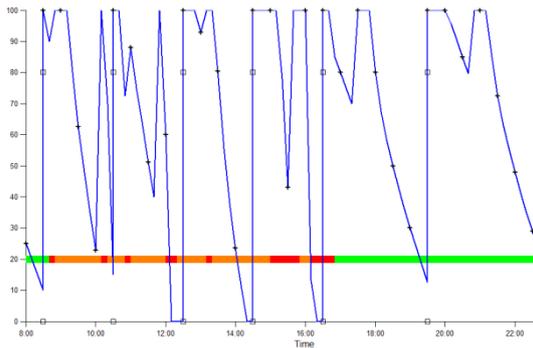


Figure 7-9. Intelligent device contribution 30

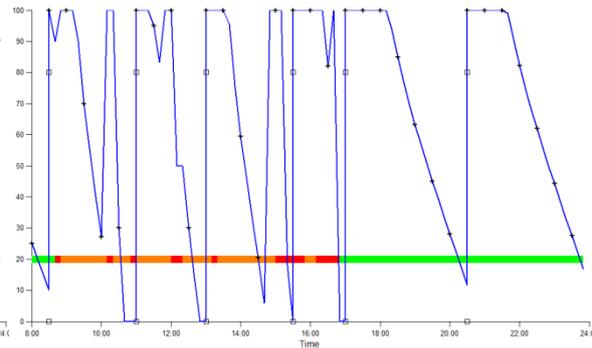


Figure 7-10. Intelligent device contribution 40

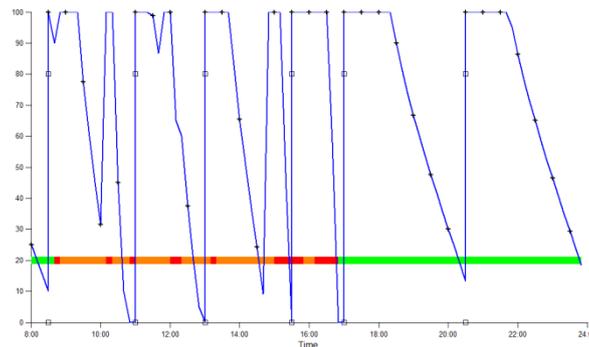
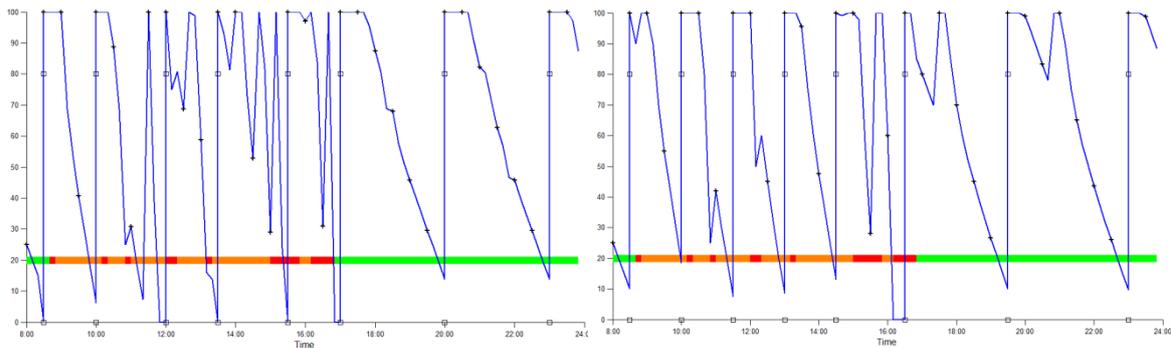


Figure 7-11. Intelligent device contribution 50

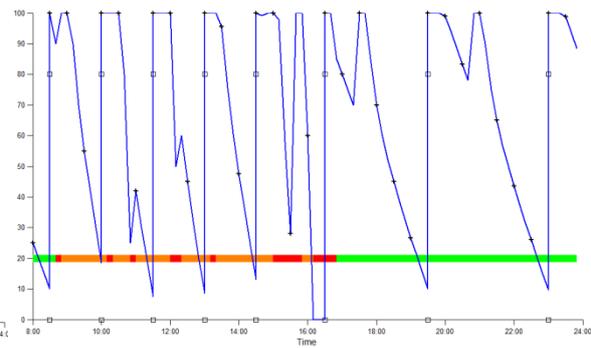
In the examples above it is clear that the main effect of varying the intelligent device contribution parameter is to reduce the number of authentications during the day from nine in Figure 7-7 to six in Figure 7-11. However, perhaps more significant is the number of authentications required when the user is not at home. It is in the higher risk environments where the user would be required to undergo fewer authentications; at home the inconvenience remains unaltered. Whilst at work or in an alien environment, setting the intelligent contribution parameter to 10 (Figure 7-7) forces six authentications, whilst increasing the parameter to 50 (Figure 7-11) requires only three. This indicates that potentially the Authentication Aura is acting too confidently with the highest setting and consequently intelligent devices are providing excessive contribution.

Logically the overall confidence percentage is maintained at a higher level for longer and is slower to degrade. With this occurring the user would have more high-level applications and functionality available for their use for greater periods of time.

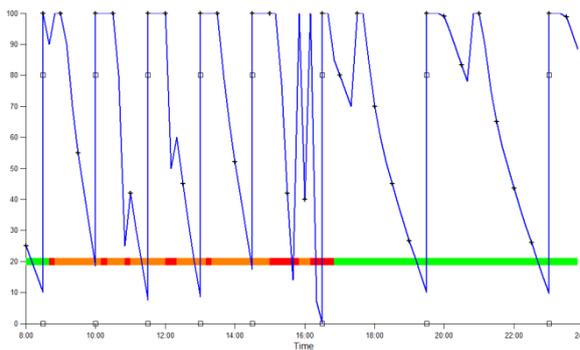
If the intelligent contribution is reset to the initial value of 20 and the token device contribution varied with values of 0.75, 1.5 (the default), 2.25 and 3 the following graphs are obtained. Figure 7-13 has once again been repetitively reproduced for ease of discussion.



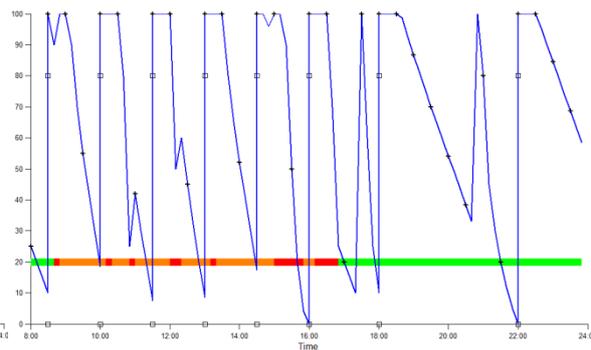
**Figure 7-12. Token device contribution 0.75**



**Figure 7-13. Token device contribution 1.5**



**Figure 7-14. Token device contribution 2.25**



**Figure 7-15. Token device contribution 3.0**

The graphs illustrate that overall the number of authentications across the different token contribution values remains unaltered at eight. The lowest value would imply that a dumb device given the highest security rank will only contribute 7.5% towards the calculation, a quarter of the capped maximum 30%, whilst in Figure 7-15 the same device would unilaterally provide the maximum. The one difference that is noticeable is the frequency of peaks and troughs exhibited by the lowest value in Figure 7-12, there are many more rapid fluctuations in the confidence calculation although it could be argued that this makes the Authentication Aura more responsive to the devices in the environment; potentially an advantage. Proceeding from this point, if the capped maximum token contribution parameter is varied and each token contributes 1.5 as a minimum, Figure 7-16-Figure 7-20 result.

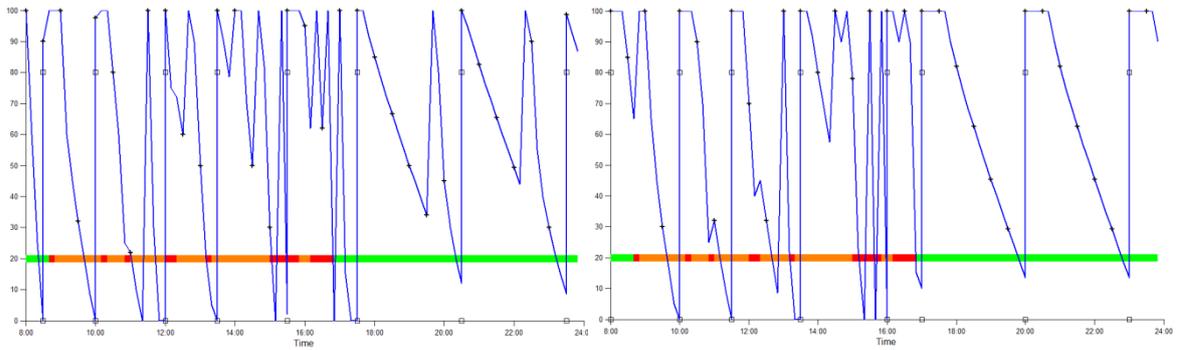


Figure 7-16. Maximum token contribution 10

Figure 7-17. Maximum token contribution 20

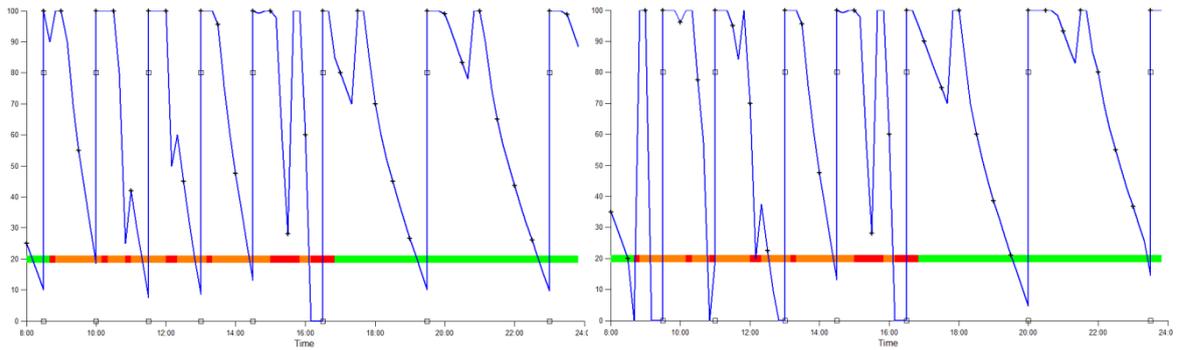


Figure 7-18. Maximum token contribution 30

Figure 7-19. Maximum token contribution 40

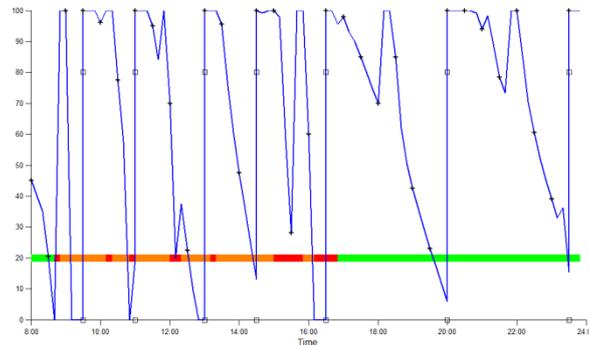
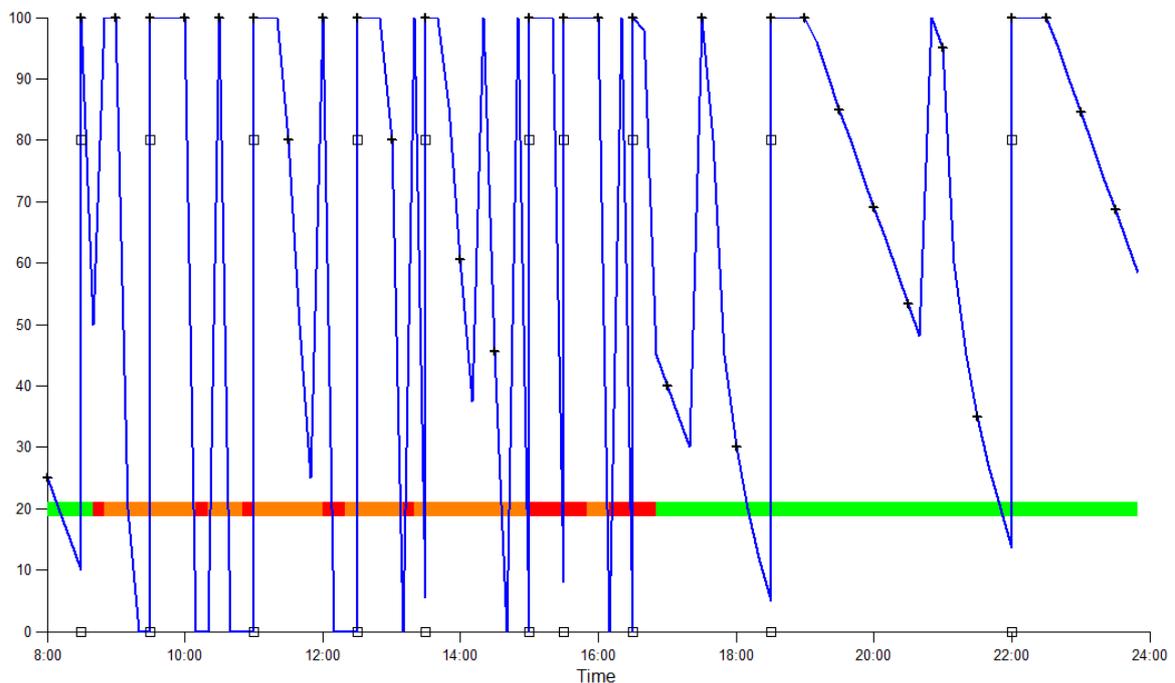


Figure 7-20. Maximum token contribution 50

Amending this value does not have a significant performance upon the Authentication Aura as shown in the graphs although it does produce a spurious result. When the maximum token contribution threshold is at its lowest test value of 10, it has the affect of delaying the first required authentication for longer than a higher value as illustrated in Figure 7-16; in fact upon simulated activation it immediately sets its own confidence to 100%. This is because the simulation is being extrapolated across all detected devices and at 8am the subject's home PC is detected. One of the assumptions of the simulation was that when an intelligent device was detected for the first time, without any prior knowledge it was assumed that authentication had just been performed on the item of equipment and confidence would then be degraded from that point on. If the subject had just authenticated on the PC at 8am it would contribute its rank multiplied by the 20% intelligent device contribution without any erosion, which in this

instance is 5x20%. In the other variations there is sufficient confidence gained from the Aura to prevent the PC authenticating which in-turn bars this anomaly from reoccurring.

Throughout the simulations that have been discussed so far, one set of parameters that have remained unaltered are the security weightings for the three locations defined during the experiment. It could be argued that the comparison of performance of the selected subject against the baseline screen lock example is unfair because in the most vulnerable locale (away from work and home) it still takes 30 minutes for 100% confidence to be eroded to zero, rather than the baseline's 10 minutes. If the location weightings are widened to increase the caution exhibited by the Authentication Aura when at work or at home the resultant graph might be deemed more comparable. To this end the tariff whilst at home was left unchanged at 2.5, work was increased to 10, and away was allocated a weighting of 30 the equivalent of eroding 100% to zero in ten minutes; the resultant graph can be seen in Figure 7-21.

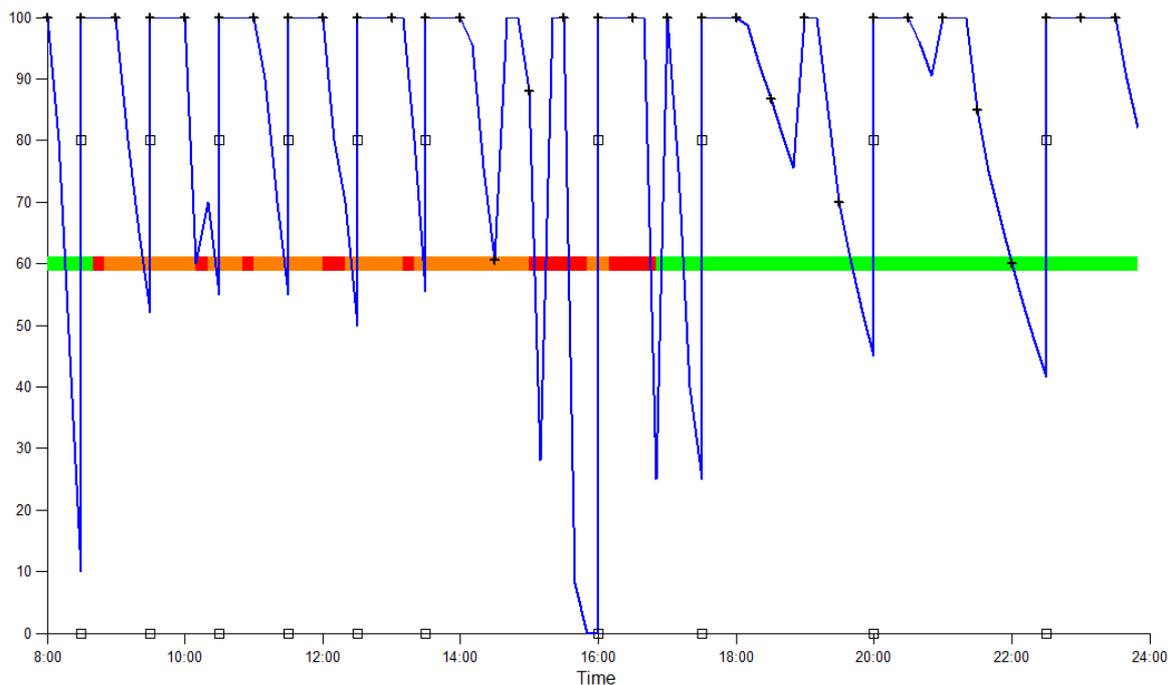


**Figure 7-21. Subject 3 on the same day with increased location weightings**

The immediate observation is the unsurprising increase in fluctuations of confidence when the subject is away from their safer environments. However, across the day still only 10 authentications are required compared with the baseline 32. Even if 9am-5pm is taken in isolation, the time when the user is at work or out of the office (away) and the associated risk is at its greatest, the number of authentications is less than half the number experienced on the baseline graph. During this time frame the user accesses their device on 17 occasions and the existing screen-lock security would require a corresponding 17 PIN entries, whilst the Authentication Aura invokes only 7 such actions. This simulation certainly seems to underline

the resilience of the Authentication Aura to changes in locations even when strict security arguments are set.

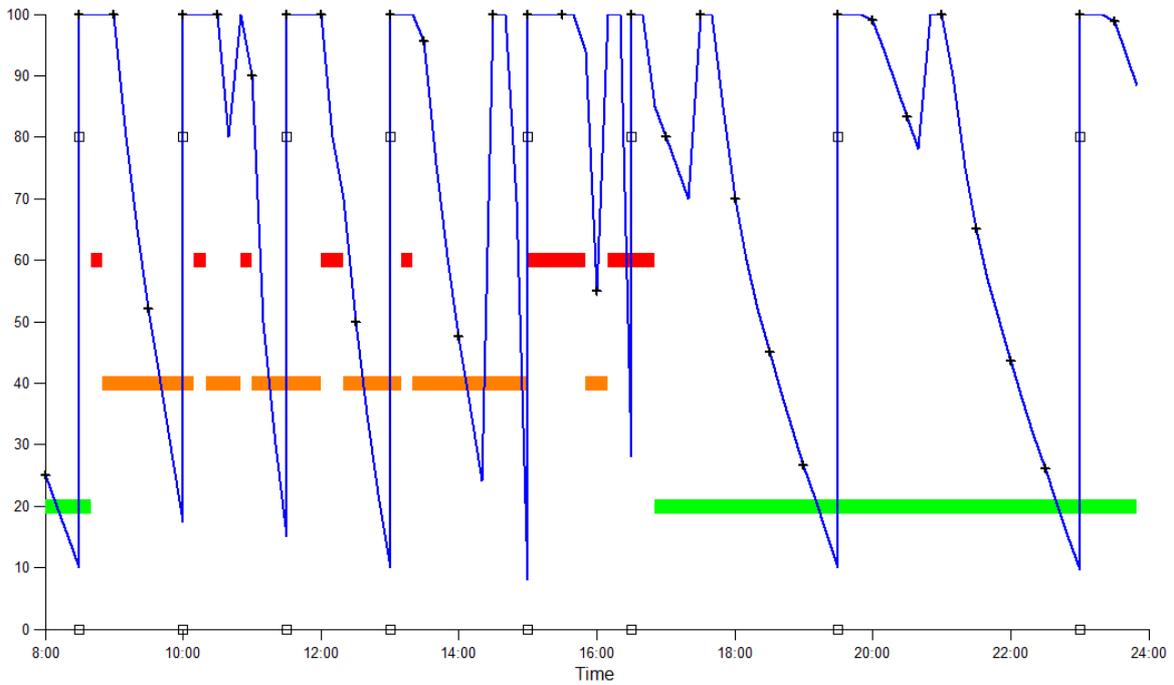
All simulations so far have been examining a low tariff app or service that within the realms of the Authentication Aura only requires 20% or more confidence to function. If this threshold is now raised to 60% simulating the use of a much more sensitive app the resultant graph is shown in Figure 7-22.



**Figure 7-22. User 3 on the simulated day with an increased authentication threshold**

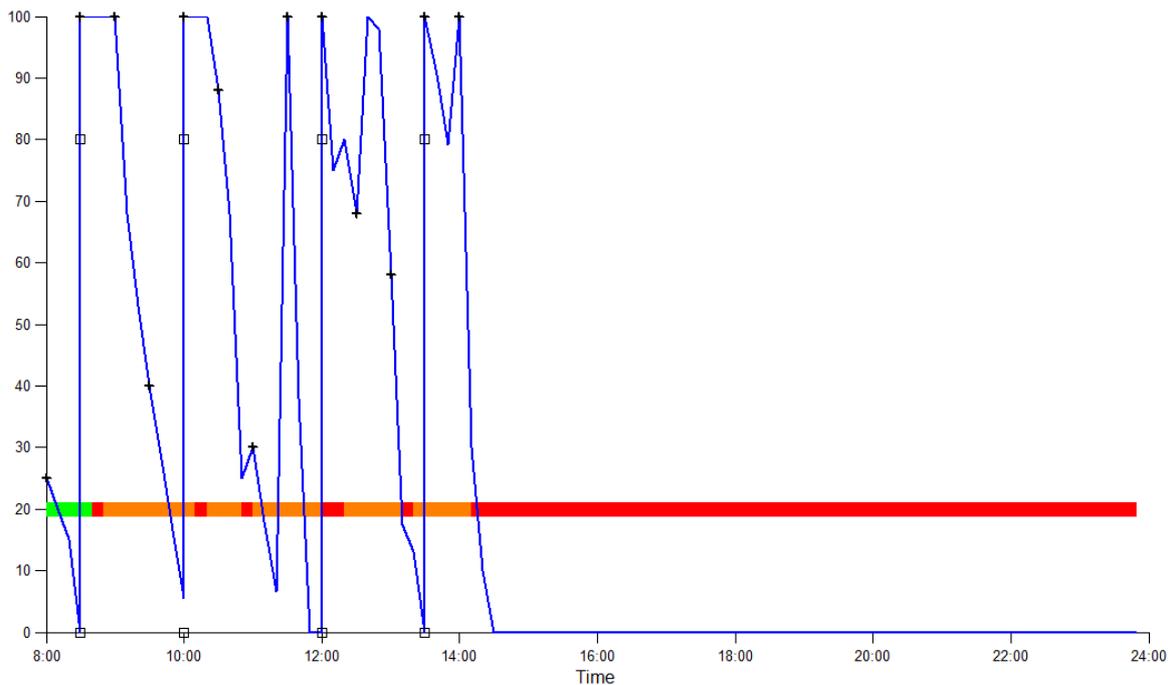
Even with the user accessing a higher tariff application the Authentication Aura still only requires ten authentications to be performed throughout the day, 31.25% of the baseline 32. The graph illustrates how the confidence remains high and even capped at its maximum for extended periods, a combination of the number of host authentications and those also performed more frequently upon the other simulated devices; the entire Aura have all uplifted their security response and positively bolstered each other.

It is also possible to extend the influence of location to assess the effect of varying the authentication threshold dependent on the locale at which the app is being activated. For instance if the threshold is set to 20% when the user is at home, 40% when they are at work, and 60% in all other instances the graph shown in Figure 7-23 is produced. On analysis the number of authentications is unchanged from the comparative simulation with a fixed 20% threshold. In fact the only observed difference is a single delayed authentication which occurs at 3:00pm rather than 2:30pm because other devices within the Aura have been simulated as re-authenticating earlier than they did previously.



**Figure 7-23. Illustration of user 3 with a location based variable authentication threshold**

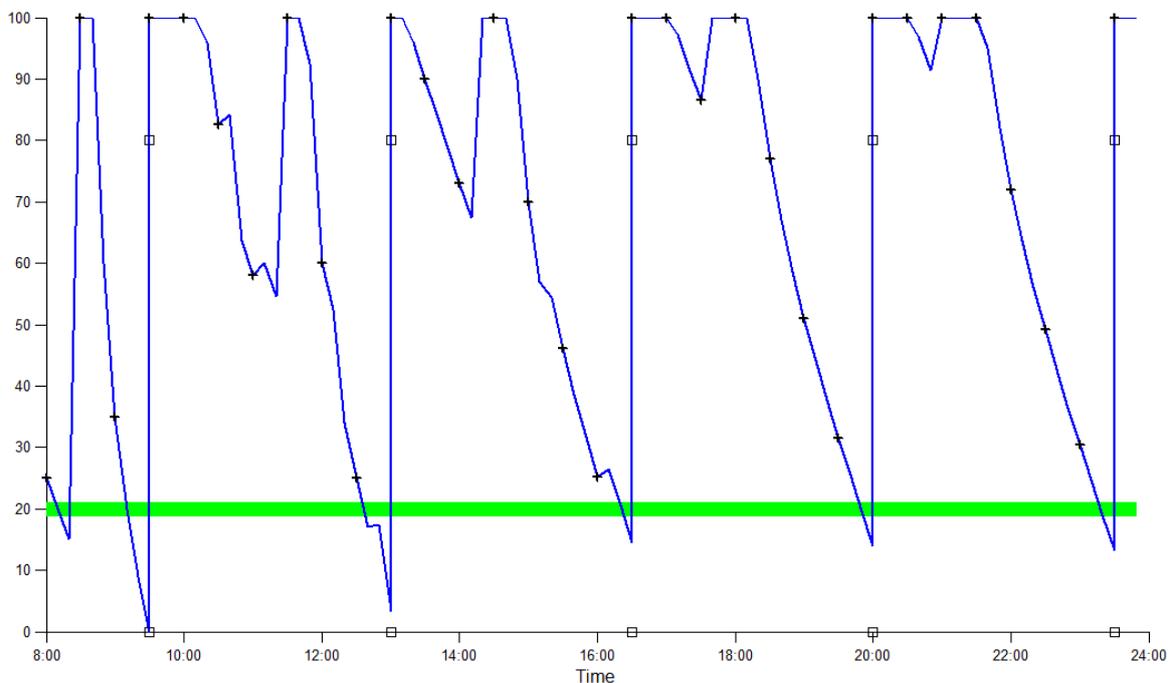
A final important question to evaluate which would be at the forefront of most users' mind is how does the Authentication Aura respond when a device is stolen? To simulate this, the parameters were all reset to their original values and the modelling script amended so from 2.01pm all device detections were blocked. This replicates the theft of the host device and its removal from familiar surroundings out of detectable range from other Aura equipment. The simulated theft of the host device is illustrated below in Figure 7-24.



**Figure 7-24. Simulated host device theft from subject 3 at 2.01pm on the same day**

Upon theft the Aura immediately reverts to the default location of away and it can be seen that without the influence of known devices within twelve minutes the confidence has fallen below 20%; it takes twenty five minutes in total for the confidence to degrade from the last activation at maximum confidence (100%) and flatten out at zero. Intuitively, as the Aura reaches this point all potential services and applications would have been barred and without re-authentication, the simulated device rendered unusable. It should be remembered that for the simulations the Aura calculations have been rerun every ten minutes. In a real life application it is anticipated that this will occur more frequently and so the response to theft would be quicker. In comparison to an unprotected or unlocked mobile phone being continually used, this is a significant improvement to the device only being blocked when the battery's charge is spent and it shuts down.

One of the major objectives of this research is to produce an approach which will postpone the need for a user to authenticate immediately upon activating a device, overcoming the inconvenience of repetitive imposition when using multiple devices. The simulation has indeed shown this to be an outcome of the Authentication Aura as demonstrated by Figure 7-25 below. This graph represents data captured by subject 13 on the first Sunday of their experiment participation, and indicates that the first authentication they were required to make was on the fourth simulated use of the device at 9.30am. This is a postponement of 90 minutes from first activation which will intuitively enhance the user experience.



**Figure 7-25. Illustration of initial authentication being delayed**

The delay in authentication being requested shown in the figure above is aided significantly by the data being gathered on a Sunday when the subject decided to stay at home. The green

authentication threshold indicates the relaxed approach to security that the Authentication Aura is taking, which in turn erodes confidence at its slowest rate. This attitude is then further enhanced by detected devices which immediately raise confidence to 25% upon activation and although it then drops below the threshold, the arrival of additional Aura members lifts the value to the capped maximum prior to the second service access being undertaken. This series of events alone encouragingly support the Authentication Aura concept and can be regarded as a significant success.

This section has introduced the simulations of the Authentication Aura that have been performed, in the next tranche of this chapter the results of extrapolated simulations are presented and the results mathematically analysed to review their significance.

## ***7.2 Assessment of Extended Simulation Results***

In the previous section graphs illustrating the simulations that have been carried out have been presented and the underlying variations discussed. However, to visually compare the adjustment in calculation parameters it has been necessary to repetitively illustrate a single user consistently. To ascertain a better understanding of the efficacy of the Authentication Aura it is appropriate to extrapolate the simulations across all experiment subjects for the entirety of their participation and mathematically assess the results; this section presents these findings.

When the Authentication Aura with the initial variable settings, and a higher location tariff as detailed earlier, were simulated the quantities of invoked authentications were recorded and are presented in Table 7-3 and Table 7-4 respectively.

Table 7-3 shows the number of simulated authentications for each user based on the scenario of a mobile phone with a ten minute screen lock and user invoked service access every 30 minutes. Compared to the baseline total of 8,448 authentications, during this simulation a total of 2,205 authentications were observed at an average rate of 8.38 per day with a standard deviation of 2.75 – a large variation. When examined the data reveals lowest and highest values of 4 and 16 authentications respectively and the total value is only 26.20% of the baseline quantity, representing an improvement of 73.80%. User 9's experiment data generated the greatest numerical saving of 384 fewer authentications, whilst in percentage terms subject 5 exhibited a reduction of 83.04 %.

User	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
<b>AUTHENTICATIONS</b>	14	9	15	16	8	12	13	14	6	16	8	8	7	8	7	10	7	8	9	7
	8	5	11	12	5	7	8	7	7	10	9	12	9	14	9	10	8	10	9	8
	8	5	5	8	4	7	9	7	5	6	9	9	5	11	9	10	7	8	9	7
	6	6	7	12	5	7	8	6	6	6	13	11	6	5	7	9	7	11	9	7
	5	5	6	12	4	8	5	5	8	7	5	6	5	9	11	13	10	10	11	11
	6	8	5	16	6	5	7	5	8	6	7	7	8	7	8	15	6	10	11	9
	6	12	8		6	5	11	5	6	8	6	6	12	7	7	11	9	7	9	6
	13	5	8			7	8	9	5	14	7	16	10	7	8	11	7	10	9	7
	13	6	9			8	11	8	5	5	8		9	11	10	15	7	6	8	6
	6	6	7			5		8	6	7	8		10	11	8	12	8	8	8	7
	7	6	7			7		8	6		5		5	12	9	10	8	8	7	10
	5	6	7			9		7	6		10		5	7	7	12	6	10	13	10
	5	6	4			6		11	4		7		8	8	10	14	9	9	7	6
	7	5	7			8		5	5		7		9	7	10	11	8	9	13	8
9		9			13		16	13		16			13	15	12	12	11	11	11	
<b>Total</b>	118	90	115	76	38	114	80	121	96	85	125	75	108	137	135	175	119	135	143	120
<b>Baseline</b>	480	448	480	192	224	480	288	480	480	320	480	256	448	480	480	480	480	480	480	480

Table 7-3. The number of simulated authentications shown per user per day

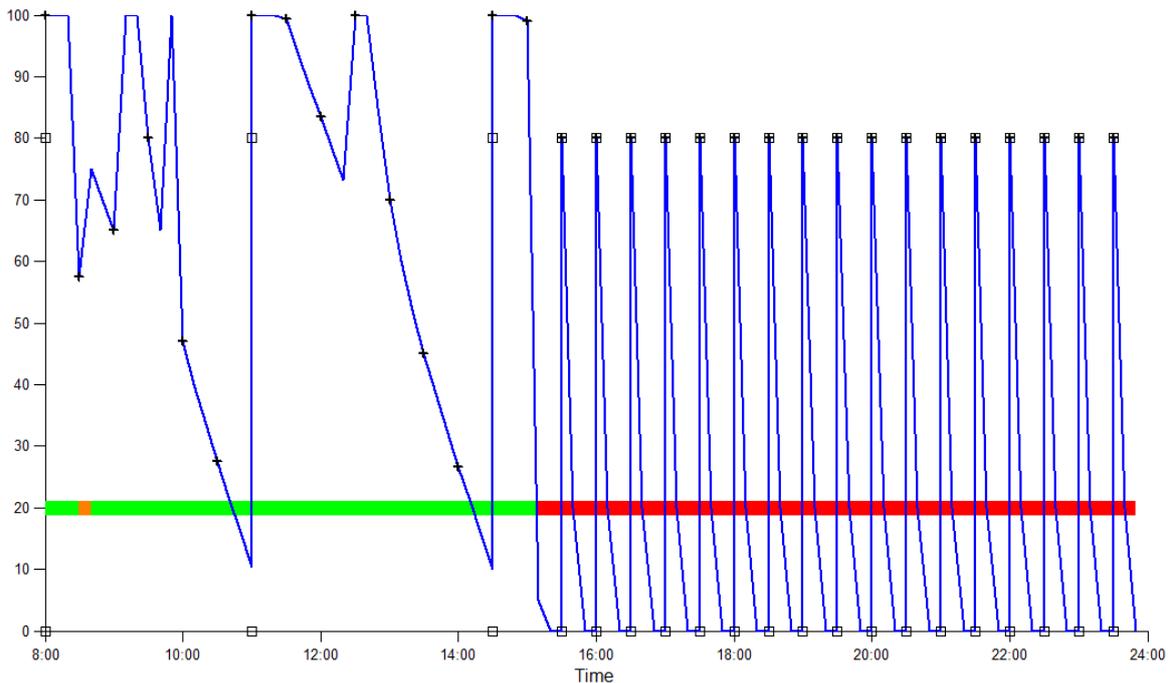
User	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
<b>A U T H E N T I C A T I O N S</b>	26	16	30	32	10	20	24	28	6	31	14	13	12	12	10	20	13	12	15	11
	9	6	19	20	5	9	12	9	7	16	13	22	12	28	14	17	13	17	16	9
	8	6	5	9	4	9	11	9	6	10	14	13	5	21	13	21	13	10	17	8
	8	4	5	22	5	9	10	8	9	7	23	20	5	5	10	19	12	22	15	8
	5	6	6	20	4	10	5	5	11	8	5	6	5	15	14	25	15	25	20	23
	6	13	5	31	8	6	10	5	11	7	11	8	13	12	10	27	9	17	17	6
	8	22	12		8	6	18	5	6	17	11	6	20	12	10	17	15	10	16	6
	26	8	10			10	10	14	5	26	12	32	16	11	10	21	11	23	16	11
	8	4	12			9	17	14	5	5	13		12	20	15	28	12	9	15	10
	8	4	12			5		14	8	11	12		16	19	11	19	12	17	15	11
	10	4	8			9		13	7		5		5	21	16	20	12	9	14	8
	6	3	11			14		10	9		18		5	10	9	20	8	5	26	12
	6	4	4			7		21	4		12		13	12	18	24	14	18	10	9
	11	6	9			12		5	7		12		11	12	18	20	13	12	24	11
	16		12			22		31	24		30			24	30	22	23	23	24	21
<b>Total</b>	161	106	160	134	44	157	117	191	125	138	205	120	150	234	208	320	195	229	260	164
<b>Baseline</b>	480	448	480	192	224	480	288	480	480	320	480	256	448	480	480	480	480	480	480	480

Table 7-4. The number of simulated authentications with higher location tariffs shown per user per day

User	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
<b>AUTHENTICATIONS</b>	26	18	30	32	14	21	24	29	8	32	16	13	15	15	13	21	13	17	18	15
	15	9	21	21	7	11	13	10	10	18	14	23	17	28	18	21	14	20	17	17
	13	13	7	11	7	12	14	11	8	11	14	15	7	23	15	21	13	17	17	14
	12	11	19	22	7	12	13	10	11	12	24	21	9	7	11	21	13	23	17	15
	7	9	10	20	7	12	7	7	12	12	7	7	7	16	22	25	16	26	20	24
	7	16	7	31	15	8	11	7	11	12	13	9	16	13	13	29	9	19	17	16
	12	24	20		13	8	19	7	7	18	13	7	22	15	13	21	15	15	17	15
	27	13	16			12	13	16	7	26	13	32	19	12	14	22	13	25	17	15
	29	12	21			12	19	14	7	7	14		18	21	17	30	13	15	16	14
	10	12	19			7		15	10	15	13		18	20	14	24	13	20	16	14
	13	11	18			12		14	9		7		7	22	17	21	13	16	15	22
	7	12	14			17		12	11		19		7	12	10	23	10	25	26	23
	7	12	7			9		22	7		13		20	14	20	24	16	19	12	11
	14	9	18			13		7	9		13		19	14	19	22	14	22	24	16
17		20			24		32	25		30			25	31	24	24	24	24	24	
<b>Total</b>	216	181	247	137	70	190	133	213	152	163	223	127	201	257	247	349	209	303	273	255
<b>With Aura</b>	161	106	160	134	44	157	117	191	125	138	205	120	150	234	208	320	195	229	260	164
<b>Baseline</b>	480	448	480	192	224	480	288	480	480	320	480	256	448	480	480	480	480	480	480	480

Table 7-5. The number of simulated authentications with higher location tariffs but without influence from the Aura

The discussion presented earlier relating to Figure 7-21 and the use of higher location weightings, suggested a tariff of 10 when the subject was at work and 30 when they were in an alien environment. Extending this simulation across all subjects produced the figures shown in Table 7-4; 3,418 polled authentications at a mean daily rate of 13.00 but with an extremely high standard deviation of 6.76. In this scenario, surprisingly the lowest number of authentications was 3 and the highest 32, a maximum figure equivalent to having no benefit from the Authentication Aura whatsoever. However, during the simulations if any devices were detected at some point during a given day, the entire day was incorporated into the results. Thus, if after an hour's use the PDA sensor's battery went flat and the device deactivated for the remainder of the day, as long as one other device had been detected during the operational hour, the simulation would indicate that for 15 hours the subject was in an alien environment without any other Aura devices nearby, incurring a large quantity of authentications. This factor means that the presented average daily value will be higher than the true operational value, and even with a 59.39% improvement on the baseline the support it offers for the efficacy of the Authentication Aura in reducing the quantity of required user interventions is even greater. This effect is demonstrated in Figure 7-26 below.



**Figure 7-26. Example of a device that becomes inactive part way through a day**

In the above example subject number 14's PDA possibly became inactive at approximately 3.30pm and so for the remainder of the day a maximum number of authentications have been simulated even though the device would not have been working, skewing the results.

Using the high location weightings (i.e. home=2.5, work=10 and away=30) should intuitively have more of an impact upon the working week when more time is spent away from home, as

opposed to the weekend. If the weekdays and weekends are analysed separately with these high tariffs the simulation produces average daily authentication requests of 13.54 and 11.42 respectively but with extremely high standard deviations of 6.56 and 7.12. This analysis underlines how the Authentication Aura gains more advantage when operating in a familiar and trusted environment, although there is a higher variation in readings during the weekend because it is likely subjects moved from high safety (at home) to high risk (away from home) more frequently. For comparison and completeness when the same analysis is performed using the default parameters an average of 8.59 for weekdays and 7.79 for weekends was observed but with improved standard deviations of 2.65 and 2.93.

One of the fundamental principles of the collective approach utilised by the Authentication Aura is the influence of the member devices and the contribution to the host's identity confidence that they make. To establish how much additional confidence they offer the simulation was re-run, across all days but still with the high location weightings, and the only incorporated effect was the influence of location, both token and intelligent contributions were ignored. This simulated activity returns the results collated in Table 7-5 on page 173 and for ease of comparison the totals from the simulation including the Aura's influence (Table 7-4) have been included.

This simulation reveals an extremely large variation in the influence of other Aura members. For subject 4 the location influence is significantly reducing the number of authentications from a baseline of 192 to 137, however the inclusion of the Aura only reduces this figure by a further three authentications across their entire experiment participation. The Aura effect is numerically greatest for user 20 who had their baseline authentications reduced from 480 to 255 initially by location but then by an additional 91 with the inclusion of the Aura. In percentage terms subject 2 exhibited the largest improvement through the Aura's influence with a drop of 41.44% from 181 to 106; the average reduction in the number of authentications was 17.89%. Overall the total daily number of authentication requests without the Aura influence was 4,146 with a mean daily value of 15.76 and a standard deviation of 6.20. These figures certainly support the principle of the Authentication Aura and suggest that even when at greatest risk it offers a significant improvement upon traditional security.

### ***7.3 Lexical Emulation***

Part of the proposed framework outlined the message interchange that would have to occur between cooperating member devices to enable the Authentication Aura to function. To investigate the efficacy of the message syntax and vocabulary, a lexical emulator has been developed and run on a laptop computer using the gathered experiment data as input. The

program utilised a user specified time, day and subject, and then proceeded at given time intervals, introducing new devices as they were sensed, and removed them when their detection ceased. The operator could interactively create the host device and control the strength of authentication it used. As the Aura operated and the confidence of the incorporated devices altered, the effect was observed.

Figure 7-27 illustrates a screen shot that was captured whilst the lexical emulation was running. The top portion of the screen represents a control panel with which the user interacts to adjust various parameters such as date, time, user, authentication threshold and whether or not authentication is performed automatically. Intelligent devices are created in a large window, and token equipment in smaller windows with just a close button for control. The background colour of the intelligent devices window reflects the current confidence held and changes at 20% intervals during degradation, from green to red. In the example above, the 'Mobile Phone #0000007056' host device was created manually during operation and with a confidence level of 53% is displayed with an amber background. The remaining devices were created automatically by the emulator using the experiment data for User 1 on Day 3. On the host device the list box labelled 'A' displays the intelligent elements of the active Aura, whilst the one labelled 'T' shows the token devices. The 12 character hexadecimal codes shown in these two list boxes represent the RFID tags of the devices captured and stored in the experiment data.

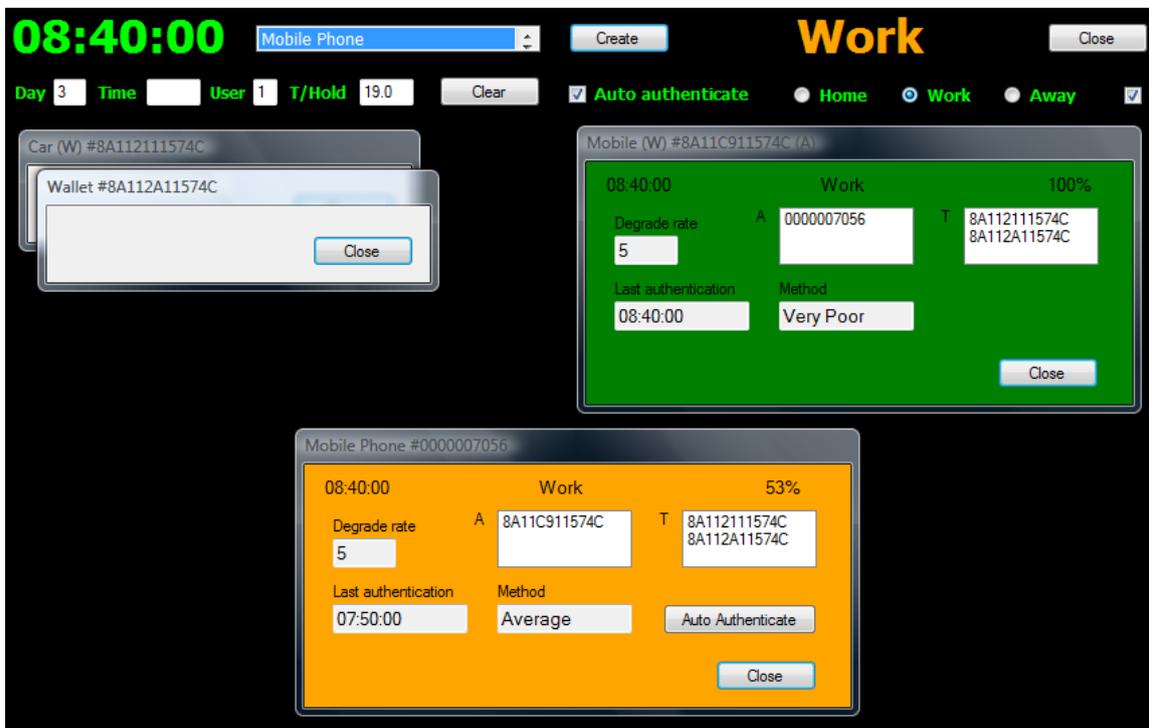


Figure 7-27. Screen capture during operation of the lexical emulation

Within the operation of this emulation, the data is only used to create and delete devices in isolation; they discover each other and trade information using the vocabulary specified. A device is created as a self contained instance of a compiled program and has no knowledge of those invoked either before or after, it learns independently. Empirically the vocabulary appears sufficient and able to support the proposed communication, and the status of each Aura member indicates information exchange is functioning well. During operation the folder through which information passed dynamically showed message arrival and collection, and also the replies to requests for detail. It fully supports the concept and proposed framework logic.

One further benefit observed during the production of the software was the structure imparted by the proposed framework. With distinct processes identified it naturally dictated the separation of the code into structured internal functions, each with its own role and responsibilities. This subdivision of functionality and approach performed well, creating a program that was easy to maintain and debug, whilst reinforcing the design integrity of the framework.

#### **7.4 Summary**

This chapter has reported the results recorded during an extensive investigation into the Authentication Aura concept and how it might reduce the burdensome requirement to repeatedly re-authenticate on a mobile device during regular daily use. Mathematical modelling software has been used to simulate a functioning Authentication Aura and gauge the influence of parameter alteration upon a single user, and then extrapolated across all users.

The reproduced graphs have given a visual indication to the detected improvement in performance with subjects' data showing up to an 80.36% reduction in requests for authentication even when the higher location weightings were used, imitating a risk averse user. These results were further supported by the extraction of quantitative results that mathematically illustrate the observed improvements and support the acceptance of the hypothesis proposed in section 7.1. There is indeed a significant reduction in the number of simulated authentications; Table 7-3 presents the results for all users across the entirety of their experiment participation, and indicates a drop from 8,416 authentications to 2,205 - a decrease of 73.8%.

Although a large amount of data was harvested from the experiment some anomalies have surfaced which appear to have been caused by device failure or user misuse. The effect of this upon the discussed calculations is to adversely influence the results because of the failsafe

approach that the simulation takes in defaulting the user to an alien environment, divested of the assurance contribution from other Aura members.

An additional simulation illustrated how the Authentication Aura would respond to theft, should the host device be removed by an unscrupulous individual. In contrast to traditional security that would not be invoked if regular use was maintained or screen lock deactivated, this new approach reached an entirely unusable and secure state within twelve minutes based on the parameters and timeframe used. In normal functioning with a realistic timeframe (much less than the simulated ten minutes), these findings suggest that the response would be rapid providing assurance to the owner.

A secondary emulation technique was used to investigate the message and status logic that was outlined as part of the framework. This second exploration further supported the proposals and illustrated that the vocabulary was sufficient to fulfil its requirements.

The results produced during this investigation have gone further to reinforce the novel concept of an Authentication Aura, illustrating how user controlled parameters can be altered to adjust its response to threat and just how assured in performance it is. The following chapter will review the work presented in this document as a whole and proceed by outlining future work and the path to developing a fully functioning prototype.

---

## **Chapter 8**

## **Conclusion**

---

## 8. Conclusion

---

Now that the research has been presented and the analysis detailed, this final chapter will review the work that has been undertaken, discuss some of the wider issues and implications, and assess the extent to which it has met its aims and objectives that were specified in Chapter 1.

The scope of the project has been to establish through experimentation and analysis what potential existed in the portable devices, familiar surroundings, and possessions that individuals carry for the formation of a novel approach to user authentication, and then to design and test a framework by which an implementation could be built in the future. It was proposed that, if successful, such an approach would reduce the number of intrusive authentications required by a user during normal device usage, and additionally in some instances remove the need to authenticate altogether. The project required an experiment to capture data from sets of co-workers that could be used to test the proposed hypotheses, based upon normal daily activity and across multiple locations. Although prior works have been conducted in the field of non-intrusive mobile security, the Aura research has not built directly upon them, and has been independently scoped and executed, leading to an entirely autonomous and novel thesis.

Given the nature of the proposed approach, it is worth briefly reflecting upon the related issues that may be raised from the legal, ethical, and social standpoints. From the legal perspective, one should consider how the user's activities would come to be monitored, and what data would then be collected. Should it be adopted and implemented to a large degree, it is anticipated that such an approach would be offered as a selectable alternative that would most likely be pulled by the user from an app repository. It is unlikely to be an all-or-nothing option that was presented to any mobile device owner. The data it gathers and uses within its operation is either from open and readily available infrastructure, or exchanged between trusted and (in the majority) owned devices. There is nothing that is required to be covert in its actions, with the only encryption occurring during the potential transfer of biometric data samples.

Equally it is not considered that the framework in isolation poses any ethical issues. Although it proposes to utilise biometric techniques to attain unobtrusive authentications where required, which may in themselves raise ethical issues, the framework per se does not. It should be the responsibility of any underlying biometric system to manage and secure the individual's

---

identity template, and (assuming an appropriately robust implementation) the Aura framework itself should not introduce an additional basis for exposure.

Similarly there are no significant social issues within the operating framework. During its operation any information received into the framework is only ever used to establish location or as part of the user's confidence calculation; each is appropriately incorporated near instantaneously and then discarded. There is a complete absence of data logging and location tracking that could potentially impinge upon privacy and social identification. Additionally the framework does not have access to, or require use of, any specific personal information during operation, merely the details outlined above.

The remainder of this chapter further reviews the undertaken work and takes a pragmatic view of some of the shortcomings of the research, discussing the implications these may have had for the results before finally outlining future work and how the research could proceed from this point.

### ***8.1 Fulfilment of the Aims and Objectives***

Upon reviewing the aims and objectives that were set out at the beginning of this document it is clear that specified details have indeed been met and satisfied by the executed work. Initially a full review of the evolution of mobile devices and personal electronic equipment was performed, to provide a foundation to the research and gauge the development towards this current point-in-time. It is certainly remarkable to revisit what is relatively recent history and review how these now ubiquitous devices have pervaded into everyday life. With the continuing fulfilment of Moore's Law and the inherent capability it delivers, the future is one that is full of potential.

Building upon the review of technology and to provide further understanding, an exhaustive investigation of the true meaning of identity was made in Chapter three, revealing how it is perceived both philosophically and psychologically. The work revealed how identification is founded upon two key issues, awareness of the traits that are unique to the subject and persistence of those traits over time. Although it could be argued that this exploration was outside of the scope of this project, the understanding it gave supported the research and highlighted the uniqueness of the individual. Indeed, some of the intricacies of this area could also be incorporated into the framework as a means of ongoing authentication. Behavioural psychometrics could well provide a method of individuation, and allow further developments to harness this approach to identity confirmation.

---

Chapter three then continued by examining the current state of authentication and the techniques that are employed on state-of-the-art devices, revealing some of the inherent weaknesses and opportunities for improvement. These elements met the criteria specified in the first aim and objective, and indeed provided knowledge that advanced the research.

To assess the proliferation of an individual's items of electronic devices and possessions and to gauge the suspected information their presence contains, an experiment was designed and executed. Twenty experiment subjects were recruited who undertook the two week experiment in four groups of five individuals, selected so that during the experiment at times they would encounter each other and concurrently occupy the same location. Each person was equipped with an RFID tag reader and tags to label equipment and personal possessions both at home and in the workplace. Data was gathered every minute around the clock and yielded 1,576,340 readings at an average of 78,817 per subject. The associated analysis revealed the extent to which people are surrounded by items, their Aura, which could be detected and used to identify location; it led to the suggestion that inert devices might actually be more significant than previously considered. It also clearly supported the premise that this Aura could be used in a novel cooperative approach to security and satisfied the second aim and objective. In an ideal situation, additional sets of subjects would have been recruited to provide a greater data set. However, the resultant size was deemed sufficient to yield statistically significant analysis and a robust set of results.

The research carried out an extensive examination of user identity confidence and how this could be influenced by location and the user's Authentication Aura. Degradation of service availability based upon the identity confidence was also investigated and a skeleton equation that would satisfy the proposal was outlined. The true novelty of this research stems from the proposal to use both location and cooperative data from other owned devices to contribute to the user's identity confidence, enabling it to react to an individual's movement and even theft of the host device.

The next aim and objective was met by the detailed explanation of the Authentication Aura's framework. This extremely detailed work examined the processes, databases, operational logic and communication vocabulary required to produce a functioning Authentication Aura. Taking a top down approach, it firstly introduced the anatomy of a software agent capable of performing the required tasks, and then proceeded to explain the autonomous processes contained within it. A communication vocabulary was presented which explained how information could be exchanged between participating devices, the effect of changes in status and how the associated triggers would be managed. To investigate this an emulation was

---

developed which lexically analysed this proposed vocabulary and provided a visual confirmation of the efficacy of the approach.

The final aim and objective was satisfied by the extensive mathematical modelling which was performed. This was used to simulate the detailed confidence equation and inter-device communication from the experiment data, producing numerous plots and statistics which illustrated that indeed an Authentication Aura did provide an improvement upon current security implementations. The performed simulations highlighted that location alone could be used to reduce the number of baseline intrusive authentications experienced by a user by 50.74%, and when the influence of the Authentication Aura was incorporated the inconvenience was lessened by a further 17.56%.

The simulation further supported the novel idea that under certain circumstances authentication following activation of a device could be delayed if sufficient imparted confidence was received from a user's Aura. Within the analysis one user was found to have had their first authentication delayed by up to 90 minutes, a significant improvement and reduction in inconvenience.

During the course of the research a number of peer-reviewed papers have been produced and presented at conferences and also accepted into journal publications. These are provided in Appendix C at the back of this document and include one that received a 'best paper' award, because of the work's novelty and the progress it brought to this field of research.

## ***8.2 Research Limitations***

With the aims and objectives of this research being met the project as a whole is deemed to be a success. However, as with any project there are some issues and limitations that may have impacted upon the findings to varying degrees and these are detailed in the section below.

The research experiment was conducted to ascertain the profile and quantity of devices, possessions and infrastructure that surround people during their daily lives. Any statistical investigation requires as many participants as possible to yield results that are regarded as significant and robust to scrutiny. Selecting a data gathering method that used RFID technology satisfied the requirements but was achieved with substantial financial cost. This available budget restricted the number of concurrent subjects that could be enrolled to five and subsequently limited the quality of the collected data. Each participant was only allocated 15 RFID tags and requested to divide these between home and work, fewer than in an ideal scenario.

The obtained active RFID tags were constructed with an onboard battery which provided them with the ability to remain continually active. However, they were constructed with an open battery slot to permit easy exchange of batteries but in some instances the experiment subjects dislodged the batteries or moved them sufficiently to stop the tag transmitting, rendering the tag powerless for the duration of the project and barring its inclusion in the survey.

Participants were unfortunately required to ensure that the PDA RFID readers remained charged for the duration of the experiment. The restricted battery life of the units resulted in them needing to be recharged twice every day, once overnight but also during waking hours as well. Although higher capacity batteries were purchased the additional weight of these caused them to detach from the back of the device and were only successfully used by a couple of the participants. These two issues combined to create periods of time when the PDAs were without power and data was missed. The times when this occurred are clearly evident in the gathered dataset and although during the simulation these periods are treated as worst case scenarios (time when the user is in an alien environment, out of range of any other owned devices) they have not impacted significantly upon the experiment's success.

Although as discussed the collected data was compromised to some degree there was still an extremely large volume collected. The number of daily observations for an individual has in turn slightly impacted upon the analysis that could be performed and for clarity the graphs were plotted in ten minute time-slices, reducing some of the detail that might otherwise have been available.

Finally, in the modelled simulation identical parameters were applied across all devices as they were encountered. This of course is not a completely accurate representation of real life because different devices would have differing setups and methods of authentication. Even so, the simulation was inclusive and reassuringly confirmed the potential of the Authentication Aura.

### **8.3 Future Work**

This research has proved that there is scope for a cooperative approach to mobile device security that can improve user convenience and even delay required authentication upon activation. Mathematical modelling and simulation have quantified potential improvement and demonstrated how knowledge can be shared amongst Aura members. The next step in future work would be the development of a fully functioning prototype that could be installed upon a set of devices to further test efficacy. This work has a solid foundation in the detailed

---

framework specification contained within Chapter 6 and is a natural progression from the research performed so far.

Additional exploration into the simulation would also further refine the observed results. Adapting the utilised simulation routine to incorporate different operational parameters for each device as discussed in section 8.2 would provide a more realistic set of results, truer to a real life implementation. It is anticipated however that with some devices operating more restrictively and others less so, the resultant effects would potentially balance themselves out and not severely alter the findings but merely provide an enhanced degree of confidence.

Another area of future work is the further investigation of distributing authentication across devices. If one device can capture data but is incapable of processing it, the framework has outlined how this information could be communicated to another device that has the necessary capability to perform the authentication and then return the outcome. To confirm the suitability of this approach a practical investigation is required and a trial performed.

With additional investigation into methods of user identification such as habitual behaviour, scope exists to provide new ways in which the user's surroundings and actions could be incorporated into the Authentication Aura framework. Although the novelty of the framework is founded upon its cooperative nature, these types of approach to identification can bring an additional layer of sophistication that will aid its operation when in isolation. Leveraging the information that can be ascertained from the user's environment can only support the degree of accuracy to which the framework operates and the speed of response.

These elements of work present significant opportunity to advance this research to the next level and further substantiate the Authentication Aura as an improvement upon traditional methods of mobile device security.

#### ***8.4 The Future for User Authentication on Mobile Devices***

With the proliferation of mobile devices and smartphones offering ubiquitous connectivity, these high cost items have become an essential piece of equipment in both personal and business life. With owners utilising them for banking, email and storing personal information, in addition to making telephone calls and sending text messages, the need to protect these devices becomes evermore important.

Although mechanisms are in place in an attempt to provide a secure means of access, the unwillingness or inability of owners to implement these rigorously is an inherent risk. Typical security is point-of-entry and once passed unrestricted access is available to the user, providing them with the opportunity to roam freely through the information contained within.

When timed barriers are invoked, with individuals porting a number of devices concurrently the associated inconvenience of multiple authentications is an inescapable burden which must be fulfilled.

The future of user authentication on mobile devices will have to consider all of these factors whilst ensuring its ease of implementation and ability to adapt to future requirements. With the introduction of smart glasses and watches, the human love of technology and its dependence upon it is only ever going to grow. It is the responsibility of those within the security arena to ensure this happens in the most secure way possible, and methods that are continuous and imperceptible to the user will be centric to the solution.

---

## References

---

## References

---

- [1] Ahmed, A. A. E. and Traore, I. (2007), 'A New Biometric Technology Based on Mouse Dynamics', *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 3, pp. 165-179
- [2] Albrechtsen, E. (2007), 'A Qualitative Study of Users' View on Information Security', *Computers and Security*, vol. 26, no. 4, pp. 276-289
- [3] Amatrudo, A. (2008), 'Understanding Subject(s): The Self As Corporation', *The Heythrop Journal*, vol. 49, no. 3, pp. 423-441
- [4] Ang, T. (2008), 'The Advantages And Disadvantages for Using Bluetooth', *Cellware website*, available: <http://cellware.blogspot.co.uk/2008/04/advantages-and-disadvantages-for-using.html>  
[accessed: 17 Jun 14]
- [5] Anthony, S. (2014), 'Samsung Galaxy S5 unveiled: Fingerprint scanner, 16-megapixel camera, but still a plastic body', *ExtremeTech website*, 24<sup>th</sup> February 2014, available: <http://www.extremetech.com/computing/177119-177119>  
[accessed: 25 Nov 14]
- [6] Apple (2010), 'iPhone Specifications', *Apple website*, available: <http://support.apple.com/kb/sp2>  
[accessed: 01 Mar 14]
- [7] Apple (2014), 'Touch ID: Security. Right at your fingertip', *Apple website*, available: <https://www.apple.com/iphone-6/touch-id/>  
[accessed: 17 Nov 14]
- [8] APWG (2014), 'APWG Phishing Attack Trends Reports', *APWG*, available: <http://www.antiphishing.org/resources/apwg-reports/>  
[accessed: 27 Jun 14]
- [9] Arandjelovic, O., Hammoud, R. and Cipolla, R. (2006), 'Multi-Sensory Face Biometric Fusion (for Personal Identification)', *Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*
- [10] Araújo, L. C. F., Sucupira Jr., L. H. R., Lizárraga, M. G., Ling, L. L. and Yabu-Uti, J. B. T. (2005), 'User Authentication Through Typing Biometrics Features', *IEEE Transactions on Signal Processing*, vol. 53, no. 2
- [11] Ask.com (nd), 'What are the percentages of different eye colors?', *Ask.com*, available: <http://uk.ask.com/question/eye-color-percentages>  
[accessed: 25 May 14]
- [12] AT & T (2012), '1946: First Mobile Telephone Call', *AT & T*, available: <http://www.corp.att.com/attlabs/reputation/timeline/46mobile.html>  
[accessed: 10 May 12]
- [13] Atkins, V. (2014), 'Global government biometrics market to reach \$6.9 billion by 2024', *Silicon Trust website*, 31<sup>st</sup> March 2014, available: <http://silicontrust.wordpress.com/2014/03/31/global-government-biometrics-market-to-reach-6-9-billion-by-2024/>  
[accessed: 22 Nov 14]

- 
- [14] AuthenticationWorld.com (2006), 'Authentication Strength', *Authenticationworld.com*, available: <http://www.authenticationworld.com/Authentication-Strength/> [accessed 11 Apr 13]
- [15] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M. and Smith, J. M. (2010), *Proceedings of the 4th USENIX Workshop On Offensive Technologies (WOOT)*, Washington DC, USA, 11-13 August 2010
- [16] Baker, T. (2011), 'Up to what distance can near field communication (NFC) operate?', *quora .com*, 4<sup>th</sup> May 2011, available: <http://www.quora.com/Up-to-what-distance-can-near-field-communication-NFC-operate> [accessed: 13 Jun 14]
- [17] Barnett, S. (2004), 'Jeff Hawkins: The man who almost single-handedly revived the handheld computer industry', *Pen Computing*, June 2004, available: <http://www.pencomputing.com/palm/Pen33/hawkins3.html> [accessed: 20 Feb 14]
- [18] Bartolacci, G., Curtin, M., Katzenberg, M., Nwana, N., Cha, S. and Tappert, C. (2005), 'Long-Text Keystroke Biometric Applications over the Internet', *Proceedings of Student /Faculty Research Day, CSIS, Pace University*
- [19] Bayometric (2013), 'How Biometric Voice Authentication system works', *Bayometric website*, available: <http://www.bayometric.com/blog/how-biometric-voice-authentication-system-works-2/> [accessed: 19 Nov 14]
- [20] Bazin, A. I., Middleton, L. and Nixon, M. S. (2005), 'Probabilistic Fusion of Gait Features for Biometric Verification', *Eighth International Conference of Information Fusion*, Philadelphia, USA, 25-28 July 2005
- [21] BBC Online (2004), 'Passwords Revealed by Sweet Deal', *BBC website*, available: <http://news.bbc.co.uk/1/hi/technology/3639679.stm> [accessed: 14 Mar 08]
- [22] Bellis, M. (nd), 'Inventors of the Modern Computer', *About.com Inventors*, available: <http://inventors.about.com/library/weekly/aa120198.htm> [accessed: 05 May 12]
- [23] Beranek, B. (2014), 'Biometrics on the smartphone: The future of mobile authentication', *Nuance website*, 10<sup>th</sup> February 2014, available: <http://whatsnext.nuance.com/customer-experience/biometrics-smartphone-future-mobile-authentication/> [accessed: 24 Jun 14]
- [24] Bergadano, F., Gunetti, D. and Picardi, C. (2003), 'Identity Verification Through Dynamic Keystroke Analysis', *Intelligent Data Analysis*, vol. 7, pp. 469-496
- [25] Biometric-Solutions.com (2013a), 'Fingerprint Recognition', *Biometric-Solutions.com*, available: [http://www.biometric-solutions.com/solutions/index.php?story=fingerprint\\_recognition](http://www.biometric-solutions.com/solutions/index.php?story=fingerprint_recognition) [accessed: 20 Nov 14]
- [26] Biometric-Solutions.com (2013b), 'Face Recognition', *Biometric-Solutions.com*, available: [http://www.biometric-solutions.com/solutions/index.php?story=face\\_recognition](http://www.biometric-solutions.com/solutions/index.php?story=face_recognition) [accessed: 20 Nov 14]
-

- [27] Biometric-Solutions.com (2013c), 'Iris Recognition', *Biometric-Solutions.com*, available: [http://www.biometric-solutions.com/solutions/index.php?story=iris\\_recognition](http://www.biometric-solutions.com/solutions/index.php?story=iris_recognition) [accessed: 21 Nov 14]
- [28] Birget, J. C., Hong, D. and Memon N. (2005), 'Graphical passwords based on robust discretization', *IEEE Transactions on Information Forensics and Security*, vol. 1 no. 3 pp. 395-399
- [29] Blatti, S. (2007), 'Animalism and Personal Identity' in M. Berkoff and J. Nystrom (Eds.), *Encyclopedia of Human-Animal Relationships* vol. 2, pp. 430-33, Greenwood Press
- [30] Block, R. (2007), 'iPhone Review', *Engadget UK*, 3<sup>rd</sup> July 2007, available: <http://www.engadget.com/2007/07/03/iphone-review/> [accessed: 01 Mar 14]
- [31] Bluetooth (2014), 'Bluetooth Basics', *Bluetooth website*, available: <http://www.bluetooth.com/Pages/Basics.aspx> [accessed: 19 May 14]
- [32] Bonneau, J. and Preibusch, S. (2010), 'The Password Thicket: Technical and Market Failures in Human Authentication on the Web', *The Ninth Workshop on the Economics of Information Security (WEIS 2010)*, Harvard University, Cambridge, Massachusetts, USA, 7-8 June 2010
- [33] Briggs, P. and Olivier, P. L. (2008), 'Biometric daemons: authentication via electronic pets', *Proceedings of conference on human factors in computing systems (CHI 2008)*, Florence, Italy, 5-10 April 2008, pp. 2423-32
- [34] Brostoff, S. and Sasse, M. A. (2000), 'Are Passfaces More Usable Than Passwords? A Field Trial Investigation', *Proceedings of HCI 2000 - People and Computers XIV*, pp. 405-424
- [35] Buck, S. (2013), 'Cell-ebration! 40 Years of Cellphone History', *Mashable*, available: <http://mashable.com/2013/04/03/anniversary-of-cellphone/> [accessed: 30 Jan 14]
- [36] Bullo, N. J. and Rysiew, P. (2007), 'A study in the cognition of individuals' identity: Solving the problem of singular cognition in object and agent tracking', *Consciousness and Cognition*, vol. 16, pp. 276-293
- [37] Burnett, M. (2011), '10,000 Top Passwords', *xato.net website*, 20<sup>th</sup> June 2011, available: <https://xato.net/passwords/more-top-worst-passwords/#.VGlxWYfVv8s> [accessed: 19 Nov 14]
- [38] CBR (1989), 'Motorola Looks To Sew Up Premium Cellular Market With 9800X Mini-Phone', *Computer Business Review*, 2<sup>nd</sup> May 1989, available: [http://www.cbronline.com/news/motorola\\_looks\\_to\\_sew\\_up\\_premium\\_cellular\\_market\\_with\\_9800x\\_mini\\_phone](http://www.cbronline.com/news/motorola_looks_to_sew_up_premium_cellular_market_with_9800x_mini_phone) [accessed: 01 Mar 14]
- [39] CESG (2002), 'Common Criteria: Common Methodology for Information Technology Security Evaluation, Biometric Evaluation Methodology Supplement', *Biometric Evaluation Methodology Working Group, CESG*, p. 3
- [40] Cho, S., Han, C., Han, D. H. and Kim, H. I. (2000), 'Web-Based Keystroke Dynamics Identity Verification Using Neural Network', *Journal of Organizational Computing and Electronic Commerce*, vol. 10, no. 4, pp. 295-307

- 
- [41] Clarke, N. L. (2011), *Transparent User Authentication: Biometrics, RFID and Behavioural Profiling*, London: Springer-Verlag London Limited
- [42] Clarke, N. L. and Furnell, S. M. (2007), 'Advanced user authentication for mobile devices', *Computers and Security*, vol. 26, no. 2, pp. 109-119
- [43] Clarke, N. L., Furnell, S. M., Reynolds, P. L. (2002), 'Biometric authentication for mobile devices', *Proceedings of the 3rd Australian Information Warfare and Security Conference 2002 (IWAR 2002)*, Perth, Australia, 28-29 November 2002
- [44] Clarke, N. L., Karatzouni, S. and Furnell, S. M. (2009), 'Emerging challenges for security, privacy and trust', *Proceedings of IFIP/SEC 2009 - 24th International Conference on Information Security*, Pafos, Cyprus, 18-20 May 2009
- [45] Clarke, N. L. and Mekala, A. (2007), 'The application of signature recognition to transparent handwriting verification for mobile devices', *Information Management & Computer Security*, vol. 15, no. 3, pp. 214-225
- [46] Colon, A. (2013), 'Apple's facial recognition patent might allow you to unlock, control your device', *GigaOM website*, 3<sup>rd</sup> December 2013, available: <https://gigaom.com/2013/12/03/apples-facial-recognition-patent-might-allow-you-to-unlock-control-your-device/>  
[accessed: 25 May 14]
- [47] CompuServe (nd), 'Strange Fact About Blue-Eyed People', *CompuServe News*, available: <http://webcenters.netscape.compuserve.com/news/fte/blueeyedpeople/blueeyedpeople>  
[accessed: 25 May 14]
- [48] Computing History (2012), 'Computer Timeline', *Computing History*, available: <http://www.computinghistory.org.uk/cgi/computing-timeline.pl>  
[accessed: 05 May 12]
- [49] Connected Earth (nd.), 'The first true mobiles', *Connected Earth*, available: <http://www.connected-earth.com/Journeys/Firstgenerationtechnologies/Mobilecommunications/Thefirsttruemobiles/index.htm>  
[accessed: 10 May 12]
- [50] ContinuityCentral (2014), 'Risky Business: The State of Mobile Security in the UK', *ContinuityCentral website*, 14<sup>th</sup> August 2014, available: <http://www.continuitycentral.com/news07323.html>  
[accessed: 26 Aug 14]
- [51] Cozma, N. (2012), 'Use voice commands from the Samsung Galaxy S3 lock screen', *CNET website*, 15<sup>th</sup> October 2012, available: <http://www.cnet.com/how-to/use-voice-commands-from-the-samsung-galaxy-s3-lock-screen/>  
[accessed: 25 May 14]
- [52] CPP (2010), '"IFraud" Fuels Rise In Scam Phone Claims', *CPP Group*, available: <http://www.cppgroupplc.com/news/press-release.shtml>  
[accessed: 26 Feb 10]
- [53] Crawford, H., Renaud, K. and Storer, T. (2013), 'A framework for continuous, transparent mobile device authentication', *Computers and Security*, vol. 39, part B, pp. 127-136

- [54] Crawford, H. and Renaud, K. (2014), 'Understanding user perceptions of transparent authentication on a mobile device', *Journal of Trust Management*, vol. 1, no. 7
- [55] Crime Scene Forensics (nd), 'History of Fingerprints', *Crime Scene Forensics, LLC*, available: [http://www.crimescene-forensics.com/History\\_of\\_Fingerprints.html](http://www.crimescene-forensics.com/History_of_Fingerprints.html) [accessed: 20 Sep 13]
- [56] CSID (2012), 'Password Habits: A study of password habits among American consumers', CSID.com, available: [http://www.csid.com/wp-content/uploads/2012/09/CS\\_Password\\_Survey\\_FullReport\\_FINAL.pdf](http://www.csid.com/wp-content/uploads/2012/09/CS_Password_Survey_FullReport_FINAL.pdf) [accessed: 25 May 14]
- [57] Culzac, N. (2014), 'Voice recognition software may be convenient but it's also a security risk, expert warns', *The Independent*, 30<sup>th</sup> September 2014, available: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/voice-recognition-software-may-be-convenient-but-its-also-a-security-risk-expert-warns-9765200.html> [accessed: 17 Nov 14]
- [58] DARPA (2012), 'Active Authentication', *Defense Advanced Research Projects Agency (DARPA)*, available: [http://www.darpa.mil/Our\\_Work/I2O/Programs/Active\\_Authentication.aspx](http://www.darpa.mil/Our_Work/I2O/Programs/Active_Authentication.aspx) [accessed: 24 May 14]
- [59] DataGenetics (2012), 'PIN Analysis', *DataGenetics website*, 3<sup>rd</sup> September 2012, available: <http://www.datagenetics.com/blog/september32012/> [accessed: 13 May 14]
- [60] Delaney, I. (2013), '40 Years of Mobile Phones', *Nokia Conversations*, available: <http://conversations.nokia.com/2013/04/03/40-years-of-mobile-phones/> [accessed: 30 Jan 14]
- [61] De Luca, A., Hang, A., Brudy, F., Lindner, C. and Hussmann, H. (2012), 'Touch me once and i know it's you!: implicit authentication based on touch screen patterns', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2012)*, Austin, Texas, USA, 5-10 May 2012, pp. 987-996
- [62] Derawi Biometrics (2011), 'Gait', *Derawi Biometrics website*, available: [http://biometrics.derawi.com/?page\\_id=38](http://biometrics.derawi.com/?page_id=38) [accessed: 21 Nov 2011]
- [63] Design Council (2010), 'Design Out Crime: Hot Product Crime', *Design Council*, available: <http://www.designcouncil.org.uk/Design-Council/Files/Landing-pages/Design-Out-Crime/Hot-Product-crime/> [accessed: 02 Mar 10]
- [64] Donohue, B. (2013), 'Could Smart-Watches Replace Passwords as Authenticators?', *threatpost.com*, 14<sup>th</sup> February 2013, available: <http://threatpost.com/could-smart-watches-replaces-passwords-authenticators-021413/77534#sthash.GOSE9bb4.dpuf> [accessed: 25 May 14]
- [65] Dowland, P. S. and Furnell, S. M. (2004), 'A Long-term Trial of Keystroke Profiling using Digraph, Trigraph and Keyword Latencies', *Proceedings of IFIP/SEC 2004 - 19th International Conference on Information Security, Toulouse, France, 23-26 August 2004*
- [66] Down, M. P. and Sands, R. J. (2004), 'Biometrics: An Overview of the Technology, Challenges and Control Considerations', *Information Systems Control Journal*, vol. 4

- [67] Drummond, J. (2014), 'How the Samsung Galaxy S5 fingerprint scanner differs from Apple's Touch ID', *iphonehacks.com*, 26<sup>th</sup> February 2014, available: <http://www.iphonehacks.com/2014/02/samsung.html>  
[accessed: 24 May 14]
- [68] Dunphy, P., Heiner, A. P. and Asokan, N. (2010), 'A closer look at recognition-based graphical passwords on mobile devices', *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS 2010)*, Redmond, Washington, USA, 14-16 July 2010
- [69] Eadicicco, L. (2014), 'People Are Willing To Go To Extreme Lengths To Retrieve Their Stolen Smartphones', *Business Insider*, 7<sup>th</sup> May 2014, available: <http://www.businessinsider.com/smartphone-theft-statistics-2014-5?IR=T>  
[accessed: 28 Jun 14]
- [70] Easy Clocking (nd), 'What is Biometrics?', *Easy Clocking website*, available: [http://www.bioelectronix.com/what\\_is\\_biometrics.html](http://www.bioelectronix.com/what_is_biometrics.html)  
[accessed: 20 Nov 14]
- [71] EU (2005), 'Common Terminological Framework for Interoperable Electronic Identity Management' *European Union commissioned Study on Identity Management in eGovernment* prepared by Modinis available online <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf>  
[accessed: 20 May 08]
- [72] Fairchild Company History (2014), 'Monolithic Integrated Circuit Patented', *Fairchild*, available: <https://www.fairchildsemi.com/about-fairchild/history/#>  
[accessed: 25 Apr 14]
- [73] Fairhurst, M. C. (2003), 'Document Identity, Authentication and Ownership: The Future of Biometric Verification', *Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR 2003)*, Edinburgh, Scotland, 3-6 August 2003
- [74] FBI (nd), 'Iris recognition', *FBI website*, available: [http://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/biometric-center-of-excellence/files/iris-recognition.pdf](http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/iris-recognition.pdf)  
[accessed: 21 Nov 14]
- [75] Federal Reserve (2014), 'Consumers and Mobile Financial Services 2014', *Federal Reserve website*, available: <http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf>  
[accessed: 29 Nov 14]
- [76] Feldman, F. (1970), 'Leibniz and Leibniz' Law', *The Philosophical Review*, vol. 79, no. 4, pp. 510-522
- [77] FindBiometrics (2014), 'Vein Recognition Biometrics', *FindBiometrics website*, available: <http://findbiometrics.com/solutions/vein-recognition/>  
[accessed: 21 Nov 14]
- [78] Florencio, D. and Herley, C. (2007), 'A large-scale study of web password habits', 16<sup>th</sup> International World Wide Web Conference (WWW2007), Banff, Alberta, Canada, 8-12 May 2007
- [79] Fraley, R. C. and Roberts, B. W. (2005), 'Patterns of Continuity: A Dynamic Model for Conceptualizing the Stability of Individual Differences in Psychological Constructs Across the Life Course', *Psychological Review*, vol. 112, no. 1, pp. 60-74

- 
- [80] Freiberger, P. A. (2013), 'The Personal Computer Revolution', *Encyclopaedia Britannica*, available: <http://www.britannica.com/EBchecked/topic/130429/computer/216069/The-personal-computer-revolution> [accessed: 25 Apr 14]
- [81] Fritz, R. (nd), 'Internet Refrigerators: Also known as Net Fridges', *About Technology website*, available: [http://compnetworking.about.com/od/homeautomationsystems/a/internet-refrigerators\\_net-fridges.htm](http://compnetworking.about.com/od/homeautomationsystems/a/internet-refrigerators_net-fridges.htm) [accessed: 17 May 14]
- [82] Fujitsu (nd), 'PalmEntry Access Control System', *Fujitsu website*, available: <http://www.fujitsu.com/us/services/biometrics/palm-vein/pac.html> [accessed: 21 Nov 14]
- [83] Furnell, S. M., Clarke, N. L. and Karatzouni, S. (2008), 'Beyond the PIN: Enhancing user authentication for mobile devices', *Computer Fraud & Security*, vol. 2008, no. 8, pp. 12-17
- [84] Gamboa, H. and Fred, A. (2004), 'A behavioural biometric system based on human computer interaction', *Proceedings of SPIE, Orlando, Florida, USA, 12 April 2004*
- [85] Garcia, F. D., de Koning Gans, G., Muijers, R., van Rossum, P., Verdult, R., Schreur, R. W. and Jacobs, B. (2008), 'Dismantling MIFARE Cards' in S. Jajodia and J. Lopez (Eds.), *ESORICS 2008, LNCS 5283*, pp. 97-114, Berlin:Heidelberg
- [86] Gartner (2014a), 'Gartner Says Worldwide Tablet Sales Grew 68 Percent in 2013', *Gartner website*, available: <http://www.gartner.com/newsroom/id/2674215> [accessed: 20 Jul 14]
- [87] Gartner (2014b), 'Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments to Grow 4.2 Percent in 2014', *Gartner website*, available: <http://www.gartner.com/newsroom/id/2791017> [accessed: 20 Jul 14]
- [88] Gibson, J. J. (1979), 'The Ecological Approach to Visual Perception' Boston: Houghton Mifflin
- [89] Glass Almanac (2014), 'The History of Google Glass', *Glass Almanac*, available: <http://glassalmanac.com/history-google-glass/> [accessed: 01 May 14]
- [90] GlobalSecurity.org (2011), 'Voice Verification', *GlobalSecurity.org website*, 13<sup>th</sup> July 2011, available: <http://www.globalsecurity.org/security/systems/biometrics-voice.htm> [accessed: 19 Nov 14]
- [91] Golfarelli, M., Maio, D. and Maltoni, D. (1997), 'On the error-reject trade off in biometric verification systems', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, pp. 786-796
- [92] Gorman, M. (2013), 'Google patents new facial recognition technology to let users unlock phones with a wink and a smile', *Engadget UK*, 7<sup>th</sup> June 2013, available: <http://www.engadget.com/2013/06/07/google-face-unlock-facial-gesture-patent/> [accessed: 25 May 14]
- [93] Goodwin, R. (2013), 'The History of Mobile Phones: 1973 to 2007', *Know Your Mobile*, 3<sup>rd</sup> April 2013, available: <http://www.knowyourmobile.com/nokia/history-mobile->

- phones/19848 /history-mobile-phones-1973-2007/page/0/1  
[accessed: 22 Feb 14]
- [94] Grama, J. L. (2010), *Legal Issues in Information Security*, Sudbury, MA: Jones & Bartlett Learning
- [95] GSM Arena (2014), 'Nokia 1110', *GSM Arena website*, available: [http://www.gsmarena.com/nokia\\_1110-1187.php](http://www.gsmarena.com/nokia_1110-1187.php)  
[accessed: 01 Mar 14]
- [96] Halevy, R. (2014), 'How to Enable the "Picture Password" Lockscreen on BlackBerry 10.2.1', *Berry Review website*, available: <http://www.berryreview.com/2014/02/04/how-to-enable-the-picture-password-lockscreen-on-blackberry-10-2-1/>  
[accessed: 22 May 14]
- [97] HardwareZone (2011), 'The Evolving Windows Phone – A History of Windows Mobile to Windows Phone 7', *HardwareZone website*, available: <http://sites.hardwarezone.com/sg/windowsphone7/news/427/>  
[accessed: 01 Mar 14]
- [98] Harris, T. (nd), 'How Fingerprint Scanners Work', *HowStuffWorks website*, available: <http://computer.howstuffworks.com/fingerprint-scanner.htm>  
[accessed: 20 Nov 14]
- [99] Hayes, D. (2014), 'Why You Should Write Down Your Passwords and Never Reuse Them', *Press Up website*, available: <http://pressupinc.com/blog/2014/04/write-passwords-never-reuse/>  
[accessed: 25 May 14]
- [100] Hazas, M., Scott, H. and Krumm, J. (2004), 'Location-Aware Computing Comes of Age', *IEEE Computer*, vol. 37, no. 2, pp. 95-97
- [101] Heyce Technologies (2014), 'Biometric Face Recognition Systems – A New World of Touch Free Authentication', *Heyce Technologies website*, available: [http://www.heyce.com/face\\_recognition\\_systems.html](http://www.heyce.com/face_recognition_systems.html)  
[accessed: 28 May 14]
- [102] Hill, S. (2013), 'From J-Phone to Lumia 1020: A complete history of the camera phone', *Digital Trends*, 11<sup>th</sup> August 2013, available: <http://www.digitaltrends.com/mobile/camera-phone-history/#ixzz337BJYhqv>  
[accessed: 24 Apr 14]
- [103] Home Office (2009), 'Reducing Crime: Robbery', Home Office website, available: <http://www.homeoffice.gov.uk/crime-victims/reducing-crime/robbery/>  
[accessed: 27 Feb 10]
- [104] Howard-Spink, J. (2008), 'Future Quotes', *FutureScoping*, available: <http://www.futurescoping.com/Futurequotes.htm>  
[accessed: 17 Sep 12]
- [105] HSW (2000), 'What does GSM mean in a cell phone?', *How Stuff Works*, available: <http://electronics.howstuffworks.com/question537.htm>  
[accessed: 01 Mar 14]
- [106] IBG (2006), 'Which is the best biometric technology', *International Biometric Group*, available: [http://www.biometricgroup.com/reports/public/reports/best\\_biometric](http://www.biometricgroup.com/reports/public/reports/best_biometric)

- .html  
[accessed: 16 Sep 08]
- [107] Ibiblio.org (nd), 'Iris', *Ibiblio.org website*, available: <http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node119.html>  
[accessed: 21 Nov 14]
- [108] ICR (nd), 'Guide to Speaker Verification & Voice Biometrics', *ICR Speech Solutions & Services website*, available: [www.icr3s.co.uk/ajax.php?do=download&id=150](http://www.icr3s.co.uk/ajax.php?do=download&id=150)  
[accessed: 19 Nov 14]
- [109] IEEE Global History Network (2013), 'Transistors and the Computer Revolution', *IEEE*, available: [http://www.ieeeahn.org/wiki/index.php/Transistors\\_and\\_the\\_Computer\\_Revolution](http://www.ieeeahn.org/wiki/index.php/Transistors_and_the_Computer_Revolution)  
[accessed: 25 Jan 14]
- [110] ISO (nd), 'ISO Biometric standards', *ISO website*, available: <http://www.iso.org/iso/home/search.htm?qt=biometric+standards&sort=rel&type=simple&published=on>  
[accessed: 28 Nov 14]
- [111] Jakobsson, M., Shi, E., Golle, P. and Chow, R. (2009), 'Implicit authentication for mobile devices', *Proceedings of the 4th USENIX Conference on Hot Topics in Security*, Berkeley, California, USA, August 2009
- [112] Jain, A. K., Ross, A. and Pankati, S. (2006) 'Biometrics: A Tool for Information Security', *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125-143
- [113] Jansen, W., Gavrilu, S. and Korolev, V. (2005), 'Proximity-based Authentication for Mobile Devices', *Proceedings of The 2005 International Conference on Security and Management (SAM'05)*, Las Vegas, Nevada, USA, 20-23 June 2005
- [114] Jansen, W., Gavrilu, S., Korolev, V., Heute, T. and Seveillac, C. (2004), 'Proximity-based Authentication for Mobile Devices', *Proceedings of The 2004 International Conference on Security and Management (SAM'04)*, Las Vegas, Nevada, USA, 21-24 June 2004
- [115] Jansson, K. (nd), 'First in the world with 4G', *TeliaSonera History*, available: <http://www.teliasonerahistory.com/pioneering-the-future/pioneering-the-future/first-in-the-world-with-4g/>  
[accessed: 01 May 14]
- [116] Jo, H-H., Karsai, M., Kertesz, J. and Kaski, K. (2012), 'Circadian patterns and Burstiness in mobile phone Communication', *New Journal of Physics*, vol. 14, 013055
- [117] John, O. P. (1990), 'The "Big Five" factor taxonomy: Dimensions of personality in the natural language and in questionnaires' in L. A. Pervin (Ed.), *Handbook of personality: Theory and research*, pp. 66-100, New York: Guilford Press
- [118] Jones, P. N. (nd), 'Toleration, Recognition, and Identity', *2nd pavia Graduate Conference in Political Philosophy*, vol. 5
- [119] Judge, A. (2014), 'The death of Oyster Card? Contactless payments via smartphone will hit TFL in September', *IT Pro Portal*, 25<sup>th</sup> July 2014, available: <http://www.itproportal.com/2014/07/25/tfl-cpntactless-payment-launch-date-september-London-underground/>  
[accessed: 01 Aug 14]

- [120] Kastrenakes, J. (2013), 'Knock app lets you unlock your Mac by tapping your iPhone', *the Verge website*, 5<sup>th</sup> November 2013, available: <http://www.theverge.com/2013/11/5/5069614/knock-iphone-app-wirelessly-unlocks-your-mac> [accessed: 25 May 14]
- [121] Kaur, G. P., Birla, J. and Ahlawat, J. (2011), 'Generations of Wireless Technology', *IJCSMS International Journal of Computer Science and Management Studies*, vol. 11, no. 2, pp. 176-180
- [122] Kelion, L. (2013), 'Google facial password patent aims to boost Android security', *BBC website*, 6<sup>th</sup> June 2013, available: <http://www.bbc.co.uk/news/technology-22790221> [accessed: 17 Nov 14]
- [123] Kelly, G. (2013), '7 Reasons Why Curved Phones Will Be Awesome', *Trusted Reviews*, 25<sup>th</sup> November 2013, available: <http://www.trustedreviews.com/opinions/7-reasons-why-curved-phones-will-be-awesome#a6SWttmLLlagOQt.99> [accessed: 04 May 14]
- [124] Kempster, J., Sparkes, M., Jones, S., Gunter, J., Williams, R., Moores, I. and Warman, M. (2014), 'Mac at 30 timeline: Apple's every major product', *The Telegraph*, 24 Jan 2014, available: <http://www.telegraph.co.uk/technology/apple/10580156/Mac-at-30-timeline-Apples-every-major-product.html> [accessed: 20 Feb 14]
- [125] Kerr, D. (2014), 'Is Samsung's Galaxy S5 fingerprint scanner secure enough?', *CNET website*, 14<sup>th</sup> May 2014, available: <http://www.cnet.com/uk/news/is-samsungs-galaxy-s5-fingerprint-scanner-secure-enough/> [accessed: 17 Nov 14]
- [126] Kurkovsky, S. and Syta, E. (2010), 'Digital natives and mobile phones: A survey of practices and attitudes about privacy and security', *2010 IEEE International Symposium on Technology and Society (ISTAS)*, Woolongong, Australia, 7-9 June 2010
- [127] Ledermuller, T. and Clarke, N. L. (2011), 'Risk Assessment for Mobile Devices', *Proceedings of Privacy and Security in Digital Business – 8th International Conference, TrustBus 2011, Toulouse, France, 30 August -2 September 2011*, pp.210-221
- [128] Lloyds Bank (nd), 'Lloyds Bank Internet Payments: Please confirm your payment details', *Lloyds Bank website*, available: [http://www.lloydsbank.com/new\\_internet\\_banking\\_demo/text\\_only/tours/tour10/stage6.html](http://www.lloydsbank.com/new_internet_banking_demo/text_only/tours/tour10/stage6.html) [accessed: 23 May 14]
- [129] Lynch, J. (2014), 'Download free iOS 7 Fingerprint Lock Screen app for Android: Get the iPhone 5S fingerprint feature on your Android phone', *IT World website*, 29<sup>th</sup> January 2014, available: <http://www.itworld.com/mobile-wireless/407462/download-free-ios-7-fingerprint-lock-screen-app-android> [accessed: 24 May 14]
- [130] Matyas, V. and Riha, Z. (2002), 'Biometric Authentication - Security and Usability', *Proceedings of IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, Portoroz, Slovenia, 2002*
- [131] MacTutor (1998), '"Charles Babbage": The MacTutor History of Mathematics archive', *University of St Andrews*, available: <http://www-gap.dcs.st-and.ac.uk/~history/Biographies/Babbage.html> [accessed: 05 May 12]

- [132] Meitiv, A. L. (2010), 'Are Android unlock patterns as secure as numeric PINs?', *Mathematics*, 14<sup>th</sup> April 2010, available: [http://playingwithmodels.wordpress.com/2010/04/14/andorid\\_unlock\\_patterns/](http://playingwithmodels.wordpress.com/2010/04/14/andorid_unlock_patterns/) [accessed: 22 May 14]
- [133] Merricks, T. (1998), 'There Are No Criteria of Identity Over Time', *Noûs*, vol. 32, no. 1, pp. 106–124
- [134] Mobbeel website (2014), 'Technology', *Mobbeel website*, available: <http://www.mobbeel.com/technology/> [accessed: 24 Jun 14]
- [135] MobiThinking (2014), 'Global mobile statistics 2014 Part A: Mobile subscribers; handset market share; mobile operators', *MobiThinking website*, available: <http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#smartphonepenetration> [accessed: 02 Jul 14]
- [136] Monroe, F. and Rubin, A. D. (2000), 'Keystroke dynamics as a biometric for authentication', *Future Generation Computer Systems*, vol. 16, pp. 351–359
- [137] Motorola (2014), 'Motorola History Timeline', *Motorola website*, available: [http://www.motorola.com/us/consumers/about-motorola-us/About\\_Motorola-History-Timeline/About\\_Motorola-History-Timeline.html](http://www.motorola.com/us/consumers/about-motorola-us/About_Motorola-History-Timeline/About_Motorola-History-Timeline.html) [accessed: 22 Feb 14]
- [138] Moore, G. E. (1965), 'Cramming More Components onto Integrated Circuits', *Electronics*, vol. 38, no. 8, pp. 114-117
- [139] Moore, G. E. (1975), 'Progress in Digital Integrated Electronics', *Proceedings of International Electron Devices Meeting Technical Digest*, vol. 19, pp.11-13
- [140] MPN (1993), 'Bellsouth, IBM unveil personal communicator phone', *Mobile Phone News*, 8<sup>th</sup> November 1993, available: <http://research.microsoft.com/en-us/um/people/bibuxton/buxtoncollection/a/pdf/press%20release%201993.pdf> [accessed: 01 Mar 14]
- [141] Muncaster J. and Turk M. (2006), 'Continuous multimodal authentication using dynamic Bayesian networks', *Proceedings of 2nd Workshop on Multimodal User Authentication, Toulouse, France, 11-12 May 2006*
- [142] NFC Forum (2014), 'About the Technology: NFC and Contactless Technologies', *NFC Forum website*, available: <http://nfc-forum.org/what-is-nfc/about-the-technology/> [accessed: 13 Jun 14]
- [143] Ngo, G., Simone, J. and St. Fort, H. (2006), 'Developing a Java-Based Keystroke Biometric System for Long-Text Input', *Proceedings of Student/Faculty Research Day, CSIS, Pace University*
- [144] Ngoc, S. N. (2007), 'Identity and Authentication', *Orange R & D Research Object Assessment*
- [145] Nickel, C., Brandt, H. and Busch, C. (2011), 'Classification of Acceleration Data for Biometric Gait Recognition on Mobile Devices', *Proceedings of the Biometrics Special Interest Group (BIOSIG11), Darmstadt, Germany, 8-9 September 2011*, pp. 57-65

- 
- [146] Nokia Developer (2012), 'Symbian OS', *Nokia Developer website*, available: [http://developer.nokia.com/community/wiki/Symbian\\_OS](http://developer.nokia.com/community/wiki/Symbian_OS)  
[accessed: 01 Mar 14]
- [147] O' Boyle, B. (2014), 'How does the Samsung Galaxy S5 fingerprint scanner work?', *Pocket-lint website*, 11<sup>th</sup> April 2014, available: <http://www.pocket-lint.com/news/127605-how-does-the-samsung-galaxy-s5-fingerprint-scanner-work>  
[accessed: 17 Nov 14]
- [148] O'Gorman, L. (2003), 'Comparing Passwords, Tokens, and Biometrics for User Authentication', *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2019-2040
- [149] Ophcrack (2014) 'What is ophcrack?', *Ophcrack website*, available: <http://ophcrack.sourceforge.net/>  
[accessed: 17 Nov 14]
- [150] Orbit (2012), 'Network Access Attacks', *Orbit Computer Solutions*, available: <http://www.orbit-computer-solutions.com/Network-Access-Attacks.php>  
[accessed: 27 Apr 12]
- [151] OWASP (2014), 'Authentication Cheat Sheet', *OWASP website*, 7<sup>th</sup> September 2014, available: [https://www.owasp.org/index.php/Authentication\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Authentication_Cheat_Sheet)  
[accessed: 19 Nov 14]
- [152] Peccei, J. (2006), 'A Beginner's Guide to Phonetics', *jcarreras.homestead.com*, available: <http://jcarreras.homestead.com/rrphonetics1.html>  
[accessed: 20 Nov 14]
- [153] Pennebaker, J. W. and King, L. A. (1999), 'Linguistic Styles: Language Use as an Individual Difference', *Journal of Personality and Social Psychology*, vol. 77, no. 6, pp. 1296-1312
- [154] Planet Biometrics (2014), 'National facial recognition deployment to prevent retail fraud', *Planet Biometrics website*, 25<sup>th</sup> April 2014, available: <http://www.planetbiometrics.com/article-details/i/1962/>  
[accessed: 29 May 14]
- [155] PR Newswire (2014), 'The Global Government Biometric Systems Market 2014-2024', *PR Newswire website*, 29<sup>th</sup> April 2014, available: <http://www.prnewswire.com/news-releases/the-global-government-biometric-systems-market-2014-2024-257218841.html>  
[accessed: 22 Nov 14]
- [156] Prabhakar, S., Pankanti, S. and Jain, A. K. (2003), 'Biometric Recognition: Security and Privacy Concerns', *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33-42
- [157] Prabhu, G. (2014), 'Here's how Apple improved Touch ID fingerprint recognition in iOS 7.1.1', *iphonehacks.com*, 25<sup>th</sup> April 2014, available: <http://www.iphonehacks.com/2014/04/touch-id-fingerprint-recognition-improved-ios-7-1-1.html>  
[accessed: 24 May 14]
- [158] Prynne, J. (2013), 'The iCrime wave: 10,000 phones are stolen in London every month', *The London Evening Standard*, 25<sup>th</sup> July 2013, available: <http://www.standard.co.uk/lifestyle/london-life/the-icrime-wave-10000-phones-are-stolen-in-london-every-month-8731350.html>  
[accessed: 28 Jun 14]
-

- 
- [159] Quine, W. V. (1950), 'Identity, Ostension, and Hypostasis', *The Journal of Philosophy*, vol. 47, no. 22, pp. 621-633
- [160] Ramsland, K. (nd), 'All about Fingerprints and Other Impressions', *CrimeLibrary website*, available: [http://www.crimelibrary.com/criminal\\_mind/forensics/fingerprints/3.html](http://www.crimelibrary.com/criminal_mind/forensics/fingerprints/3.html) [accessed: 20 Nov 14]
- [161] Randewich, N. and Carew, S. (2013), 'Cars, homes smarten up at Vegas tech extravaganza', *Reuters website*, available: <http://uk.reuters.com/article/2013/01/05/us-ces-wireless-idUKBRE90405O20130105> [accessed: 5 Jan 13]
- [162] Rapid NFC (2013), 'The Difference Between NFC and RFID – Explained', *Rapid NFC website*, 29<sup>th</sup> April 2013, available: [http://rapidnfc.com/blog/72/the\\_difference\\_between\\_nfc\\_and\\_rfid\\_explained](http://rapidnfc.com/blog/72/the_difference_between_nfc_and_rfid_explained) [accessed: 14 June 2014]
- [163] Research and Markets (2014), 'Global Mobile Biometrics Market 2014-2018', *Research and Markets website*, available: [http://www.researchandmarkets.com/research/wszs6c/global\\_mobile](http://www.researchandmarkets.com/research/wszs6c/global_mobile) [accessed: 25 Jun 14]
- [164] RFID Journal (2013), 'What Models of Phones Have RFID Functionality?', *RFID Journal website*, 27<sup>th</sup> June 2013, available: <http://www.rfidjournal.com/blogs/experts/entry?10606> [accessed: 13 June 14]
- [165] Richter, F. (2013), 'The Average Smartphone User Has Installed 26 Apps', *Statista website*, 5<sup>th</sup> September 2013, available: <http://www.statista.com/chart/1435/top-10-countries-by-app-usage/> [accessed: 26 May 14]
- [166] Ridden, P. (2011), 'NEC unveils contactless fingerprint scanner', *GizMag website*, 25<sup>th</sup> February 2011, available: <http://www.gizmag.com/nec-develops-contactless-fingerprint-scanner/17989/> [accessed: 20 Nov 14]
- [167] Riverside (2007), 'Iritis: How is it treated?', *Riverside website*, 1<sup>st</sup> March 2007, available: [http://www.riversideonline.com/health\\_reference/Eye/HQ00940.cfm](http://www.riversideonline.com/health_reference/Eye/HQ00940.cfm) [accessed: 21 Nov 14]
- [168] Rohde, L. (2000), 'Ericsson demos first Bluetooth phone: Delayed wireless technology finally emerging', *PC Advisor*, 6<sup>th</sup> June 2000, available: <http://www.pcadvisor.co.uk/news/desktop-pc/100/ericsson-demos-first-bluetooth-phone/> [accessed: 01 Mar 14]
- [169] Rohde, L. (2001), 'UK Government Asks Industry to Fight Mobile Phone Theft', *Infoworld*, vol. 23, no. 5, p. 76
- [170] Ross, A. and Jain, A. K. (2004), 'Multimodal Biometrics: An Overview', *Proceedings of 12<sup>th</sup> European Signal Processing Conference (EUSIPCO)*, pp. 1221-1224
- [171] Sager, I. (2012) 'The First Smartphone', *Bloomberg Businessweek Technology*, 29<sup>th</sup> June 2012, available: <http://www.businessweek.com/articles/2012-06-29/before-iphone-and-android-came-simon-the-first-smartphone> [accessed: 01 Mar 14]
-

- [172] Salford (2010), 'Mobile Phones – the first 25 years', *University of Salford*, available: <http://www.cntr.salford.ac.uk/comms/25yrsofthemobile/survey.php> [accessed: 30 Jan 14]
- [173] Seltzer, L. (2013), 'Cell Phone Inventor Talks of First Cell Call', *Information Week*, 3<sup>rd</sup> April 2013, available: <http://www.informationweek.com/wireless/cell-phone-inventor-talks-of-first-cell-call/d/d-id/1109376?> [accessed: 22 Feb 14]
- [174] Sheth, M., Chand, A., Daswani, K. and Shenvi, S. (2014), 'Iris Image Compression Using Different Algorithms', *International Journal of Software and Web Sciences (IJSWS)*, iss. 8, vol. 1, pp. 31-37
- [175] Shoemaker, S. (2006), 'Identity and Identities', *Daedalus*, Fall 2006, pp. 40-48
- [176] Siciliano, R. (2013), 'More Than 30% of People Don't Password Protect Their Mobile Devices', *McAfee website*, available: <http://blogs.mcafee.com/consumer/unprotected-mobile-devices> [accessed: 25 Jun 14]
- [177] Smith, R. E. (2001), 'Authentication – from Passwords to Public Keys', Addison-Wesley publications
- [178] Sobrado, L. and Birget, J. C. (2002), 'Graphical Passwords' *The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research Volume 4*, available: <http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm> [accessed: 20 Apr 08]
- [179] Statista (2012), 'Smartphones: Statistics and Facts', *Statista website*, available: <http://www.statista.com/topics/840/smartphones/> [accessed: 02 Mar 14]
- [180] Statista (2014), 'Global smartphone sales to end users from 1st quarter 2009 to 4th quarter 2013, by operating system', *Statista website*, available: <http://www.statista.com/statistics/266219/global-smartphone-sales-since-1st-quarter-2009-by-operating-system/> [accessed: 20 Mar 14]
- [181] Styles, K. (2013), '7 in 10 People in the UK Now Own a Smartphone', *Mobile Marketing Magazine*, 24<sup>th</sup> June 2013, available: <http://mobilemarketingmagazine.com/7-10-people-uk-now-own-smartphone/> [accessed: 25 Nov 14]
- [182] Sverdlove, H. and Cilley, J. (2012), 'Pausing Google Play: More Than 100,000 Android Apps May Pose Security Risks', *Bit9 report, October 2012*, available: <https://www.bit9.com/download/reports/Pausing-Google-Play-October2012.pdf> [accessed: 13 May 14]
- [183] Symantec (2006), Symantec Internet Security Threat Report Trends for January 06–June 06, vol. X, p. 22, available: [http://www.symantec.com/specprog/threatreport/ent-whitepaper\\_symantec\\_internet\\_security\\_threat\\_report\\_x\\_09\\_2006.en-us.pdf](http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf) [accessed: 3 Mar 08]
- [184] Tanvi, P., Sonal, G. and Kumar, S.M. (2011) 'Token Based Authentication Using Mobile Phone', International Conference on Communication Systems and Network Technologies (CSNT) 2011, Katra, Jammu, India, 3-5 June 2011, pp. 85-88

- [185] Tanviruzzaman, M., Ahamed, S. I., Hasan, C. S. and O'Brien, C. (2009), 'ePet: when cellular phone learns to recognize its owner', in Ehab Al-Shaer, Mohamed G. Gouda, Jorge Lobo, Sanjai Narain and Felix Wu, ed., 'SafeConfig', ACM, pp. 13-18
- [186] Telegraph (2013), 'The 20 bestselling mobile phones of all time', *The Telegraph*, 3<sup>rd</sup> April 2013, available: <http://www.telegraph.co.uk/technology/picture-galleries/9818080/The-20-best-selling-mobile-phones-of-all-time.html?frame=2459004> [accessed: 30 Jan 14]
- [187] Top, D. (2013), 'Using Voice Biometrics for Strong Authentication and Risk Reduction', *Opus Research website*, available: <http://opusresearch.net/wordpress/2013/07/29/using-voice-biometrics-for-strong-authentication-and-risk-reduction/> [accessed: 24 Jun 14]
- [188] Trader, J. (2012), 'Iris Recognition vs. Retina Scanning – What are the Differences?', *M2SYS Blog On Biometric Technology*, 11<sup>th</sup> June 2012, available: <http://blog.m2sys.com/biometric-hardware/iris-recognition-vs-retina-scanning-what-are-the-differences/> [accessed: 21 Nov 14]
- [189] Van Halteren, H. (2004), 'Linguistic profiling for authorship recognition and verification', *Proceedings of the 42nd Meeting of the Association for Computational Linguistics (ACL'04), Barcelona, Spain, July 2004*, main vol., pp. 199–206
- [190] Varela, F. J. (1997), 'Patterns of Life: Intertwining Identity and Cognition', *Brain and Cognition*, vol. 34, no. 1, pp. 72–87
- [191] Veitch, J. (1901), Translation of 'Rene Descartes: Meditations on First Philosophy', available: <http://www.filepedia.org/files/Descartes'%20Meditations%20on%20First%20Philosophy.pdf> [accessed: 22 Aug 11]
- [192] Velazco, C. (2012), 'Nuance's Dragon ID Lets You Unlock Your Smartphone Or Tablet By Talking To It', *Tech crunch website*, 5<sup>th</sup> June 2012, available: <http://techcrunch.com/2012/06/05/nuances-dragon-id-lets-you-unlock-your-smartphone-by-talking-to-it/> [accessed: 24 May 14]
- [193] Vrankulj, A. (2014), 'Explainer: Finger Vein Recognition', *BiometricUpdate.com website*, 28<sup>th</sup> February 2014, available: <http://www.biometricupdate.com/201402/explainer-finger-vein-recognition> [accessed: 21 Nov 14]
- [194] Vu, K-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B-L., Cook, J. and Schultz, E. E. (2007), 'Improving password security and memorability to protect personal and organizational information', *International Journal of Human-Computer Studies*, vol. 65, no. 8, pp. 744–757
- [195] Ward, M. (2013), 'Smartphone sensors reveal security secrets', *BBC website*, 29<sup>th</sup> January 2013, available: <http://www.bbc.co.uk/news/technology-21203035> [accessed: 16 Nov 14]
- [196] Weinstein, R. (2005), 'RFID: A Technical Overview and Its Application to the Enterprise', *IT Pro, IEEE Computer Society*, May-June 2005, pp. 27-33
- [197] Welch, M. (2014), 'Biometrics on mobile and wearable devices set to become the universal personal authenticator', *Goode Intelligence website*, 17<sup>th</sup> June 2014, available: <http://www.goodeintelligence.com/media-centre/view/biometrics-on-mobile-and->

- wearable-devices-set-to-become-the-universal-personal-authenticator  
[accessed: 25 Jun 14]
- [198] Wood, H. M. (1977), 'The Use of Passwords for Controlling Access to Remote Computer Systems and Services', Proceedings of American Federation of Information Processing Societies: 1977 National Computer Conference (AFIPS 77), Dallas, Texas, USA, 13-16 June 1977, pp. 27-33
- [199] Woollaston, V. (2013a), 'Finally! An UNBREAKABLE phone screen: LG unveils a flexible display ahead of its rumoured mobile launch next month', *Mail Online website*, 8<sup>th</sup> October 2013, available: <http://www.dailymail.co.uk/sciencetech/article-2449413/UNBREAKABLE-flexible-display-phone-screen-unveiled-LG.html#ixzz331Kjj8LF>  
[accessed: 04 Apr 14]
- [200] Woolaston, V. (2013b), 'Unlock your phone with your FACE', *Mail Online website*, 12<sup>th</sup> December 2013, available: <http://www.dailymail.co.uk/sciencetech/article-2522605/Unlock-phone-FACE-Hidden-software-lets-Android-owners-use-head-PIN-people-similar-looks-able-hack-it.html>  
[accessed: 28 Nov 14]
- [201] Woollaston, V. (2014), 'How often do YOU look at your phone? The average user now picks up their device more than 1,500 times a week', *MailOnline website*, 8<sup>th</sup> October 2014, available: <http://www.dailymail.co.uk/sciencetech/article-2783677/How-YOU-look-phone-The-average-user-picks-device-1-500-times-day.html#ixzz3KT9l15zH>  
[accessed: 19 Nov 14]
- [202] Xiao, S., Gong, W. and Towsley, D. (2013), 'Dynamic Secrets in Communication Security', *Springer Science & Business Media*, 13 Aug 2013, p.59
- [203] Xu, F. (2007), 'Sortal concepts, object individuation, and language', *Trends in Cognitive Sciences*, vol. 11, no. 9, pp. 400-406
- [204] Your Dictionary (nd), 'Who Said "United We Stand Divided We Fall"?', *Your Dictionary website*, available: <http://quotes.yourdictionary.com/articles/who-said-united-we-stand-divided-we-fall.html>  
[accessed: 19 Nov 14]

---

# Appendices

---

## Appendix A. PDA Software

---

```
Imports System
Imports System.IO

Public Class Form1

    ' Define global variables -----
    -----
    Dim minutes As Decimal = 1 ' Alter this to adjust the time between polls of the
environment
    Dim minutesFromStart As Decimal = (0 - minutes) ' Keeps an accumulative time since
start of reading cycle
    Dim lastDay, outputFilePath, outputFileRoot, userId As String
    Dim outputFile, summaryFile As System.IO.TextWriter
    Dim nodeEnabled As Boolean = True
    Dim fileNumber As Integer = 0
    ' -----
    -----

    ' Settings for spPort1 -----
    ' spPort.BaudRate = 38400
    ' spPort.Parity = Parity.None
    ' spPort.PortName = "COM4"
    ' spPort.ReadTimeout = 1000
    ' spPort.StopBits = StopBits.One
    ' -----

    Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles MyBase.Load
        btnStop.Visible = False
        btnListen.Visible = True

        ' Initialise variables ---
        outputFileRoot = "Tagdata"
        lastDay = ""
        ' -----

        ' Immediately begin -----
        startListening()
        ' -----

    End Sub

    Private Sub openFile()
        Dim format As String = "yyMMdd"

        If Not lastday = Now.ToString(format) Then
            If Not lastday = "" Then
                ' lastDay = "" signifies first time through, so close file because it
must be open
                outputFile.Close()
                outputFile.Dispose()

                summaryFile.Close()
                summaryFile.Dispose()
            End If

            lastDay = Now.ToString(format)

            ' Open new file for new day
            outputFilePath = outputFileRoot + lastDay + "_" + userId
            outputFile = New StreamWriter(outputFilePath + ".txt", True)

            summaryFile = New StreamWriter("Summary" + lastDay + "_" + userId + ".txt",
True)

        End If
    End Sub

    Private Sub nodeSwitch(ByVal state As String)
        If state = "on" Then
            If Not nodeEnabled Then
                spPort1.WriteLine("TE1" + vbCr) ' Enables the node
                nodeEnabled = True
            End If
        Else

```

```

        spPort1.WriteLine("TE0" + vbCr) ' Disables the node
        nodeEnabled = False
    End If
End Sub

Private Sub readComPort()
    Dim txt As String = "Nothing read"
    Dim bufferTxt As String = ""
    Dim bufferArray As String()
    Dim bufferPos, signal, position As Integer
    Dim foundTags, tagSignal, tagCount As New ArrayList()
    Dim format As String = "dd/MM/yy,HH:mm:ss"

    lbText.Items.Add(" ")

    Try
        bufferTxt = spPort1.ReadExisting ' Read input buffer from node

        If bufferTxt.Length > 0 Then

            bufferArray = Split(bufferTxt, vbCrLf)

            For bufferPos = 0 To bufferArray.Count - 1

                txt = bufferArray(bufferPos).ToString

                If txt.Length = 32 Then ' Tag replies are 32 bytes long

                    signal = Convert.ToInt16(Mid(txt, 7, 2), 16) ' Extract the
signal strength as HEX
and converts to decimal
                    signal = Int((signal / 255) * 100) ' Convert the signal into a
percentage

                    txt = Mid(txt, 21, 12) ' Extract the tag id

                    position = foundTags.IndexOf(txt)
                    If position < 0 Then ' First time the tag has been seen

                        foundTags.Add(txt) ' Keeps track of whats already been found
this cycle

                        tagCount.Add(1)
                        tagSignal.Add(signal)

                    Else ' Existing tag

                        tagCount(position) += 1
                        tagSignal(position) += signal

                    End If

                End If

            Next bufferPos

            ' Loop through and write details to list box and file
            For arrayPos = 0 To foundTags.Count - 1
                txt = foundTags(arrayPos).ToString

                lbText.Items.Add(txt)
                lbText.Refresh()

                txt += "," + userId + "," + Now.ToString(format) + "," +
minutesFromStart.ToString + "," + _
(Int(tagSignal(arrayPos) / tagCount(arrayPos))).ToString
                outputFile.WriteLine(txt)

            Next arrayPos

            outputFile.Flush()

        End If

        ' -----

        lbText.Items.Add(" ")
        txt = foundTags.Count.ToString
        lbText.Items.Add(txt + " Found")
        txt += "," + userId + "," + Now.ToString(format) + "," +
minutesFromStart.ToString
        summaryFile.WriteLine(txt)
    
```

```

        summaryFile.Flush()

    Catch ex As Exception
        ' MessageBox.Show("Read timed out!", "Fatal error")

        lbText.Items.Add("*** FATAL ERROR ***")
        lbText.Items.Add("Close and restart application")

    End Try

End Sub

Private Sub btnStop_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnStop.Click
    btnStop.Visible = False
    btnListen.Visible = True

    tmrNodeTimer.Enabled = False
    tmrListenTimer.Enabled = False

    If spPort1.IsOpen Then
        ' nodeSwitch("on") ' Leave the node in an "on" state
        spPort1.DiscardInBuffer()
        spPort1.Close()
        spPort1.Dispose()
    End If

    outputFile.Close()
    summaryFile.Close()

End Sub

Private Sub tmrNodeTimer_Tick(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles tmrNodeTimer.Tick
    tmrNodeTimer.Interval = minutes * 60 * 1000 ' Timer uses milliseconds so convert
to true minutes
    minutesFromStart += minutes

    lbText.Items.Clear()
    lbText.Items.Add("About to read..." + Now.TimeOfDay.ToString)
    lbText.Refresh()

    spPort1.DiscardInBuffer() ' Clear unprocessed data
    nodeSwitch("on") ' Activate node
    tmrListenTimer.Enabled = True ' Enable listening timer so node active for 10
secs
    openFile() ' Checks on date and opens output text files

    ' If it's the first time through write block of asterisks to files
    If minutesFromStart = minutes Then
        outputFile.WriteLine("*****")
        outputFile.Flush()
        summaryFile.WriteLine("*****")
        summaryFile.Flush()
    End If
    ' -----

End Sub

Private Sub tmrListenTimer_Tick(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles tmrListenTimer.Tick
    tmrListenTimer.Enabled = False 'Ends 10sec listening
    ' *****
    'tmrNodeTimer.Enabled = False
    ' *****
    nodeSwitch("off") ' Turn off node

    readComPort() 'Process received data

    spPort1.DiscardInBuffer() ' Clear unprocessed data
End Sub

Private Sub btnListen_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnListen.Click
    startListening()
End Sub

Private Sub startListening()
    Dim delay, seconds, separation As Integer
    btnListen.Visible = False

```

```

btnStop.Visible = True
lbText.Text = vbNullString
Me.Refresh()

getUserId()

Try
    If spPort1.IsOpen = False Then
        spPort1.Open()
        spPort1.DiscardInBuffer()
    Else
        MessageBox.Show("Want to open port but it is still open")
    End If

    ' Work out the first delay to offset al.l 5 PDAs by an even no. seconds ----
    -----
    delay = Convert.ToInt32(userId)
    separation = minutes * 60
    delay = (delay Mod 5) * (separation / 5)
    seconds = ((Now.Minute * 60) + Now.Second) Mod separation
    delay = delay - seconds ' Work out no. seconds to go
    If delay < 0 Then ' If delay -ve then add minutes
        delay = delay + separation
    End If

    nodeSwitch("off") ' Switch off node so it doesn't block others
    lbText.Items.Add("System commencing in " + delay.ToString + " seconds")

    delay = (delay * 1000) + 100 ' Convert to miliseconds and add 100 for peace
of mind
    ' -----
    -----

    tmrNodeTimer.Interval = delay ' Forces first read to happen at offset amount
    tmrNodeTimer.Enabled = True

    lbText.Refresh()

    Catch ex As Exception
        MessageBox.Show("Port '" + spPort1.PortName + "' could not be opened! You
will have to reset the PDA and restart the program again.", "Fatal error")
        spPort1.Close()
        spPort1.Dispose()

        If Not lastDay = "" Then ' lastday is set once a file has been opened
            outputFile.Close()
            summaryFile.Close()
        End If

        btnListen.Visible = True
        btnStop.Visible = False

    End Try

End Sub

Public Sub getUserId()
    Dim userIdFile As String = "UserId.txt"

    If 1 = 0 Then
        If File.Exists(userIdFile) Then
            System.IO.File.Delete(userIdFile)
        End If

        Dim userFile As System.IO.TextWriter = New StreamWriter(userIdFile, True)

        userId = 13 ' Change this to the required number

        userFile.WriteLine(userId)

        userFile.Close()
        userFile.Dispose()

        Application.Exit()
    End If

    If File.Exists(userIdFile) Then
        Dim userFile As System.IO.TextReader = New StreamReader(userIdFile, True)

```

```
        userId = userFile.ReadLine

        userFile.Close()
        userFile.Dispose()
    End If

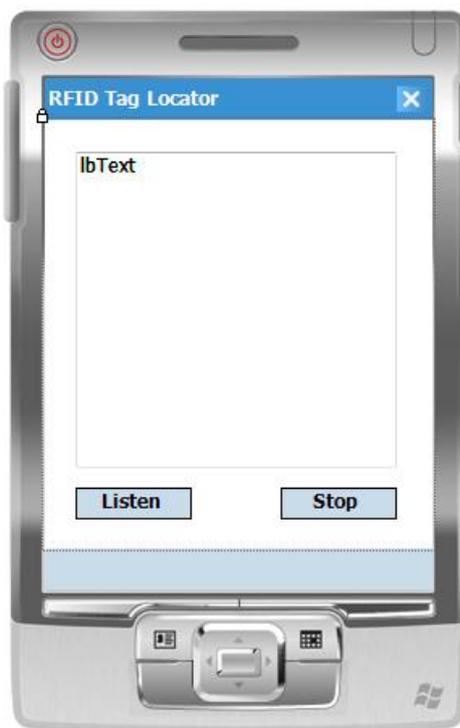
    If userId = "" Then
        Dim userFile As System.IO.TextWriter = New StreamWriter(userIdFile, True)

        userId = Now.ToString("HHmmss")

        userFile.WriteLine(userId)

        userFile.Close()
        userFile.Dispose()
    End If
End Sub

End Class
```



**Figure 0-1. The visual basic form associated with the PDA software**

## Appendix B. MATLAB Simulation Script

---

```
% This script plots the confidence factor based on the experiment data.
% This is done for all selected days and users.
% Observations are grouped into 10 minute clusters and the days start at 8am.
% Infrastructure is also included as a contributing device.
% Plots start at 8am and usage is required every paameterised minutes

% Allows for shared devices by recognising user 99

clear;

outputPath='Z:\Analysis\Simulation\Simulation';
userGroup=1;

if userGroup==1;
    fileName='Tag xref 1-5'; userStart=1; userEnd=5;
end;
if userGroup==2;
    fileName='Tag xref 6-10'; userStart=6; userEnd=10;
end;
if userGroup==3;
    fileName='Tag xref 11-15'; userStart=11; userEnd=15;
end;
if userGroup==4;
    fileName='Tag xref 16-20'; userStart=16; userEnd=20;
end;

[xref,xrTxt,xraw] = xlsread(strcat('Data\',fileName, '.xlsx'));

periodLength=10; % Number of minutes for each period
periodCutOff=49; % Start of day e.g. 37 for 10 min period = 6am, 49 8am
periodMax=144; % Total number of periods
periodUsage=3; % Number of periods between useage

allDaysDone(20)=0;
userCount=0;

%userStart=13; %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Maintain %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%userEnd =13; %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Maintain %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

tokenContribution=1.5; tokenContributionText='1pt5'; % was 1.5
tokenContributionMax=30; % was 30
intelligentDeviceContribution=20; % was 20
intelDegrade=1; % Boolean
intelDegradeText='_deg';

auraMinimum=0; % Stops confidence dropping below this value

auraData(5,20,110)=0;
auraLogons(5,20,40)=0;
auraLocations(5,20,50,2)=0;
auraDeviceUsage(5,20,40)=0;

for user=userStart:userEnd;

    userCount=userCount+1;

    clear d* f* g* l* m* txt raw conf*;

    fileName=strcat('MatlabTagData',num2str(user))
    [data,txt,raw] = xlsread(strcat('Data\',fileName, '.xlsx'));

    dataSize=size(data);
    maxReads=dataSize(1);
    devicePresence{periodMax,77,21}='0'; % 10 mins, tag, day

    % Set logon parameters -----
    logonTrigger=20; % was 20
    periodDegradation=2; % Every period this figure is subtracted from conf
    simDeviceAuthenticationLevel=3; % Set as reverse - 5=secure, 1=weak
    logonPercentage=110-(simDeviceAuthenticationLevel*10);
    % -----

    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Change these to control how many days are done and which
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% are included
    weekday=[1 2 3 4 5 8 9 10 11 12 15 16 17 18 19];
```

```

weekend=[6 7 13 14 20 21];

%incDays=[1 2 3];
%incDays=[1 2 3 4 5 6 7];
%incDays=[8 9 10 11 12 13 14];
%incDays=[15 16 17 18 19];
incDays=[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19];
%incDays=[5 6 7];
%incDays=[1 2 3 4 5 8 9 10 11 12 15 16 17 18 19]; % weekdays
%incDays=[6 7 13 14]; % weekends
%incDays=[9];
%weekday=[1 2 3 4 5];
%weekend=[6 7];
%weekday=[3 6];
%weekend=[4, 7];

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

dow=0; % Day of week - M=1,Tu=2 etc.
lastPeriod=-1;
confRow=1;
PeriodCount=0;
lastDow=0;
lastDay=0;
noDays=0;
daysDone=0;

% First build the array to show which devices are visible at each time
% slot
for row=1:maxReads;
    dataRow=row;

    % Get variable values
    dataTemp=data(dataRow,1:7);
    xXrefRow=dataTemp(1,1);
    xrefTemp=xref(xXrefRow,1:9);
    txtTemp=xrTxt(xXrefRow+1,1:10);

    dow=dataTemp(1,5);
    includeDay=0;
    if any(abs(incDays-dow)<1e-10); % Checks if dow in include array
        includeDay=1;
    end;

    if includeDay==1;

        if dow~=lastDay;
            lastDay=dow;
            noDays=noDays+1;
            daysDone(noDays)=dow;

            dayPos=mod(dow, 7);
            if dayPos==0;
                dayPos=7;
            end;

            allDaysDone(dow)=1;

        end;

        tag=txtTemp(1,1);
        userId=dataTemp(1,1);
        % count=dataTemp(1,5);
        period=floor(dataTemp(1,4)*1440/periodLength)+1; % Time, 1440=(60*24)
        strength=dataTemp(1,7);
        location=txtTemp(1,4);
        item=txtTemp(1,5);
        label=xXrefRow;
        type=txtTemp(1,6);
        intel=txtTemp(1,7);
        rank=xrefTemp(1,7);
        maxCont=xrefTemp(1,8);
        minStrength=xrefTemp(1,9);
        tagUserId=xrefTemp(1,2);

        % Allow for shared devices -----
        if tagUserId==99;
            tagUserId=user;
        end;
        % -----
    end;
end;

```

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
includeObs=1;

% Work out if item is infrastructure -----
infrastructure=0;
if strcmp(type,'I');
    infrastructure=1;
else
    if tagUserId~=user; % Exclude other's devices that aren't Inf.
        includeObs=0;
    end;
end;
% -----

% Work out if observation is to be included -----
if period<periodCutOff; % Cut off day at 6am = 36 10 minute periods
    includeObs=0;
end;
% -----

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

if includeObs==1;
    devicePresence{period, xXrefRow, dow}=location;
end;

end; % end of include

end; % end of row loop

if noDays>0;
    dataSize=size(daysDone);
    maxDays=dataSize(2);

    for dayNo=1:maxDays;
        dow=daysDone(dayNo);

        % Null the working variables
        clear auraDevice deviceDetail;
        deviceDetail(77,8)=0;
        auraDevice(1,8)=0;
        periodUsageCount=3;

        for period=periodCutOff:periodMax;

            % Set up the current devices for this period -----
            location='A';
            locationMultiplier=10; % was 10 high=30
            locationFlag=3;
            clear currentDevices;
            lastDevice=0;
            for device=1:77;
                loc=devicePresence{period, device, dow};
                if isempty(loc);
                    % Wipe out device detail for those not present
                    deviceDetail(device,1)=0;
                else
                    if strcmp(loc,'H') || (location=='H');
                        location='H';
                        locationMultiplier=2.5;
                        locationFlag=1;
                    else
                        if strcmp(loc,'W') && (location~='H');
                            location='W';
                            locationMultiplier=5; % was 5 high=10
                            locationFlag=2;
                        end;
                    end;
                end;

                lastDevice=lastDevice+1;
                currentDevices(lastDevice)=device;
            end;
        end;

        % Maintain location array -----
        if auraLocations(userCount,dow,1,1)==0;
            auraLocations(userCount,dow,1,1)=2;
            auraLocations(userCount,dow,2,1)=period-periodCutOff+1;

```

```

        auraLocations (userCount, dow, 2, 2)=locationFlag;
    else
        if
auraLocations (userCount, dow, auraLocations (userCount, dow, 1, 1), 2)~=locationFlag;           %
Location changed

auraLocations (userCount, dow, 1, 1)=auraLocations (userCount, dow, 1, 1)+1;

auraLocations (userCount, dow, auraLocations (userCount, dow, 1, 1), 1)=period-periodCutOff+1;

auraLocations (userCount, dow, auraLocations (userCount, dow, 1, 1), 2)=locationFlag;
        end;
    end;
    % -----

    % Set current devices for this period
    for deviceNum=1:lastDevice;
        device=currentDevices (deviceNum);

        if deviceDetail (device, 1)==0; % New device or just back

            xrefTemp=xref (device, 1:9);
            userId=xrefTemp (1, 2);
            deviceDetail (device, 1)=userId;

            if deviceDetail (device, 4)==0; % New
                txtTemp=xrTxt (device+1, 1:10);

                type=txtTemp (1, 6);
                intel=txtTemp (1, 7);
                rank=xrefTemp (1, 7);
                maxCont=xrefTemp (1, 8);

                if strcmp (type, 'D');
                    deviceDetail (device, 2)=1; % 1 indicates device, 0
everything else
                else
                    deviceDetail (device, 2)=0;
                end;
                if strcmp (intel, 'I');
                    deviceDetail (device, 3)=1; % 1 indicates intelligent, 0
dumb
                else
                    deviceDetail (device, 3)=0;
                end;
                deviceDetail (device, 4)=rank;
                deviceDetail (device, 5)=maxCont;
            end;

            deviceDetail (device, 6)=0; % Confidence
            deviceDetail (device, 7)=0; % Time of last authentication
            deviceDetail (device, 8)=0; % Contribution from other devices

        end;
    end;

    % Work out current device confidences
    for deviceNum=1:lastDevice;
        device=currentDevices (deviceNum);
        auraCont=0;
        tokenCont=0;

        for deviceTempNum=1:lastDevice; % Loop through and work out aura
cont for this device
            if deviceTempNum~=deviceNum;
                deviceTemp=currentDevices (deviceTempNum);

                token=0;

                if deviceDetail (deviceTemp, 1)==deviceDetail (device, 1); %
Same users
                    if deviceDetail (deviceTemp, 3)==1; % Intelligent

                        level=simDeviceAuthenticationLevel; % Authentication
security
                    if deviceDetail (deviceTemp, 7)==0; % Not
authenticated
                        % If not authenticated then cannot
                        % contribute any confidence but can

```

```

        % act as token I guess!!
        token=1;
    else % Authenticated
        if period==deviceDetail(deviceTemp,6);
            auraCont=auraCont+((6-
level)*intelligentDeviceContribution);
        else
            if intelDegrade==1;
                auraCont=auraCont+((6-
level)*intelligentDeviceContribution) / (period-deviceDetail(deviceTemp,6));
            else
                auraCont=auraCont+((6-
level)*intelligentDeviceContribution);
            end;
        end;
    end;
    else % Dumb
        token=1;
    end;
    else % Different users
        token=1;
    end;

    if token==1;
        % tokenCont / rank

tokenCont=tokenCont+(tokenContribution*deviceDetail(deviceTemp,4));
        end;

        end; % end of deviceTempNum loop

    if tokenCont>tokenContributionMax;
        tokenCont=tokenContributionMax;
    end;

    % Used to remove Aura influence -----
    % auraCont=0;tokenCont=0; % was commented out
    % -----

    deviceDetail(device,8)=auraCont+tokenCont;

    % Check if it can and needs to authenticate and then do
    % so - check if intelligent & low confidence+aura cont
    if (deviceDetail(device,3)==1);
        if
((deviceDetail(device,6)+deviceDetail(device,8))<logonTrigger); % was this line
%
((deviceDetail(device,6)+deviceDetail(device,8))<(logonTrigger*locationFlag));
        deviceDetail(device,6)=logonPercentage;
        deviceDetail(device,7)=period;
    else
        deviceDetail(device,6)=deviceDetail(device,6)-
(periodDegradation*locationMultiplier);
    end;
end;

end; % end of deviceNum loop
% -----

% Work out confidence of aura device -----
auraCont=0;
tokenCont=0;
for deviceNum=1:lastDevice;
    device=currentDevices(deviceNum);

    token=0;

    if deviceDetail(device,1)==user; % Same users
        if deviceDetail(device,3)==1; % Intelligent

            level=simDeviceAuthenticationLevel; % Authentication
security

            if deviceDetail(device,7)==0; % Not authenticated
                % If not authenticated the cannot
                % contribute any confidence but can
                % act as token I guess!!

```

```

        token=1;
        else % Authenticated
            if period==deviceDetail(device,6);
                auraCont=auraCont+((6-
level)*intelligentDeviceContribution);
            else
                if intelDegrade==1;
                    auraCont=auraCont+(((6-
level)*intelligentDeviceContribution) / (period-deviceDetail(device,7)));
                else
                    auraCont=auraCont+((6-
level)*intelligentDeviceContribution);
                end;
            end;
        end;
        else % Dumb
            token=1;
        end;
    else % Different users
        token=1;
    end;

    if token==1;
        % tokenCont / rank
        tokenCont=tokenCont+(tokenContribution*deviceDetail(device,4));
    end;

end; % end of deviceNum loop

if tokenCont>tokenContributionMax;
    tokenCont=tokenContributionMax;
end;

% Used to remove Aura influence -----
%   auraCont=0;tokenCont=0; % was commented out
% -----

auraDevice(1,8)=auraCont+tokenCont;

auraDevice(1,6)=auraDevice(1,6)-(periodDegradation*locationMultiplier);

% Check if needs to authenticate and then do so
% Check if low confidence+aura cont
if
((auraDevice(1,6)+auraDevice(1,8))<logonTrigger)&&(periodUsageCount==periodUsage); % was
this line
%
((auraDevice(1,6)+auraDevice(1,8))<(logonTrigger*locationFlag))&&(periodUsageCount==peri
odUsage);
    auraLogons(userCount,dow,1)=auraLogons(userCount,dow,1)+1; % Tracks
the logon count
    logonPos=(auraLogons(userCount,dow,1)*2);
    auraLogons(userCount,dow,logonPos)=period-periodCutOff+1;
    if (auraDevice(1,6)+auraDevice(1,8)) < 0;
        auraLogons(userCount,dow,logonPos+1)=0;
    else
auraLogons(userCount,dow,logonPos+1)=(auraDevice(1,6)+auraDevice(1,8));
    end;

    auraDevice(1,6)=logonPercentage;
    auraDevice(1,7)=period;
%else
%auraDevice(1,6)=auraDevice(1,6)-
(periodDegradation*locationMultiplier);
end;

conf=auraDevice(1,6)+auraDevice(1,8);
if conf>100;
    conf=100;
elseif conf<0;
    conf=0;
end;

auraData(userCount,dow,period-periodCutOff+1) = conf;

% -----

if periodUsageCount==3;
    periodUsageCount=0;

```

```

auraDeviceUsage(userCount, dow, 1) = auraDeviceUsage(userCount, dow,
1)+1;
auraDeviceUsage(userCount, dow, auraDeviceUsage(userCount, dow,
1)+1) = conf;
end;
periodUsageCount=periodUsageCount+1;

end; % End of period loop

%%% Sort out plot details %%%
clear x y xl yl ylz xdu ydu
numPeriods=0;
numLogons=1;
numExtras=0;
for period=periodCutOff:periodMax;
numPeriods=numPeriods+1;

% Add in extra logon points where necessary -----
if (numLogons<=auraLogons(userCount, dow, 1));
if (auraLogons(userCount, dow, numLogons*2)==period-periodCutOff+1);
if period>periodCutOff; % Stops logon on axis
x(numPeriods+numExtras)=auraLogons(userCount, dow,
((numLogons*2)+1));
y(numPeriods+numExtras)=period-periodCutOff+1;
numExtras=numExtras+1;
end;
numLogons=numLogons+1;
end;
end;
% -----

x(numPeriods+numExtras)=auraData(userCount, dow, period-periodCutOff+1);
y(numPeriods+numExtras)=period-periodCutOff+1;
end;

% Location plots -----
if auraLocations(userCount,dow, 1, 1) > 0;
for i=2:auraLocations(userCount,dow, 1, 1);
if auraLocations(userCount,dow, i, 2)==1; % Home
colour=[0 1 0]; % Green
logonTriggerTemp=20;
else
if auraLocations(userCount,dow, i, 2)==2; % Work
colour=[1 0.5 0]; % Orange
logonTriggerTemp=40;
else % Away
colour=[1 0 0]; % Red
logonTriggerTemp=60;
end;
end;

xl=auraLocations(userCount,dow, i, 1);
if auraLocations(userCount,dow, i+1, 1)==0; % No upper
x2=periodMax-periodCutOff+1;
else
x2=auraLocations(userCount,dow, i+1, 1);
end;

clear xdummy ydummy;
pos=0;
for j=x1:x2;
pos=pos+1;
xdummy(pos)=j;
ydummy(pos)=logonTrigger; % was logonTrigger;
end;
plot(xdummy,ydummy,'Color',colour,'Linewidth',10);
hold on;
end;
else
clear xdummy;
ydummy(numPeriods)=logonTrigger;
plot(y,ydummy,'Color','red','Linewidth',5);
hold on;
end;
% -----

% Percentage plot -----
plot(y,x,'Color','Blue','Linewidth',2);
hold on;

```

```

% -----
% Logon markers -----
if auraLogons(userCount, dow, 1)>0;
    for pos=1:auraLogons(userCount, dow, 1);
        xl(pos)=auraLogons(userCount, dow, pos*2);
        yl(pos)=logonPercentage;
        ylz(pos)=0;
    end;

    % Plot black squares at authentication points
    scatter(xl,yl, 's','MarkerEdgeColor','k');
    scatter(xl,ylz,'s','MarkerEdgeColor','k');
end;
% -----

% Device usage markers -----
if auraDeviceUsage(userCount, dow, 1)>0;
    for pos=1:auraDeviceUsage(userCount, dow, 1);
        xdu(pos)=(pos-1)*periodUsage+1;
        ydu(pos)=auraDeviceUsage(userCount, dow, pos+1);
    end;

    % Plot black plus at device usage points
    scatter(xdu,ydu, '+','MarkerEdgeColor','k', 'LineWidth', 2);
end;
% -----

axis([1 numPeriods+1 0 100]);
xlabel('Time', 'fontSize', 12);
set(gca, 'TickDir', 'out', 'YTick', [0:10:100], 'XTick',
[1:12:numPeriods+1], 'XTickLabel', {'8:00' '10:00' '12:00' '14:00' '16:00' '18:00'
'20:00' '22:00' '24:00'});
set(gca, 'box', 'off');
% Legend
%legend(txt{1:nextOwnTag-2,1}, 'Location', 'EastOutside');
%legend_handle = findobj(gcf,'Tag','legend');
%legend_title = get(legend_handle,'Title');
%set(legend_title,'fontSize',12,'String','Device');

%%% Sort out frame size and send to file %%%
scrsz = get(0,'ScreenSize');
set(gcf,'Position',[scrsz(1) scrsz(2)+scrsz(4)/20 scrsz(3) scrsz(4)*17/20]);
% Background
% set(gca, 'Color', [0 0 0]); % Background colour of plot
fig_handle = figure(1); % Returns the handle to the figure object
set(fig_handle, 'color', 'white'); % Sets the colour to white
% Write
frame=getframe(gcf);
%imwrite(frame.cdata,
strcat('Graphs\', 'AuraSim u',int2str(user),'_d',int2str(dow),'_lo',int2str(logonPercenta
ge),'_th',int2str(logonTrigger),'_uf',int2str(periodUsage*periodLength),'_dc',int2str(in
telligentDeviceContribution),'_tm',int2str(tokenContributionMax),'_tc',tokenContribution
Text,'_al',int2str((6-simDeviceAuthenticationLevel)),intelDegradeText,'_8am.bmp')); %
Alternate to saveas(fig_handle, fileName, 'tif');
    imwrite(frame.cdata,
strcat(outputPath, '_user=',int2str(user),'_day=',int2str(dow),'.bmp')); % Alternate to
saveas(fig_handle, fileName, 'tif');
    close(fig_handle);

end; % end of dayNo loop

end; % end of noDays if

end; % end of user loop

% Section used for getting stats out of the system -----
if l==0; % Logons per day
    userCount=0;
    for user=userStart:userEnd;
        userCount=userCount+1;
        userCount
        for day=1:20;
            z=auraLogons(userCount,day,1);
            if z>0;
                z
            end;
        end;
    end;
end;
end;

```

```
end;

if l==0; % Total logons
    userCount=0;
    for user=userStart:userEnd;
        userCount=userCount+1;
        userCount
        z=sum(auraLogons (userCount, :, 1));
        if z>0;
            z
        end;
    end;
end;

if l==0; % Latest first logon
    userCount=0;
    for user=userStart:userEnd;
        userCount=userCount+1;
        latestDay=0; latestLogon=0;
        for day=1:20;
            z=auraLogons (userCount, day, 1);
            if z>0;
                z=auraLogons (userCount, day, 2); %%%%%%%%%%% first logon
                if z>latestLogon;
                    latestLogon=z;
                    latestDay=day;
                end;
            end;
        end;
        user
        latestDay
        latestLogon
    end;
end;
% -----
```

## Appendix C. Publications

---

In the following pages the publications listed below are presented.

Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2010), 'A distributed and cooperative user authentication framework', 6th International Conference on Information Assurance and Security (IAS 2010), Atlanta, USA, 23-25 August 2010, pp. 304-310.

Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2011), 'Authentication Aura - A distributed approach to user authentication', Journal of Information and Assurance, vol. 6, iss.2, pp. 149-156.

Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2011), 'A preliminary investigation of distributed and cooperative user authentication', Proceedings of the 9th Australian Information Security Management Conference (secAU 2011), Perth, Australia, 5-7 December 2011.

(Awarded the Hutchinson prize for best paper in conference)

Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2013), 'Co-operative user identity verification using an Authentication Aura', Computers and Security, vol. 39, part B, pp. 486-502.

# A distributed and cooperative user authentication framework

C. G. Hocking<sup>1</sup>, S. M. Furnell<sup>1,2</sup>, N. L. Clarke<sup>1</sup> and P. L. Reynolds<sup>1</sup>

<sup>1</sup>Centre for Security, Communications and Network  
Research  
University of Plymouth  
Plymouth, United Kingdom  
info@csan.org

<sup>2</sup>School of Computer and Information Science  
Edith Cowan University  
Perth, Western Australia

**Abstract**—As the requirement for companies and individuals to protect information and personal details comes more into focus, the implementation of security that goes beyond the ubiquitous password or Personal Identification Number (PIN) is paramount. With the ever growing number of us utilizing more than one device simultaneously, the problem and need is compounded. This paper proposes a novel approach to security that leverages the collective confidence of user identity held by the multiplicity of devices present at any given time. User identity confidence is reinforced by sharing established credentials between devices, enabling them to make informed judgments on their own security position. An Adaptive Security Control Engine (ASCE) is outlined, illustrating how an environment sensitive and adaptive security envelope can be established and maintained around an individual.

**Keywords**- authentication, identification, mobile, security, biometric, identity

## I. INTRODUCTION

The aspiration of people to be mobile and yet remain in communication with colleagues, family and friends has driven the use of devices that support and complement this lifestyle. Estimates suggest that worldwide Wi-Fi hotspot usage during 2009 increased to 1.2 billion connections, an increase of 47% from 2008, with this being driven by a 50% increase in the sale of Wi-Fi capable handsets between 2007 and 2008 [1]. Technological evolution has enabled powerful and sophisticated systems to be accommodated into these handheld electronic gadgets furnishing them with extensive storage and processing capabilities, making them an increasing target for thieves. In 2007-8 over 700,000 handsets were stolen in the UK, with 50% of all robberies targeting a mobile phone in the items taken and in 33% of those offences it was the only stolen possession [2]. Between May and June 2009 alone, the UK saw an 11% increase in the reporting of missing/stolen mobile phones, with 84% of theft victims failing to retrieve their lost handsets [3].

However, theft is not the sole reason for concern; a New York survey revealed that during a six month period in 2008, 31,544 phones and 2,752 other types of handheld device (laptops, PDAs, memory sticks etc.) were simply left in the city's Yellow Cabs, an average of more than two per cab [4]. In this climate, the requirement to protect and secure the potentially large volumes of sensitive and personal

information contained within these desirable pieces of equipment is imperative and even acknowledged and supported by Government [5],[6].

The problem is magnified because users are finding themselves in possession of an ever growing number of digital devices, each one having its own associated security requirements. With several being carried concurrently, at the moment of initial use it is likely that similar procedures of authentication are undertaken repeatedly across the disparate entities to ensure full activation. This repetitive and time-consuming operation raises the question of whether there is a better way and does the collective identity knowledge possessed by the multiplicity of secured devices utilized by an individual at any given time present an opportunity to improve security. As each device is activated a set of authentication credentials are determined and access is either granted or denied. By enabling the individual and distinct devices to communicate their own authentication status and to share established user identity confidence it may be possible to synthesize an enhanced form of security.

This paper explores this concept and proposes an approach through which authentication credentials can be distributed amongst devices and how this information can be used to create a novel method of security and user control. It addresses the requirements to produce a flexible, adaptive and non-intrusive security mechanism that will meet future demands and provide a foundation for further development. Firstly, the background explores the current methods of securing mobile devices and the associated weaknesses. Once these foundations have been laid the paper continues to outline the new proposals and considers how they will improve upon the situation at present.

## II. BACKGROUND

Security is founded on three key principles – something an individual knows, they possess or they are [7]. Knowledge and possession based security both rely upon the inherently weak link in the chain – the user. The first utilizes a piece of significant or memorable information which is often forgotten or written down [8]; the second, the presentation of a physical key or token at the required moment. Forgetting, mislaying or losing the crucial item or information will bar further access attempts.

The ubiquitous point of entry user identity code/password has been rendered susceptible to abuse through the inability or unwillingness of individuals to protect and administer this sensitive information correctly [9]. To maintain security it is supposedly known or more precisely memorized exclusively by the creator [10] but is too often shared or inadvertently communicated [11]. Although different; identification and authentication both rely upon the recognition of the identity of a user interacting with a device at any given moment. Hand held mobile devices typically assume the identity of the user and utilize personal identification numbers (PINs) to authenticate<sup>1</sup> this at point-of-entry. The authentication is Boolean; the subject is either deemed to be whom they purport to be or they are not, without any middle ground. Frequently passing the one-off process will permit unregulated access to all facilities and utilities installed on the device [12]. Therefore once access has been gained the ability to incur large telephone bills or excessive high-cost data downloads is readily available to impostors who compromise the PIN.

In the search for evermore appropriate and robust authentication, attention has turned to biometrics (something the user is) to establish methods that cannot easily be compromised, are non-intrusive and equally eliminate the potential threat posed by social engineering [13]. A finer granularity of identification can be achieved; ultimately the device will either issue or refuse access to the user, however the starting confidence can precisely reflect how well the supplied identity matches the known template sample. Having this ability will allow a device to tailor its reaction to strong and weak authentication attempts accordingly. Further, without fundamentally changing the habits to which users are accustomed improvements can be implemented. As a supplementary development, layered authentication techniques have been explored and employed to compound protection and expand the sophistication required to circumvent defense mechanisms including; password and facial recognition [14], fingerprint scan and tokenized random number [15], teeth imaging and voice pattern verification [16]. This can then be reinforced by elements such as location information which indicates whether or not a user is operating in a known and unsurprising locale [17].

Currently security that is founded on point of entry authentication that remains static for the duration of interaction is unable to prevent misuse succeeding a hijack, when following a legitimate log-on the piece of equipment is illicitly removed or used by another. If this occurs and the device is kept active and not switched off, free and open use can be maintained for a significant period of time. With 85% of owners admitting their mobile phone is on for over 10 hours per day [9], to counteract this weakness proposals to degrade service availability over time have been made [13],[14] enabling the device to shut down functionality unless re-authentication occurs.

As several gadgets are frequently carried simultaneously any intrinsic security weakness is amplified especially as

people will often use the same PIN for more than one device, if not all of them [9]. Once one is compromised by the discovery or disclosure of the PIN then it is possible that all the owned devices become vulnerable.

To circumvent the associated weaknesses of point-of-entry authentication it would be advantageous to augment the process with ongoing reassurances. Establishing user identification during the initial sign-on and then authenticating at intervals to maintain confidence allows opened devices to be secured against potential theft or loss. Although a device may be open and fully usable upon stealing, without successful re-authentication within a limited timeframe it would become inoperable. Ongoing re-authentication can be either intrusive by interrupting the user and requiring a password or PIN to be entered, or non-intrusive in the case of biometrics where for example the user's identity is confirmed by their typing characteristics [18],[19]. If correctly implemented, either will be an improvement upon the current situation but it is important to consider the most flexible and appropriate approach.

Section III discusses and then outlines a potential framework that addresses these weaknesses and provides a means by which mobile device security could be enhanced.

### III. ENHANCING SECURITY FOR MOBILE DEVICES

With individuals being likely to carry more than one portable device and simultaneously interact with, or at least be known to, other technology in their local vicinity at any given time, possibilities exist to maximize this security potential. For instance, in the morning on leaving the house a worker might activate their business phone and Personal Digital Assistant (PDA) whilst at the same time picking up their car keys. By leveraging the relationship the user has with these multiple devices and associating the identification knowledge that each independently possesses, enhanced assurance of the owner's identity can be determined. At the time of authentication, each device establishes a confidence in the identity of the user, either true or false. Facilitating a means of communicating the current security status between the unique entities would allow them to bolster their own confidence in the user's identity.

Utilizing environmental awareness<sup>2</sup> and enabling the devices to request and trade their current authentication confidence, would provide a more flexible approach to security administration. This self-governing method would allow the party devices to adjust their own status through the consideration of their peers and the surrounding environment. The main drive is to achieve a position where a newly activated piece of equipment would not require an authentication process to be undertaken because the surrounding near vicinity contains sufficient confidence in the user's identity, that it is considered unnecessary to do so. Additionally, as the user relocates between areas of differing threat (public spaces to a home or work environment), the

---

<sup>1</sup> As opposed to devices such as laptop computers that generally rely on a user name and associated password.

---

<sup>2</sup> Devices such as mobile phones and laptop computers detect cellular and wireless networks and other such information that provide a means to recognize their current locale at any given time.

devices could relay the situation to their counterparts allowing each to react accordingly.

In order for such a system to operate, it is necessary to first give some consideration to the underpinning requirements:

#### A. Biometrics

Using biometrics fits the requirements of a heightened security methodology for mobile devices, on the basis that they are characteristics that cannot be forgotten, divulged or lost by their owner [20]. Further, biometrics divides into two distinct tranches of study, physiological and behavioral [21]. The use of physiological biometrics is more often preferred for identification purposes because of the greater degree of uniqueness, experienced consistency and resilience to external corruption [22]. However, it is best suited to point-of-entry scenarios where an individual would be happy or certainly less discontent to tolerate the inconvenience necessary to undergo the required process of identification. For instance, having to place a hand upon a particular device, or head at a specific angle, to enable the relevant scan to be taken are both obtrusive procedures. Conversely, behavioral biometrics lend themselves to authentication scenarios where the identity of the individual is already established and confirmation of a user's continuing presence is sought. Behavioral traits can be detected unobtrusively enabling validation to be carried out imperceptibly to the user [9],[14],[18]. Capturing a voice sample during a mobile telephone conversation would allow the device to compare extracted voice patterns and nuances against a known and expected reference vocal template. Executing such a process regularly during use, facilitates a means by which the mobile device could gain appropriate confidence in the user's identity during extended periods of otherwise unchecked access.

Although upon first consideration a single layer of protection maybe deemed sufficient, [23] observed that "Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates". With individual biometrics failing to meet appropriate levels of acceptance, attention has been turned to combining techniques in multimodal authentication systems [14],[24]. There are a plethora of circumstances where multimodal biometrics are advantageous and would be the authentication method of choice but not readily available because of technological limitations.

By combining devices and available techniques it may be possible to achieve the same objective without multi-layering on any individual piece of equipment. Drawing together authentication confidence from a number of disparate devices would enable any one entity to make stronger and more informed judgment calls. With the likelihood that distinct devices will utilize different biometric techniques with differing rigor and strength, combining the otherwise unilateral decisions will further improve the ultimate recognition process. An added advantage of this is that captured identity samples could be communicated from devices without the processing capability to analyze the data,

to a local entity sufficiently powerful to complete the operation. However, if no local device was available but network or internet services were, the samples could alternatively be passed to a remote authentication system where the analysis could be executed and decision returned.

#### B. Security degradation

It can be argued that rather than remain static, the authentication confidence should be eroded over time, reducing service and application availability<sup>3</sup> [13]. Upon reaching a significant point, re-authentication would be necessary to re-determine the user's credentials and once more allocate appropriate confidence. Should this undertaking be unsuccessful (as anticipated in the case of a hijacking), service provision would degrade to such a degree that the entity would be rendered un-usable; protecting the information stored within and further misuse.

Some functions of mobile devices are more sensitive than others and their illicit use could potentially incur greater cost or harm. Rather than regarding every type of feature equally it is sensible to enable a degree of flexibility in how each is treated and protected with the introduction of confidence cut-offs. Operative tasks and applications could be allocated a security tariff allowing some functions to be carried out with a low confidence whilst at an equal level others would be blocked entirely. For instance with low confidence it would be acceptable to operate a calculator application but the ability to instigate a telephone call would be barred. Additionally, the calculator application would not only function at a lower tariff but it could be allowed a slower rate of degradation implying that it would take longer for it to reach the cutoff point of inoperability [20].

Dynamically adjusting the rate of decay to reflect the environment in which a device is being used will enable the model to adapt. In public, high-risk areas, a steeper rate of erosion could be utilized, whilst in a familiar and perceived low risk environment a flatter more sedate timescale employed. Indeed the decay space becomes a complex n-dimensional curve with degrees of freedom including application sensitivity, time, location, method of authentication and user behavior. Consideration of these factors and more will dictate at what percentage point confidence will be at any given moment in time.

Section III(C) builds on this approach and further explores how it could be used to improve security.

#### C. Device interaction

As proposed in section III(A) enabling disparate devices owned by the user to communicate will bring advantages in achieving strong methods of authentication. Additional identity confidence could also be obtained by gathering the authentication status of nearby devices. Distinct devices are likely to utilize different methods of authentication and using this array of approaches arguably establishes a more robust security profile. By enabling entities to recognize each other

---

<sup>3</sup> For instance, within the first few minutes following device activation the likelihood that the owner has been replaced by an impostor is much less than it would be after an hour.

and communicate their current state of user identity confidence, the degradation process could be slowed or even reversed.

Fig. 1 below shows a conceptual diagram of the relationship paths that might be established by a user's set of personal devices<sup>4</sup> and the variety of authentication techniques that might be employed.

Information sharing would be carried out between trusted pairs via a near field communication (NFC) channel such as Bluetooth. Utilizing NFC will ensure the security envelope is restricted to the local vicinity and acquired confidence is confined to entities within the physical proximity of the requesting device. Additionally, ensuring the intra device trust would effectively eliminate responses from unknown third party entities. Without doing this, a degrading device might poll the surrounding near vicinity for listening pieces of equipment and one owned by a different user might respond with an assurance of confidence which although true, would not be in the same user's identity. If accepted and permitted to proceed, the alien device would falsely bolster the observed identity confidence.

Furthermore, associating a weighting tariff to the method of authentication would allow equipment to utilize robust techniques that they would otherwise not have the ability to use [13]. The tariff system could then be extended to either slow or accelerate the rate of confidence decay (see section III(B)). For instance, a laptop computer might have an inbuilt fingerprint scanner with a high tariff of robustness. The same

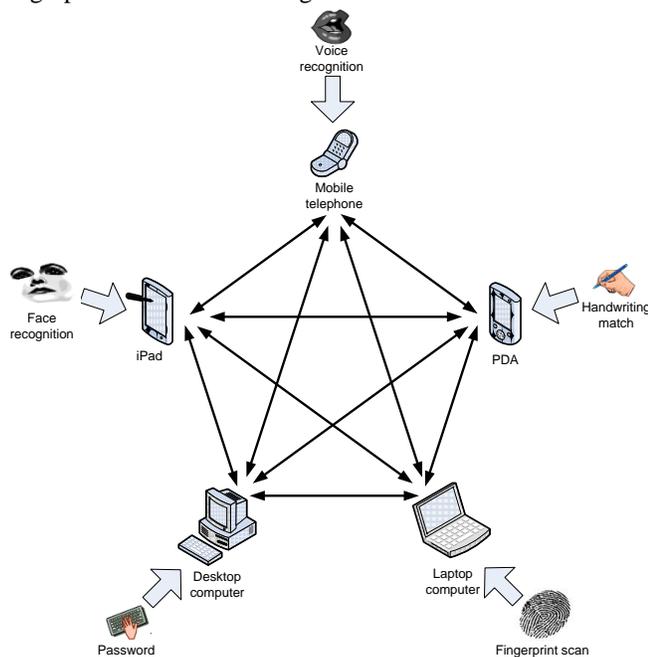


Figure 1. The potential intra-device relationship and authentication techniques for a given user

<sup>4</sup> The mobile telephone is shown as centric to the scheme because of the likelihood that it is the one device that is ever present upon the legitimate user's person.

person's mobile telephone might only authenticate via a PIN number; a far less rigorous form of authentication. Thus by drawing upon the laptop's high tariff confidence, the mobile phone could gain an enhanced state of assurance and thereby extend a slower degradation than would otherwise have been appropriate. Introducing additional items and allowing every device to trade and negotiate confidence with every other will synthesize a flexible and self maintaining security environment.

This region of localized security can also be augmented by constructing the system in such a way that it can be introduced and subsequently recognize the local environment. This could be achieved by sensing available wireless networks and associating them with locations, allowing degradation tariffs to be correspondingly allocated within an administration function. The tariffs or weightings associated with public spaces can be utilized to degrade confidence more rapidly than those linked with more private arenas. By integrating the ability to detect and consequently recognize known locales, the model will react and adapt independently of human intervention. Hence, as the user crosses environment boundaries security and awareness can be immediately heightened or relaxed respectively increasing or reducing the frequency that re-authentication is requested. It may even be possible to associate the user's behavior and device interaction with locations or at least perceived security threats. That is, through use and experience each device might be able to recognize that the user only activates certain applications when at home or in equally low threat surroundings. Vice versa particular services or operations might be utilized in public areas or correspondingly high risk locations, allowing immediate yet discrete security adjustments to be made. This is achievable via the adaptation of behavior based identification techniques [25].

#### IV. SYSTEM ANATOMY

Having explored the core features and requirements of the proposed approach to mobile device security it is now possible to examine and discuss in greater detail how such a framework could be implemented. This section addresses the core elements, the role each plays and how they might be united to achieve a robust and adaptive security system.

The suggested system would consist of a core control engine with the ability to hook into and utilize five peripheral elements; the local environment, database storage, device operating system, one or more authentication mechanisms and the other member devices. Fig. 2 outlines how the elements would combine and the direction of information flow between the disparate parts of the anatomy. It also illustrates the elements that are located within the physical body of the device and those that lie beyond.

Centric to each device is envisaged to be the Adaptive Security Control Engine (ASCE), which will manage and direct the internal security. It will be required to hook into the device operating system in order to influence and apply relevant security policies based upon the action and authentication success of the user. Post-initial authentication and the establishment of an identity confidence the ASCE

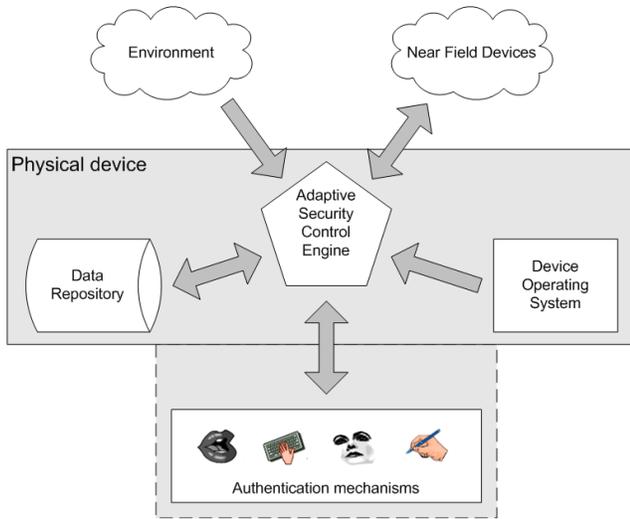


Figure 2. Adaptive security environment

will administer the degradation of confidence using the methodology (or similar to) outlined in subsection III(B). This concept of degradation will potentially be further influenced by the environment in which the device is being operated. To achieve this, ASCE will need to utilize an environment-sensing module that will learn to recognize localities and their associated threat, and use this to affect the rate at which the confidence in the user's identity is being eroded. As discussed earlier in this document, operating a laptop at home is expected to be less of a threat than using one whilst waiting in a public space; by adjusting the rate of decay accordingly, these expectations can be incorporated into the framework.

Authentication, although controlled and requested by the ASCE, will be carried out by authentication mechanisms that communicate via a generic interface. This will allow the ASCE to be a portable concept that can be applied to many different types of device, making it independent of a specific set of hardware. The generic approach aligns itself with the

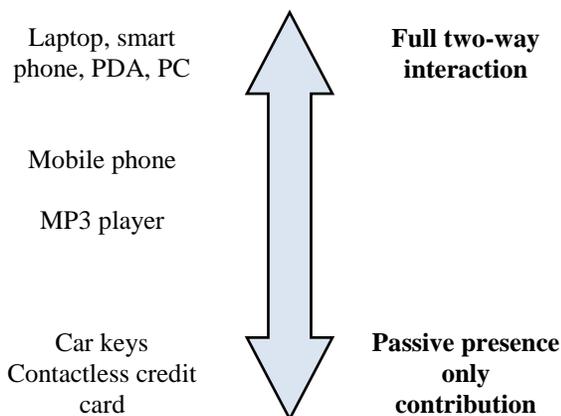


Figure 3. Varying levels of device sophistication and consequent contribution to the authentication process.

objectives of the BioAPI Consortium [26] which has specified an international standard for interfacing to biometric systems. Utilizing this framework and extending it to both biometric and non-biometric methodologies would enable a single engine to accept and function with a number of identity confirming processes. That is, a mobile phone should be typically capable of utilizing authentication via PIN, voice recognition, facial recognition or even keystroke analysis. One or more of these could be plugged into the engine facilitating the necessary provision of identity recognition.

Some devices will operate a two-way interaction with their surrounding security counterparts; for instance a laptop computer will both request and provide security details. However, it may be possible to utilize some entities that only contribute by their presence, providing a form of token-based security. Car keys are an example of such an item; incorporating these so that their mere presence, indicated by replying to a polled request, can be used to bolster security confidence in the user's identity (i.e. because the holder can show themselves to be in possession of a larger set of physical artifacts associated with the legitimate user).

Fig. 3 above shows a succinct representation of the relative sophistication of devices that might be used by the ASCE. It can be argued that any device that can be placed on the scale from "Full two-way" to "Passive presence only" can in some way contribute to the security envelope. Thus this approach is ultimately flexible and scalable to a huge variety of devices with or without built in processing intelligence.

Finally, as illustrated in Fig. 2, the ASCE will use a data repository to store relevant information, parameters and details, of its own status and other devices in the security partnership. The repository is made up of a number of data tables that would store both persistent reference information and working details updated in real-time.

## V. DISCUSSION

In addition to the base technological concepts there are other matters that will require careful consideration prior to implementation of the framework. Privacy and the associated risk of transmitting biometric template information between devices when one is incapable of unilaterally processing a sample, is such an example. Appropriate encryption and communication channel security will have to be employed to protect against eavesdropping and remove the potential for man-in-the-middle attacks. Introducing such protection will incur additional processing overheads that will impact upon the operational performance of the framework.

Indeed, computational, memory, battery and network performance issues also demand investigation to ensure that the framework can be adapted to function on as many categories and types of device as possible. Ultimately it is desirable to employ the smallest footprint possible, so it is inevitable that there will be some element of compromise to avoid precluding potential technology.

Although this paper has proposed biometrics as a suitable authentication candidate, it is important to note that with

distinct methods greatly differing levels of performance can be experienced. This is amplified by the need to adapt some biometric techniques so they can be employed in a non-intrusive manner [9]. Designing the framework to operate with a plug-and-play capability will lessen some of these demands and enable alternatives to be used but will concurrently increase the complexity of the necessary interface.

Trust is another major area of focus. Trust between devices will need to be established and at times revoked. It is imperative that this process correctly addresses usability and is implemented in a way that is logical, secure, yet easy to use. Aside from aesthetics, devices will also need the ability to receive and utilize un-trusted environmental information. Parsing this information correctly will enable devices to draw appropriate detail whilst remaining secure and removed from threat.

Operational thresholds for applications and device services are one final area that requires further investigation. As yet it is unclear how best to invoke them; a simple ranking and user selected scale may be suitable for some applications but for others a more complex approach dependent upon a number of variables might be more fitting. As the design of the framework evolves it is hoped that these factors will clarify and allow appropriate decisions to be taken.

## VI. CONCLUSION

It is desirable that security and the way in which most users authenticate themselves with mobile devices should now evolve to a more holistic level. For too long manufacturers have had little choice but to rely upon password or PIN-based mechanisms to secure what are becoming ever more sophisticated devices, with ever increasing replacement and misuse costs. This paper suggests an approach that will allow disparate personal devices to trade security information and glean confidence of identity from their peers. It may potentially offer a way in which user identity can be ascertained and communicated to non-personal devices, supporting the interactions individual's have and augmenting the safeguards that are currently in place.

The ability to create a near-field security space will enable technologists to review device activation procedures. Under certain circumstances they may even be able to demote or possibly remove a user's requirement to repetitively logon to multiple entities during successive activations. Further work will undertake the development of a prototype framework to determine the feasibility and working advantage of such an approach, whilst reviewing the perception and response of the wider user population.

## ACKNOWLEDGMENT

It is acknowledged that the research outlined in this paper has been undertaken with the generous backing of Orange-France Telecom.

## REFERENCES

- [1] "Hotspot usage is increasingly shifting away from notebooks and laptops and toward handhelds", In-stat website, available: <http://www.instat.com/newmk.asp?ID=2695&SourceID=0000035200000000000> [accessed: 18 Jan. 09].
- [2] "Reducing Crime: Robbery", Home Office website, available: <http://www.homeoffice.gov.uk/crime-victims/reducing-crime/robbery/> [accessed: 27 Feb. 10].
- [3] " 'IFraud' Fuels Rise In Scam Phone Claims", CPP Group website, available: <http://www.cppgroupplc.com/news/press-release.shtml> [accessed: 26 Feb. 10].
- [4] "Mountains of Mobiles Left in the Back of New York Cabs", Credant website, available: <http://www.credant.com/news-a-events/press-releases/229-mountains-of-mobiles-left-in-the-back-of-new-york-cabs.html> [accessed: 26 Feb. 10].
- [5] L. Rohde, "UK Government Asks Industry to Fight Mobile Phone Theft", Infoworld, vol. 23, Jan. 2001, no. 5, p. 76.
- [6] "Design Out Crime: Hot Product Crime", Design Council website, available: <http://www.designcouncil.org.uk/Design-Council/Files/Landing-pages/Design-Out-Crime/Hot-Product-crime/> [accessed: 02 Mar 10].
- [7] H. M. Wood, "The Use of Passwords for Controlling Access to Remote Computer Systems and Services", Proc. of American Federation of Information Processing Societies: 1977 National Computer Conference (AFIPS 77), AFIPS Press, Jun. 77, pp. 27-33, doi: 10.1145/1499402.1499410.
- [8] E. Albrechtsen, "A Qualitative Study of Users' Views on Information Security", Computers & Security, vol. 26, Jun. 2007, no. 4, pp. 276-289, doi:10.1016/j.cose.2006.11.004.
- [9] N. L. Clarke and S. M. Furnell, "Authentication of Users on Mobile Telephones – A Survey of Attitudes and Opinions", Computers & Security, vol. 24, Oct. 2005, no. 7, pp. 519-527, doi:10.1016/j.cose.2005.08.003.
- [10] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proc. of the IEEE, IEEE Press, vol. 91, Dec. 2003, no. 12, pp. 2019-2040, doi: 10.1109/JPROC.2003.819611.
- [11] K-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B-L. Tai, J. Cook and E. E. Schultz, "Improving Password Security and Memorability to Protect Personal and Organizational Information", Int. J. of Human-Computer Studies, vol. 65, Aug. 2007, no. 8, pp. 744-757, doi: 10.1016/j.ijhcs.2007.03.007.
- [12] T. Sim, S. Zhang, R. Janakiraman and S. Kumar, "Continuous Verification Using Multimodal Biometrics", IEEE Trans. on Pattern Analysis and Machine Intelligence, IEEE Press, vol. 29, Apr. 2007, no. 4, pp. 687-700, doi:10.1109/TPAMI.2007.1010.
- [13] N. L. Clarke and S. M. Furnell, "Advanced User Authentication for Mobile Devices", Computers & Security, vol. 26, Mar. 2007, no. 2, pp. 109-119, doi:10.1016/j.cose.2006.08.008.
- [14] A. Azzini, E. Damiani and S. Marrara, "Ensuring the Identity of a User in Time: A Multi-Modal Fuzzy Approach", Proc. IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMS A 2007), IEEE Press, 27-29 Jun. 2007, pp. 94-99, doi:10.1109/CIMS A.2007.4362546.
- [15] A. T. B. Jin, D. N. C. Ling and A. Goh, "Biobhashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number", Pattern Recognition, vol. 37, Nov. 2004, no. 11, pp. 2245-2255, doi:10.1016/j.patcog.2004.04.011.
- [16] D-J. Kim and K-S. Hong, "Multimodal Biometric Authentication using Teeth Image and Voice in Mobile Environment", IEEE Trans. on Consumer Electronics, IEEE Press, vol. 54, Nov. 2008, no. 4, pp. 1790-1797, doi: 10.1109/TCE.2008.4711236.
- [17] R. J. Hulsebosch and P. W. G. Ebben, "Enhancing Face Recognition with Location Information", Proc. 2008 Third International Conference on Availability, Reliability and Security (ARES 08), IEEE Press, 4-7 Mar. 2008, pp. 397 - 403, doi: 10.1109/ARES.2008.45.

- [18] N. L. Clarke and S. M. Furnell, "Authenticating Mobile Phone Users Using Keystroke Analysis", *Int. J. of Information Security*, vol. 6, Jan. 2007, no. 1, pp. 1-14, doi:10.1007/s10207-006-0006-6.
- [19] F. Monrose and A. D. Rubin, "Keystroke Dynamics as a Biometric for Authentication", *Future Generation Computer Systems*, vol. 16, Feb. 2000, no. 4, pp. 351-359, doi: 10.1016/S0167-739X(99)00059-X.
- [20] S. M. Furnell, N. L. Clarke and S. Karatzouni, "Beyond the PIN: Enhancing user authentication for mobile devices", *Computer Fraud & Security*, vol. 2008, Aug. 2008, no. 8, pp. 12-17, doi:10.1016/S1361-3723(08)70127-1.
- [21] A. C. Weaver, "Biometric Authentication", *Computer*, vol. 39, Feb. 2006, no. 2, pp. 96-97, doi: 10.1109/MC.2006.47.
- [22] S. Prabhakar, S. Pankanti and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy*, vol. 1, Mar. 2003, no. 2, pp. 33-42, doi: 10.1109/MSECP.2003.1193209.
- [23] A. Ross and A. K. Jain, "Multimodal Biometrics: An Overview", *Proc. of 12th European Signal Processing Conference (EUSIPCO)*, EURASIP Press, Sep. 2004, pp. 1221-1224.
- [24] O. Arandjelovic, R. Hammoud and R. Cipolla, "Multi-sensory Face Biometric Fusion (for Personal Identification)", *Proc. IEEE 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 06)*, IEEE Press, 17-22 Jun. 2006, p. 52, doi: 10.1109/CVPRW.2006.136.
- [25] A. Boukerche and M. S. M. Annoni Notare, "Behavior-based Intrusion Detection in Mobile Phone Systems", *Parallel and Distributed Computing*, vol. 62, Sep. 2002, no. 9, pp. 1476-1490, doi: 10.1006/jpdc.2002.1857.
- [26] "Objectives", *BioAPI Consortium website*, available: <http://www.bioapi.org/objectives.asp> [accessed: 03 Dec. 09].

# Authentication Aura - A distributed approach to user authentication

C. G. Hocking<sup>1</sup>, S. M. Furnell<sup>1,2</sup>, N. L. Clarke<sup>1,2</sup> and P. L. Reynolds<sup>1</sup>

<sup>1</sup> Centre for Security, Communications and Network Research, University of Plymouth,  
Drake Circus, Plymouth, United Kingdom  
*info@csan.org*

<sup>2</sup> School of Computer and Security Science, Edith Cowan University,  
Perth, Western Australia

**Abstract:** The ubiquitous password or personal identification number (PIN) has been the accepted form of user authentication on mobile devices since their inception. With increasing numbers of owners failing to implement these simple barriers or taking any greater precaution against misuse, the requirement to secure the information contained within has never been so great. This paper proposes a new approach to identity authentication on mobile devices based upon a framework that can transparently improve user security confidence. Information pertaining to user authentication is shared amongst the owner's devices, collectively enabling a near field adaptive security envelope to be established and maintained around the individual; the user's Authentication Aura.

**Keywords:** authentication, identification, mobile, security, biometric, authentication aura.

## I. Introduction

The aspiration of people to be mobile and yet remain in communication with colleagues, family and friends has driven the use of devices that support and complement this lifestyle. Estimates suggest that worldwide Wi-Fi hotspot usage during 2009 grew to 1.2 billion connections, an increase of 47% from 2008, with this being driven by a 50% growth in the sale of Wi-Fi capable handsets between 2007 and 2008 [1]. Surveys indicate that, mobile devices have become the preferred method of accessing the Internet amongst young users [2]. With technological evolution enabling powerful and sophisticated systems to be accommodated into these handheld electronic gadgets, their extensive storage and processing capabilities has made them an increasing target for thieves. In 2007-8 over 700,000 handsets were stolen in the UK, with 50% of all robberies targeting a mobile phone in the items taken and in 33% of those offences it was the only stolen possession [3]. Between May and June 2009 alone, the UK saw an 11% increase in the reporting of missing/stolen mobile phones, with 84% of theft victims failing to retrieve their lost handsets [4].

However, theft is not the sole reason for concern; a New York survey revealed that during a six month period in 2008, 31,544 phones and 2,752 other types of handheld device (laptops, PDAs, memory sticks etc.) were simply left in the

city's Yellow Cabs, an average of more than two per cab [5]. In this climate, the requirement to protect and secure the potentially large volumes of sensitive and personal information contained within these desirable pieces of equipment is imperative and even acknowledged and supported by Government [6], [7].

As time passes and the proportion of technically-aware digital natives (i.e. those who have been born and grown up surrounded by technology) [8] grows, one would expect security usage and awareness to be greatly improved. Surprisingly though, this is not the case. Recent research has indicated that there has been no significant improvement in users' attitudes or habits during 2005 to 2010 [2], [9]. In this period the use of a PIN as a means of security by 18-25 year-olds has in fact dropped by 50% [2]. Device owners are simply failing to take responsibility for protecting themselves.

The problem is magnified because users are finding themselves in possession of an ever growing number of digital devices, each one having its own associated security requirements. With several being carried concurrently, at the moment of initial use it is likely that similar procedures of authentication are undertaken repeatedly across the disparate entities to ensure full activation. This repetitive and time-consuming operation raises the question of whether there is a better way and does the collective identity knowledge possessed by the multiplicity of secured devices utilized by an individual at any given time present an opportunity to improve security. As each device is activated a set of authentication credentials are determined and access is either granted or denied. By enabling the individual and distinct devices to communicate their own authentication status and to share established user identity confidence it may be possible to synthesize an enhanced form of security.

This paper explores this concept and proposes an approach through which authentication credentials can be distributed amongst devices and how this information can be used to create a novel method of security and user control. It addresses the requirements to produce a flexible, adaptive and non-intrusive security mechanism that will meet future demands and provide a foundation for further development. Firstly, the background explores the current methods of

securing mobile devices and the associated weaknesses. Once these foundations have been laid the paper continues to outline the new proposals and considers how they will improve upon the situation at present.

## II. Background

Security is founded on three key principles – something an individual knows, they possess or they are [9]. Knowledge and possession based security both rely upon the inherently weak link in the chain – the user. The first utilizes a piece of significant or memorable information which is often forgotten or written down [11]; the second, the presentation of a physical key or token at the required moment. Forgetting, mislaying or losing the crucial item or information will bar further access attempts.

The ubiquitous point of entry user identity code/password has been rendered susceptible to abuse through the inability or unwillingness of individuals to protect and administer this sensitive information correctly [9]. To maintain security it is supposedly known or more precisely memorized exclusively by the creator [12] but is too often shared or inadvertently communicated [13]. Although different; identification and authentication both rely upon the recognition of the identity of a user interacting with a device at any given moment. Hand held mobile devices typically assume the identity of the user and utilize personal identification numbers (PINs) to authenticate<sup>1</sup> this at point-of-entry. The authentication is Boolean; the subject is either deemed to be whom they purport to be or they are not, without any middle ground. Frequently passing the one-off process will permit unregulated access to all facilities and utilities installed on the device [14]. Therefore once access has been gained the ability to incur large telephone bills or excessive high-cost data downloads is readily available to impostors who compromise the PIN.

In the search for evermore appropriate and robust authentication, attention has turned to biometrics (something the user is) to establish methods that cannot easily be compromised, are non-intrusive and equally eliminate the potential threat posed by social engineering [15]. A finer granularity of identification can be achieved; ultimately the device will either issue or refuse access to the user, however the starting confidence can precisely reflect how well the supplied identity matches the known template sample. Having this ability will allow a device to tailor its reaction to strong and weak authentication attempts accordingly. Further, without fundamentally changing the habits to which users are accustomed improvements can be implemented. As a supplementary development, layered authentication techniques have been explored and employed to compound protection and expand the sophistication required to circumvent defence mechanisms including; password and facial recognition [16], fingerprint scan and tokenized random number [17], teeth imaging and voice pattern verification [18]. This can then be reinforced by elements such as location information which indicates whether or not a

user is operating in a known and unsurprising locale [19].

Currently security that is founded on point of entry authentication that remains static for the duration of interaction is unable to prevent misuse succeeding a hijack, when following a legitimate log-on the piece of equipment is illicitly removed or used by another. If this occurs and the device is kept active and not switched off, free and open use can be maintained for a significant period of time. With 85% of owners admitting their mobile phone is on for over 10 hours per day [9], to counteract this weakness proposals to degrade service availability over time have been made [15], [16] enabling the device to shut down functionality unless re-authentication occurs.

As several gadgets are frequently carried simultaneously any intrinsic security weakness is amplified especially as people will often use the same PIN for more than one device, if not all of them [9]. Once one is compromised by the discovery or disclosure of the PIN then it is possible that all the owned devices become vulnerable.

To circumvent the associated weaknesses of point-of-entry authentication it would be advantageous to augment the process with ongoing reassurances. Establishing user identification during the initial sign-on and then authenticating at intervals to maintain confidence allows opened devices to be secured against potential theft or loss. Although a device may be open and fully usable upon stealing, without successful re-authentication within a limited timeframe it would become inoperable. Ongoing re-authentication can be either intrusive by interrupting the user and requiring a password or PIN to be entered, or non-intrusive in the case of biometrics where for example the user's identity is confirmed by their typing characteristics [20], [21]. If correctly implemented, either will be an improvement upon the current situation but it is important to consider the most flexible and appropriate approach.

Section III discusses and then outlines a potential framework that addresses these weaknesses and provides a means by which mobile device security could be enhanced.

## III. Enhancing Security for Mobile Devices

With individuals being likely to carry more than one portable device and simultaneously interact with, or at least be known to, other technology in their local vicinity at any given time, possibilities exist to maximize this security potential. For instance, in the morning on leaving the house a worker might activate their business phone and Personal Digital Assistant (PDA) whilst at the same time picking up their car keys. By leveraging the relationship the user has with these multiple devices and associating the identification knowledge that each independently possesses, enhanced assurance of the owner's identity can be determined. At the time of authentication, each device establishes a confidence in the identity of the user, either true or false. Facilitating a means of communicating the current security status between the unique entities would allow them to bolster their own confidence in the user's identity.

<sup>1</sup> As opposed to devices such as laptop computers that generally rely on a user name and associated password.

Utilizing environmental awareness<sup>2</sup> and enabling the devices to request and trade their current authentication confidence, would provide a more flexible approach to security administration. This self-governing method would allow the party devices to adjust their own status through the consideration of their peers and the surrounding environment. The main drive is to achieve a position where a newly activated piece of equipment would not require an authentication process to be undertaken because the surrounding near vicinity contains sufficient confidence in the user's identity, that it is considered unnecessary to do so. Additionally, as the user relocates between areas of differing threat (public spaces to a home or work environment), the devices could relay the situation to their counterparts allowing each to react accordingly.

In order for such a system to operate, it is necessary to first give some consideration to the underpinning requirements:

#### A. Biometrics

Using biometrics fits the requirements of a heightened security methodology for mobile devices, on the basis that they are characteristics that cannot be forgotten, divulged or lost by their owner [22]. Further, biometrics divides into two distinct tranches of study, physiological and behavioural [23]. The use of physiological biometrics is more often preferred for identification purposes because of the greater degree of uniqueness, experienced consistency and resilience to external corruption [24]. However, it is best suited to point-of-entry scenarios where an individual would be happy or certainly less discontent to tolerate the inconvenience necessary to undergo the required process of identification. For instance, having to place a hand upon a particular device, or head at a specific angle, to enable the relevant scan to be taken are both obtrusive procedures. Conversely, behavioural biometrics lend themselves to authentication scenarios where the identity of the individual is already established and confirmation of a user's continuing presence is sought. Behavioural traits can be detected unobtrusively enabling validation to be carried out imperceptibly to the user [9], [16], [20]. Capturing a voice sample during a mobile telephone conversation would allow the device to compare extracted voice patterns and nuances against a known and expected reference vocal template. Executing such a process regularly during use, facilitates a means by which the mobile device could gain appropriate confidence in the user's identity during extended periods of otherwise unchecked access.

Although upon first consideration a single layer of protection maybe deemed sufficient, [25] observed that "Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates". With individual biometrics failing to meet appropriate levels of acceptance, attention has been turned to combining techniques in multimodal authentication systems [16], [26]. There are a

plethora of circumstances where multimodal biometrics are advantageous and would be the authentication method of choice but not readily available because of technological limitations.

By combining devices and available techniques it may be possible to achieve the same objective without multi-layering on any individual piece of equipment. Drawing together authentication confidence from a number of disparate devices would enable any one entity to make stronger and more informed judgment calls. With the likelihood that distinct devices will utilize different biometric techniques with differing rigor and strength, combining the otherwise unilateral decisions will further improve the ultimate recognition process. An added advantage of this is that captured identity samples could be communicated from devices without the processing capability to analyze the data, to a local entity sufficiently powerful to complete the operation. However, if no local device was available but network or internet services were, the samples could alternatively be passed to a remote authentication system where the analysis could be executed and decision returned.

#### B. Security degradation

It can be argued that rather than remain static, the authentication confidence should be eroded over time, reducing service and application availability<sup>3</sup> [15]. Upon reaching a significant point, re-authentication would be necessary to re-determine the user's credentials and once more allocate appropriate confidence. Should this undertaking be unsuccessful (as anticipated in the case of a hijacking), service provision would degrade to such a degree that the entity would be rendered un-usable; protecting the information stored within and further misuse.

Some functions of mobile devices are more sensitive than others and their illicit use could potentially incur greater cost or harm. Rather than regarding every type of feature equally it is sensible to enable a degree of flexibility in how each is treated and protected with the introduction of confidence cut-offs. Operative tasks and applications could be allocated a security tariff allowing some functions to be carried out with a low confidence whilst at an equal level others would be blocked entirely. For instance with low confidence it would be acceptable to operate a calculator application but the ability to instigate a telephone call would be barred. Additionally, the calculator application would not only function at a lower tariff but it could be allowed a slower rate of degradation implying that it would take longer for it to reach the cut-off point of inoperability [22].

Dynamically adjusting the rate of decay to reflect the environment in which a device is being used will enable the model to adapt. In public, high-risk areas, a steeper rate of erosion could be utilized, whilst in a familiar and perceived low risk environment a flatter more sedate timescale employed. Indeed the decay space becomes a complex n-dimensional curve with degrees of freedom including application sensitivity, time, location, method of authentication and user behaviour. Consideration of these

<sup>2</sup> Devices such as mobile phones and laptop computers detect cellular and wireless networks and other such information that provide a means to recognize their current locale at any given time.

<sup>3</sup> For instance, within the first few minutes following device activation the likelihood that the owner has been replaced by an impostor is much less than it would be after an hour.

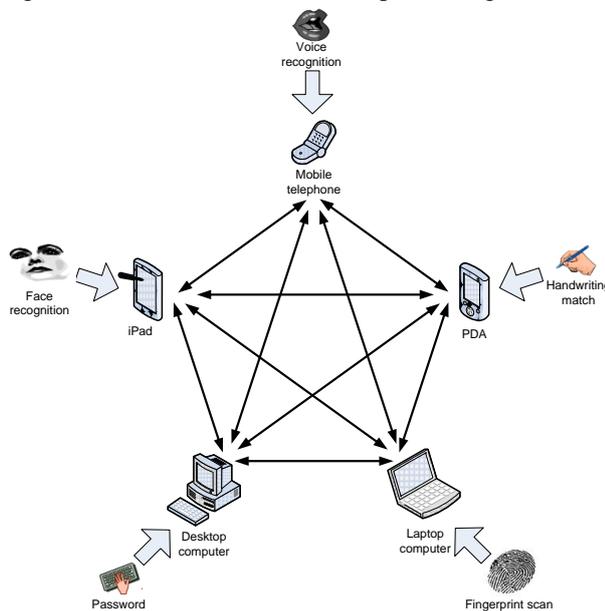
factors and more will dictate at what percentage point confidence will be at any given moment in time.

Section C builds on this approach and further explores how it could be used to improve security.

### C. Device interaction

As proposed at the start of this section, enabling disparate devices owned by the user to communicate will bring advantages in achieving strong methods of authentication. Additional identity confidence could also be obtained by gathering the authentication status of nearby devices. Distinct devices are likely to utilize different methods of authentication and using this array of approaches arguably establishes a more robust security profile. By enabling entities to recognize each other and communicate their current state of user identity confidence, the degradation process could be slowed or even reversed.

Figure 1 below shows a conceptual diagram of the



**Figure 1.** Potential intra-device relationship and authentication techniques

relationship paths that might be established by a user's set of personal devices<sup>4</sup> and the variety of authentication techniques that might be employed.

Information sharing would be carried out between trusted pairs via a near field communication (NFC) channel such as Bluetooth. Utilizing NFC will ensure the security envelope or authentication aura is restricted to the local vicinity and acquired confidence is confined to entities within the physical proximity of the requesting device. Additionally, ensuring the intra device trust would effectively eliminate responses from unknown third party entities. Without doing this, a degrading device might poll the surrounding near vicinity for listening pieces of equipment and one owned by a different user might respond with an assurance of confidence which although true, would not be in the same user's identity. If accepted and permitted to proceed, the alien device would falsely bolster the observed identity

<sup>4</sup> The mobile telephone is shown as centric to the scheme because of the likelihood that it is the one device that is ever present upon the legitimate user's person.

confidence.

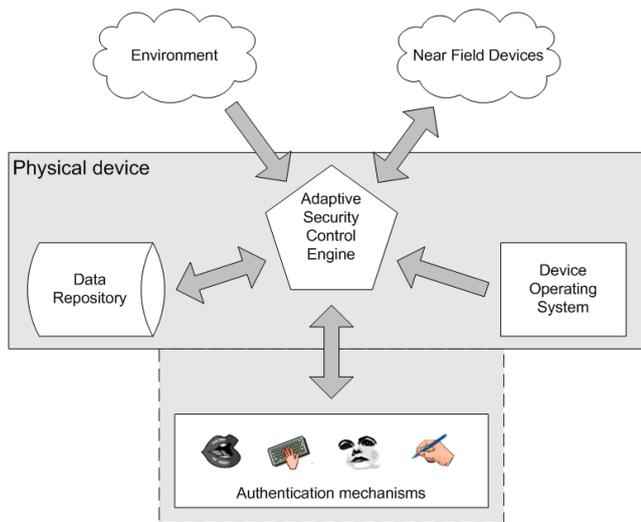
Furthermore, associating a weighting tariff to the method of authentication would allow equipment to utilize robust techniques that they would otherwise not have the ability to use [15]. The tariff system could then be extended to either slow or accelerate the rate of confidence decay (see section B). For instance, a laptop computer might have an inbuilt fingerprint scanner with a high tariff of robustness. The same person's mobile telephone might only authenticate via a PIN number; a far less rigorous form of authentication. Thus by drawing upon the laptop's high tariff confidence, the mobile phone could gain an enhanced state of assurance and thereby extend a slower degradation than would otherwise have been appropriate. Introducing additional items and allowing every device to trade and negotiate confidence with every other will synthesize a flexible and self maintaining security environment.

This region of localized security can also be augmented by constructing the system in such a way that it can be introduced and subsequently recognize the local environment. This could be achieved by sensing available wireless networks and associating them with locations, allowing degradation tariffs to be correspondingly allocated within an administration function. The tariffs or weightings associated with public spaces can be utilized to degrade confidence more rapidly than those linked with more private arenas. By integrating the ability to detect and consequently recognize known locales, the model will react and adapt independently of human intervention. Hence, as the user crosses environment boundaries security and awareness can be immediately heightened or relaxed respectively increasing or reducing the frequency that re-authentication is requested. It may even be possible to associate the user's behaviour and device interaction with locations or at least perceived security threats. That is, through use and experience each device might be able to recognize that the user only activates certain applications when at home or in equally low threat surroundings. Vice versa particular services or operations might be utilized in public areas or correspondingly high risk locations, allowing immediate yet discrete security adjustments to be made. This is achievable via the adaptation of behaviour based identification techniques [27].

## IV. System Anatomy

Having explored the core features and requirements of the proposed approach to mobile device security it is now possible to examine and discuss in greater detail how such a framework could be implemented. This section addresses the core elements, the role each plays and how they might be united to achieve a robust and adaptive security system.

The suggested system would consist of a core control engine with the ability to hook into and utilize five peripheral elements; the local environment, database storage, device operating system, one or more authentication mechanisms and the other member devices. Figure 2 outlines how the elements would combine and the direction of information flow between the disparate parts of the anatomy. It also illustrates the elements that are located within the physical body of the device and those that lie beyond.



**Figure 2.** Adaptive security environment

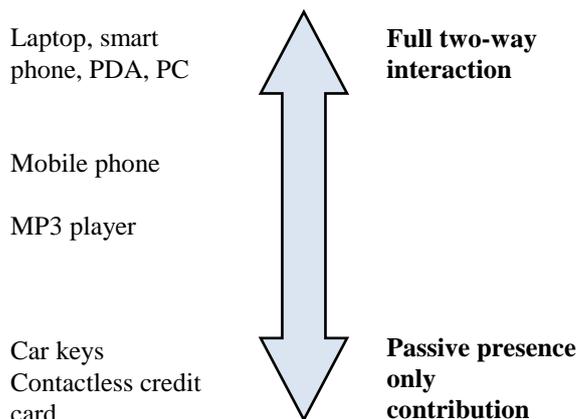
Centric to each device is envisaged to be the Adaptive Security Control Engine (ASCE), which will manage and direct the internal security. It will be required to hook into the device operating system in order to influence and apply relevant security policies based upon the action and authentication success of the user. Post-initial authentication and the establishment of an identity confidence the ASCE will administer the degradation of confidence using the methodology (or similar to) outlined in subsection B. This concept of degradation will potentially be further influenced by the environment in which the device is being operated. To achieve this, ASCE will need to utilize an environment-sensing module that will learn to recognize localities and their associated threat, and use this to affect the rate at which the confidence in the user's identity is being eroded. As discussed earlier in this document, operating a laptop at home is expected to be less of a threat than using one whilst waiting in a public space; by adjusting the rate of decay accordingly, these expectations can be incorporated into the framework.

Authentication, although controlled and requested by the ASCE, will be carried out by authentication mechanisms that communicate via a generic interface. This will allow the ASCE to be a portable concept that can be applied to many different types of device, making it independent of a specific set of hardware. The generic approach aligns itself with the objectives of the BioAPI Consortium [28] which has specified an international standard for interfacing to biometric systems. Utilizing this framework and extending it to both biometric and non-biometric methodologies would enable a single engine to accept and function with a number of identity confirming processes. That is, a mobile phone should be typically capable of utilizing authentication via PIN, voice recognition, facial recognition or even keystroke analysis. One or more of these could be plugged into the engine facilitating the necessary provision of identity recognition. Figure 2 indicates that these authentication mechanisms can potentially be either internal or external to the physical device. Thus it is imperative that the generic interface be capable of meeting this additional requirement

and interacting seamlessly with either approach.

Some devices will operate a two-way interaction with their surrounding security counterparts; for instance a laptop computer will both request and provide security details. However, it may be possible to utilize some entities that only contribute by their presence, providing a form of token-based security. Car keys are an example of such an item; incorporating these so that their mere presence, indicated by replying to a polled request, can be used to bolster security confidence in the user's identity (i.e. because the holder can show themselves to be in possession of a larger set of physical artefacts associated with the legitimate user).

Figure 3 below shows a succinct representation of the relative sophistication of devices that might be used by the ASCE. It can be argued that any device that can be placed on



**Figure 3.** Varying levels of device sophistication and consequential contribution to authentication

the scale from “Full two-way” to “Passive presence only” can in some way contribute to the authentication aura. Indeed it can be argued that the use of passive technology carries a greater significance than active devices. Items that contribute only by their presence are likely to be carried out-of-sight, for instance car keys or contactless travel cards are held in a pocket or handbag and are not readily visible to a potential thief. Thus this inclusive approach is ultimately flexible and scalable to a huge variety of devices with or without built in processing intelligence.

Finally, as illustrated in Figure 2, the ASCE will use a data repository to store relevant information, parameters and details, of its own status and other devices in the security partnership. The repository is made up of a number of data tables that would store both persistent reference information and working details updated in real-time.

## V. Discussion

In addition to the base technological concepts there are other matters that will require careful consideration prior to implementation of the framework. Privacy and the associated risk of transmitting biometric template information between devices when one is incapable of unilaterally processing a sample, is such an example. Appropriate encryption and communication channel security will have to be employed to protect against eavesdropping and remove the potential for

man-in-the-middle attacks. Introducing such protection will incur additional processing overheads that will impact upon the operational performance of the framework.

Indeed, computational, memory, battery and network performance issues also demand investigation to ensure that the framework can be adapted to function on as many categories and types of device as possible. Ultimately it is desirable to employ the smallest footprint possible, so it is inevitable that there will be some element of compromise to avoid precluding potential technology. The greater the number of devices that can be usefully employed within the aura, the more robust the system will become.

Although this paper has proposed biometrics as a suitable authentication candidate, it is important to note that with distinct methods greatly differing levels of performance can be experienced. This is amplified by the need to adapt some biometric techniques so they can be employed in a non-intrusive manner [15]. Designing the framework to operate with a plug-and-play capability will lessen some of these demands and enable alternatives to be used. Extrapolating this concept further, it will even allow devices to respond to the environment or mode of operation accordingly. Transparent authentication is the most desirable solution and equipping a mobile phone with the ability to undertake voice, facial and typing pattern recognition will provide techniques that cover the majority of occasions. However, such flexibility will concurrently increase the complexity of the necessary interface.

Trust is another major area of focus. Trust between devices will need to be established and at times revoked. It is imperative that this process correctly addresses usability and is implemented in a way that is logical, secure, yet easy to use. Aside from aesthetics, devices will also need the ability to receive and utilize un-trusted environmental information. Parsing this information correctly will enable devices to draw appropriate detail whilst remaining secure and removed from threat. Gaining the trust of users is one further aspect that should not be underestimated. For too long, owners have relied upon passwords and PINs to uphold their security. It will not be easy to sufficiently reassure them to accept an approach that could potentially not require them to enter any form of identity confirmation. If enough recognisable devices are present and the aura is strong, a newly activated device may be content to allow usage without any form of polled authentication.

Operational thresholds for applications and device services are one final area that requires further investigation. As yet it is unclear how best to invoke them; a simple ranking and user selected scale may be suitable for some applications but for others a more complex approach dependent upon a number of variables might be more fitting. It is required to empirically establish the latent potential that is believed to exist in the surroundings and the devices that are in regular everyday use. Through this experimentation, ongoing research and as the design of the framework evolves it is hoped that these factors will clarify and allow appropriate decisions to be taken.

## VI. Conclusion

It is desirable that security and the way in which most users authenticate themselves with mobile devices should now evolve to a more holistic level. For too long manufacturers have had little choice but to rely upon password or PIN-based mechanisms to secure what are becoming ever more sophisticated devices, with ever increasing replacement and misuse costs. This paper suggests an approach that will allow disparate personal devices to trade security information and glean confidence of identity from their peers. It may potentially offer a way in which user identity can be ascertained and communicated to non-personal devices, supporting the interactions individual's have and augmenting the safeguards that are currently in place.

The ability to create a near-field authentication aura will enable technologists to review device activation procedures. Under certain circumstances they may even be able to demote or possibly remove a user's requirement to repetitively logon to multiple entities during successive activations. Further work will undertake the development of a prototype framework to determine the feasibility and working advantage of such an approach, whilst reviewing the perception and response of the wider user population.

## Acknowledgment

It is acknowledged that the research outlined in this paper has been undertaken with the generous backing of Orange-France Telecom.

## References

- [1] "Hotspot usage is increasingly shifting away from notebooks and laptops and toward handhelds", In-stat website, available: <http://www.instat.com/newmk.asp?ID=2695&SourceID=00000352000000000000> [accessed: 18 Jan. 09].
- [2] S. Kurkovsky, E. Syta, "Digital natives and mobile phones: A survey of practices and attitudes about privacy and security", In *Proceedings of IEEE International Symposium on Technology and Society (ISTAS 2010)*, IEEE Press, pp.441-449, 7-9 June 2010 doi: 10.1109/ISTAS.2010.5514610.
- [3] "Reducing Crime: Robbery", Home Office website, available: <http://www.homeoffice.gov.uk/crime-victims/reducing-crime/robbery/> [accessed: 27 Feb. 10].
- [4] "'IFraud' Fuels Rise In Scam Phone Claims", CPP Group website, available: <http://www.cppgroupplc.com/news/press-release.shtml> [accessed: 26 Feb. 10].
- [5] "Mountains of Mobiles Left in the Back of New York Cabs", Credant website, available: <http://www.credant.com/news-a-events/press-releases/229-mountains-of-mobiles-left-in-the-back-of-new-york-cabs.html> [accessed: 26 Feb. 10].
- [6] L. Rohde, "UK Government Asks Industry to Fight Mobile Phone Theft", *Infoworld*, vol. 23, no. 5, p. 76, Jan. 2001.
- [7] "Design Out Crime: Hot Product Crime", Design Council website, available: <http://www.designcouncil.com>

- org.uk/Design-Council/Files/ Landing-pages /Design-Out-Crime/Hot-Product-crime [accessed: 02 Mar 10].
- [8] M. Prenksy, "Digital Natives", *Digital Immigrants On the Horizon*, vol. 9, no. 5, pp. 1-6, October 2001 doi: 10.1108/10748120110424816.
- [9] N. L. Clarke and S. M. Furnell, "Authentication of Users on Mobile Telephones – A Survey of Attitudes and Opinions", *Computers & Security*, vol. 24, no. 7, pp. 519-527, October 2005 doi:10.1016/j.cose.2005.08.003.
- [10] H. M. Wood, "The Use of Passwords for Controlling Access to Remote Computer Systems and Services", In *Proceedings of American Federation of Information Processing Societies: 1977 National Computer Conference (AFIPS 77)*, AFIPS Press, pp. 27-33, June 1977 doi: 10.1145/1499402.1499410.
- [11] E. Albrechtsen, "A Qualitative Study of Users' Views on Information Security", *Computers & Security*, vol. 26, no. 4, pp. 276-289, June 2007 doi:10.1016/j.cose.2006.11.004.
- [12] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", In *Proceedings of the IEEE*, IEEE Press, vol. 91, no. 12, pp. 2019-2040, December 2003 doi: 10.1109/JPROC.2003.819611.
- [13] K-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B-L. Tai, J. Cook and E. E. Schultz, "Improving Password Security and Memorability to Protect Personal and Organizational Information", In *International Journal of Human-Computer Studies*, vol. 65, no. 8, pp. 744–757, August 2007 doi: 10.1016/j.ijhcs.2007.03.007.
- [14] T. Sim, S. Zhang, R. Janakiraman and S. Kumar, "Continuous Verification Using Multimodal Biometrics", In *IEEE Transactions on Pattern Analysis and Machine Intelligence*, IEEE Press, vol. 29, no. 4, pp. 687-700, April 2007 doi:10.1109/TPAMI.2007.1010.
- [15] N. L. Clarke and S. M. Furnell, "Advanced User Authentication for Mobile Devices", *Computers & Security*, vol. 26, no. 2, pp. 109-119, March 2007 doi:10.1016/j.cose.2006.08.008.
- [16] A. Azzini, E. Damiani and S. Marrara, "Ensuring the Identity of a User in Time: A Multi-Modal Fuzzy Approach", In *Proceedings of IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSAs 2007)*, IEEE Press, pp. 94-99, 27-29 June 2007 doi:10.1109/CIMSAs.2007.4362546.
- [17] A. T. B. Jin, D. N. C. Ling and A. Goh, "Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number", *Pattern Recognition*, vol. 37, no. 11, pp. 2245-2255, November 2004 doi:10.1016/j.patcog.2004.04.011.
- [18] D-J. Kim and K-S. Hong, "Multimodal Biometric Authentication using Teeth Image and Voice in Mobile Environment", In *IEEE Transactions on Consumer Electronics*, IEEE Press, vol. 54, no. 4, pp. 1790-1797, November 2008 doi: 10.1109/TCE.2008.4711236.
- [19] R. J. Hulsebosch and P. W. G. Ebben, "Enhancing Face Recognition with Location Information", In *Proceedings of 2008 Third International Conference on Availability, Reliability and Security (ARES 08)*, IEEE Press, pp. 397-403, 4-7 March 2008 doi: 10.1109/ARES.2008.45.
- [20] N. L. Clarke and S. M. Furnell, "Authenticating Mobile Phone Users Using Keystroke Analysis", In *International Journal of Information Security*, vol. 6, no. 1, pp. 1-14, January 2007 doi:10.1007/s10207-006-0006-6.
- [21] F. Monrose and A. D. Rubin, "Keystroke Dynamics as a Biometric for Authentication", *Future Generation Computer Systems*, vol. 16, no. 4, pp. 351–359, February 2000 doi: 10.1016/S0167-739X(99)00059-X.
- [22] S. M. Furnell, N. L. Clarke and S. Karatzouni, "Beyond the PIN: Enhancing user authentication for mobile devices", *Computer Fraud & Security*, vol. 2008, no. 8, pp. 12-17, August 2008 doi:10.1016/S1361-3723(08)70127-1.
- [23] A. C. Weaver, "Biometric Authentication", *Computer*, vol. 39, no. 2, pp. 96-97, February 2006 doi: 10.1109/MC.2006.47.
- [24] S. Prabhakar, S. Pankanti and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33-42, March 2003 doi: 10.1109/MSECP.2003.1193209.
- [25] A. Ross and A. K. Jain, "Multimodal Biometrics: An Overview", In *Proceedings of 12th European Signal Processing Conference (EUSIPCO)*, EURASIP Press, pp. 1221-1224, September 2004
- [26] O. Arandjelovic, R. Hammoud and R. Cipolla, "Multi-sensory Face Biometric Fusion (for Personal Identification)", In *Proceedings of IEEE 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 06)*, IEEE Press, p. 52, 17-22 June 2006 doi: 10.1109/CVPRW.2006.136.
- [27] A. Boukerche and M. S. M. Annoni Notare, "Behavior-based Intrusion Detection in Mobile Phone Systems", *Parallel and Distributed Computing*, vol. 62, no. 9, pp. 1476-1490, September 2002 doi: 10.1006/jpdc.2002.1857.
- [28] "Objectives", BioAPI Consortium website, available: <http://www.bioapi.org/objectives.asp> [accessed: 03 Dec. 09].

## Author Biographies



**Chris Hocking** achieved a BSc (Hons) in mathematics and statistics from the University of London, Goldsmiths' College in 1986. After an eighteen year career in industry he returned to education attaining an MSc in web technologies and security from the University of Plymouth in 2007. Since this time Chris has focussed his research on the security of mobile devices and anticipates completing his PhD during 2011.

**Professor Steven Furnell** gained a BSc (Hons) in computing and informatics from the University of Plymouth, UK in 1992, followed by a PhD in information security from the same institution in 1995. His



research interests continue to focus upon security issues, including user authentication, intrusion detection, usability, and security culture. Prof. Furnell is active within three working groups of the International Federation for Information Processing (IFIP) – namely Information Security Management, Information Security Education, and Human Aspects of Information Security & Assurance. He is the author of over 210 papers in refereed international journals and conference proceedings, as well as books including *Cybercrime: Vandalizing the Information Society* (2001) and *Computer Insecurity: Risking the System* (2005). Further details can be found at [www.plymouth.ac.uk/cscan](http://www.plymouth.ac.uk/cscan).



**Dr Nathan Clarke** graduated with a BEng (Hons) degree in electronic engineering in 2001 and a PhD in 2004 from the University of Plymouth. He has remained at the institution and is now an Associate Professor in Information Security and Digital Forensics within the Centre for Security, Communications and Network Research. Dr Clarke is also an adjunct scholar at Edith Cowan University, Western Australia. His research interests include user identity, mobility and intrusion detection; having published 55 papers in international journals and conferences. Dr Clarke is a chartered engineer, a fellow of the British Computing Society

(BCS), and a UK representative in the International Federation of Information Processing (IFIP) working groups relating to the Human Aspects of Information Security & Assurance (co-vice chair), Identity Management and Information Security Education. Dr Clarke is the author of *Computer Forensics: A Pocket Guide* published by IT Governance and a forthcoming book on Transparent Authentication to be published by Springer in 2011.



**Professor Paul Reynolds** is a technical specialist in Internet based mobile telecommunications. He has a doctorate in Advance Telecommunications and is a Fellow of the Institution of Electrical Engineers. Until recently he was Head of Research for France Telecom/Orange and currently is the CTO of a software start-up company "Conetivita". Among other things he has: directed the European Union's funded research into distributed computing for mobile telecommunications; designed mobile telecommunication networks for eight countries; chaired sessions at two European Union Mobile Communication Summits; been the technical leader of the Mobile Wireless Internet Forum and of two major European Union research projects; and, been the chairman of EU's Group responsible for leadership of Europe wide next generation mobile telecommunications. Since 1993 he has authored 11 patents, and over 40 published technical papers, in the area of telecommunications.

# A preliminary investigation of distributed and cooperative user authentication

C. G. Hocking<sup>1</sup>, S. M. Furnell<sup>1,2</sup>, N. L. Clarke<sup>1,2</sup> & P. L. Reynolds<sup>1</sup>

<sup>1</sup> Centre for Security, Communications and Network Research, Plymouth University,  
Plymouth, United Kingdom  
info@cscan.org

<sup>2</sup> School of Computer and Information Science, Edith Cowan University,  
Perth, Western Australia

## Abstract

*Smartphones and other highly mobile yet sophisticated technologies are rapidly spreading through society and increasingly finding their way into pockets and handbags. As reliance upon these intensifies and familiarity grows, human nature dictates that more and more personal details and information is now to be found upon such devices. The need to secure and protect this valuable and desirable information is becoming ever more prevalent. Building upon previous work which proposed a novel approach to user authentication, an Authentication Aura, this paper investigates the latent security potential contained in surrounding devices in everyday life. An experiment has been undertaken to ascertain the technological infrastructure, devices and inert objects that surround individuals to establish if these items might be significant. The results suggest that inert possessions may offer a surprisingly large potential with some being in close proximity to experimental subjects for over 45% of the entire period. With other graphical analysis illustrating the consistency of presence, this work suggests that everyday possessions and devices can be leveraged to augment traditional approaches and even in certain circumstances, during device activation remove the need to authenticate.*

## Keywords

Authentication, identification, mobile, security, identity

## INTRODUCTION

As modern communication technology permeates ever further throughout society, the desire to remain in constant contact with colleagues, friends and family is increasingly met. The recent surge in sales of smart phones and other sophisticated mobile devices has driven a correlated explosion in Wi-Fi hotspot usage (In-stat, 2009; In-stat, 2011). Technological boundaries are stretching and the devices people carry are evolving with expanding storage capabilities and processing power, enabling the porting of greater amounts of information and personal details. As this becomes the norm for us all, these personal items become an ever-increasing target for theft (CPP, 2010; Home Office, 2009). In this climate, the requirement to protect and secure the potentially large volumes of sensitive and personal information contained within these desirable pieces of equipment is imperative and even acknowledged and supported by Government (Design Council, 2010; Rohde, 2001).

Authentication of the user's identity by any device provides the first line of defence in the battle to maintain data integrity following theft or loss. Establishing as far as possible that the operator is whom they purport to be, provides a device with the necessary degree of confidence to allow access and service utilisation. However, although steps have been taken to ensure the devices are only accessed by accredited individuals, the ubiquitous point of entry user identity code and password has been rendered susceptible to abuse through the inability or unwillingness of individuals to protect and administer this sensitive information correctly (Albrechtsen, 2007; Clarke and Furnell, 2005). In the event that several devices are carried simultaneously, the repeated intrusive accreditation process becomes laborious and inconvenient. Improving and evolving the employed authentication mechanism will go some way to counteract this burden and potentially provide an opportunity to increase the confidence in user identity.

Previous research established a proposal through which authentication credentials could be distributed amongst devices, providing a novel, flexible and adaptive security mechanism; termed an Authentication Aura (Hocking et al., 2010). In this approach disparate devices with established trust will trade user identity confidence between each other. Information relating to time since last authentication and rigour of method used is relayed via a near field communication channel. This is then coupled with details of unintelligent detected equipment and environment awareness to form a bolstered and reactive user identity confidence which is used to delay re-authentication or even postpone the login process upon a device's activation.

This paper builds upon the concept of an Authentication Aura, investigating the latent potential contained within the electronic devices and currently dumb objects that are pervasive within everyday life. Experiments have been carried out to assess the potential and quantify the contribution that could be made by a user's localised surrounding gadgets and possessions.

The following two sections briefly outline the Authentication Aura concept and then proceed to detail an experiment which has been undertaken to investigate the potential of using localised equipment to support established user identity. This is then succeeded by an analysis of the experimental findings, exploring the manner in which identity confidence could be influenced and how it could be utilised to calculate a new and reactive status. A summary of the paper's findings are then outlined in a conclusion.

## BACKGROUND

With the accepted fragility of the ubiquitous point of entry user identity and password authentication, research has been widespread in attempting to improve upon this current situation (O' Gorman, 2003; Vu et al., 2007). One tranche of work, the Authentication Aura, suggested a distributed approach in which trusted and known devices that had all performed unilateral authentication, shared information between one another to bolster confidence in their own user's identity (Hocking et al., 2010). This section briefly outlines the concept of the Aura, enabling the reader to gain an understanding for the motivation behind the current research.

As an individual authenticates with a personal device, the piece of equipment establishes a confidence in the user's identity. In most scenarios this is Boolean, the user is either whom they claim to be (they pass the authentication process) or they are not (they fail); thus the confidence is set at either complete (100%) and access is granted or it is none and the user is barred. The Authentication Aura suggests the use of confidence erosion following validated access which can in turn be utilised to reduce the availability of device functionality. High confidence will permit the use of expensive applications and access to sensitive data, whilst reduced confidence will block the use of these functions.

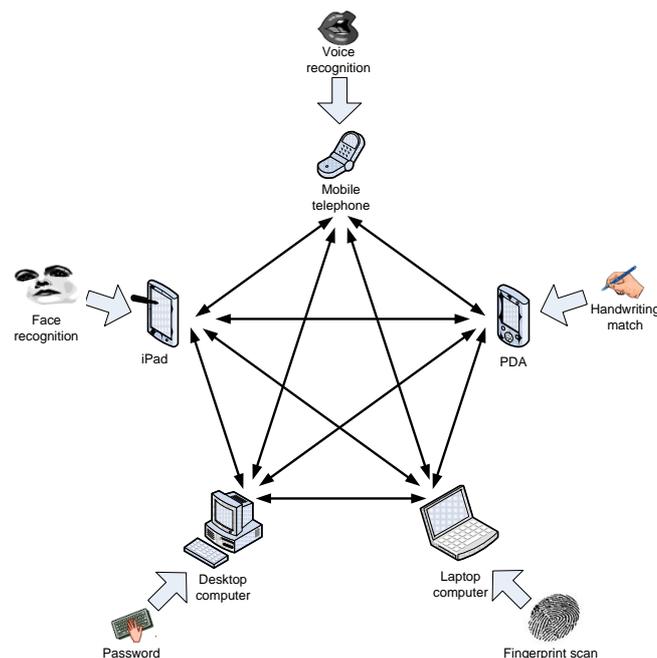


Figure 1. The potential intra-device relationship and authentication techniques (Hocking et al., 2010)

Then when confidence has eroded to a suitably low level, re-authentication of the user will be necessary to ensure continuing availability of use. To counteract this one-way-street, information pertaining to location, time since and method of authentication can be communicated between devices, providing the potential to boost the receiving equipment's confidence in its user's identity. Figure 1 shows an example of how the information might be relayed amongst a group of commonly owned devices.

For some intelligent devices it might be possible to undertake continuous authentication (such as voice recognition during telephone calls) to provide frequently reconfirmed identity details and a valuable confidence contribution, whilst others might simply act as tokens, their presence the only information of use. Figure 2 summarises this.

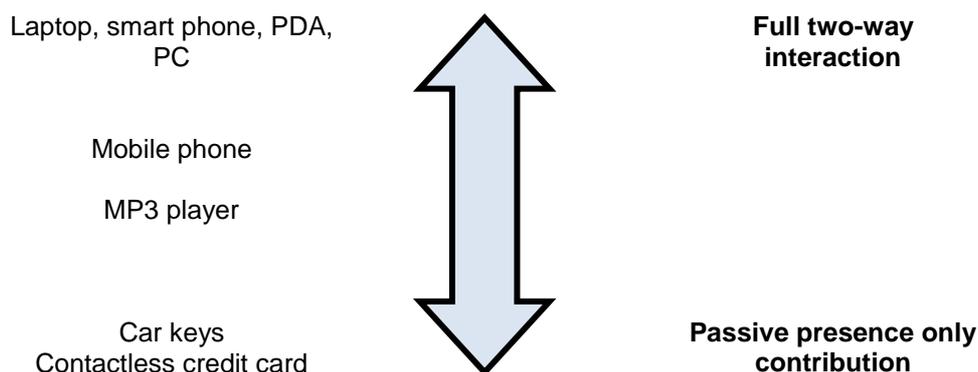


Figure 2. Varying levels of device sophistication and consequent contribution to the authentication process

If the Authentication Aura is successfully implemented, there is the potential to achieve device activation without the need for authentication. For instance, if a user with a number of present and active devices proceeds to switch on another item of equipment, there might be sufficient relayed confidence available to make the newly activated item content to permit access immediately without additional intervention. With users currently performing many authentications during a day, any savings that can be gleaned must intuitively be of benefit.

## EXPERIMENT

### Motivation and approach

The concept of an Authentication Aura relies on the intercommunication of information between intelligent devices supplemented by the detection of inert household or personal items (Hocking et al., 2010). To initially gauge the viability of this concept it is imperative that a data gathering exercise be undertaken to ascertain what devices are present within a short distance of an experimental participant at various points in time. This information can then be analysed to determine if there is a latent potential in surrounding devices that can be leveraged to augment traditional security.

It would have been relatively straightforward to execute such a task on entirely intelligent devices however the premise dictates that both dumb objects and those that might be intelligent in the future (such as household white goods), are also included. An obvious solution would be to provide experimental subjects with pen and paper to record devices and items that surround them at any given moment, over a period of days. Intuitively this is far from practical. Forgetfulness and sheer imposition renders this an inappropriate approach; an alternative means of surveying an individuals surrounding locale needed to be found.

With the requirement to include dumb and currently incapable devices, the selected method by which the appropriate information could be identified and recorded uses radio frequency identity (RFID) tags and associated sensing equipment. Each tag transmits a unique identification marker continuously across a short distance. By positioning a number of these on or near individual devices and objects of interest, it is possible for a small portable lightweight RFID reader to be constantly carried by a subject, allowing all detected tags to be recorded at discrete time intervals. This is of suitable imposition to ensure experimental volunteers were forthcoming.

### Details

To facilitate the experiment equipment was purchased to enable the recording of data simultaneously for five subjects. Although in an ideal world as many candidates as possible would undertake the experiment at any one time, the prohibitive cost of equipment restricted the sample groups to five, an affordable number that would yield a meaningful set of results. The PDA RFID readers were Dell Axim x51s, each equipped with CompactFlash RFID nodes, capable of reading both passive and active RFID tags. Passive tags transmit their identity in response to a polled request from the reader inducing their power from the received signal; active tags however contain their own independent power supply in the form of a battery. Although active tags are much more expensive to buy their main advantage is that they can be detected over a far greater range, 10-15m in clear line-of-sight, opposed to a maximum of 0.5m for the passive tags. Wi-Fi network infrastructure can provide

connections over a wide area and so with the need to emulate this, the experiment requires detection of tags across several metres and through walls; it was therefore deemed prudent to spend the extra resource and secure the active variety. As such, seventy-five active tags were purchased enabling each individual volunteer to be supplied with fifteen, permitting them to identify and record a sufficient number of devices both at home and in their workspace.

Mobile phone	Work PC	Home PC/Laptop	Work Wi-Fi point
Home Wi-Fi Point	TV (s)	Car interior	Car keys
Wallet/purse	mp3 player	Work bag/briefcase	Home telephone
Bedside clock	Fridge	Hi-Fi	Coat pocket

Table 1. Suggested locations for the RFID tags

Groups of volunteers that worked together were picked to ensure there was a degree of crossover within their daytime activity allowing each subject's recording equipment to detect other participant's tags. In a functioning Aura environment additional security could be engendered from familiar devices belonging to friends or colleagues even though they are not specifically owned by the same user. Selecting groups in this way would provide a dimension to the results data that could be analysed to assess this premise.

Each group of five subjects was instructed to undertake the experiment for fourteen days continuously, carrying the PDA with them at all times whilst ensuring that it remained charged and active. Software was written and deployed to the PDAs which recorded all detectable tag identities within range, their signal strength and time stamp, at one minute intervals. The individual's tags were placed upon or attached to items of interest representing intelligent and dumb devices, personal possessions and infrastructure. A cross-reference list of tag identities and locations was recorded, enabling the identification of relevant items during later phases.

### Initial observations

Upon removing the data files and commencing analysis some initial observations have been made. With observations occurring each and every minute, twenty four hours a day, seven days a week the data set is intuitively large. For each of the participants the experiment yields 1,440 sets of readings each day which equates to 10,080 in total across a single week.

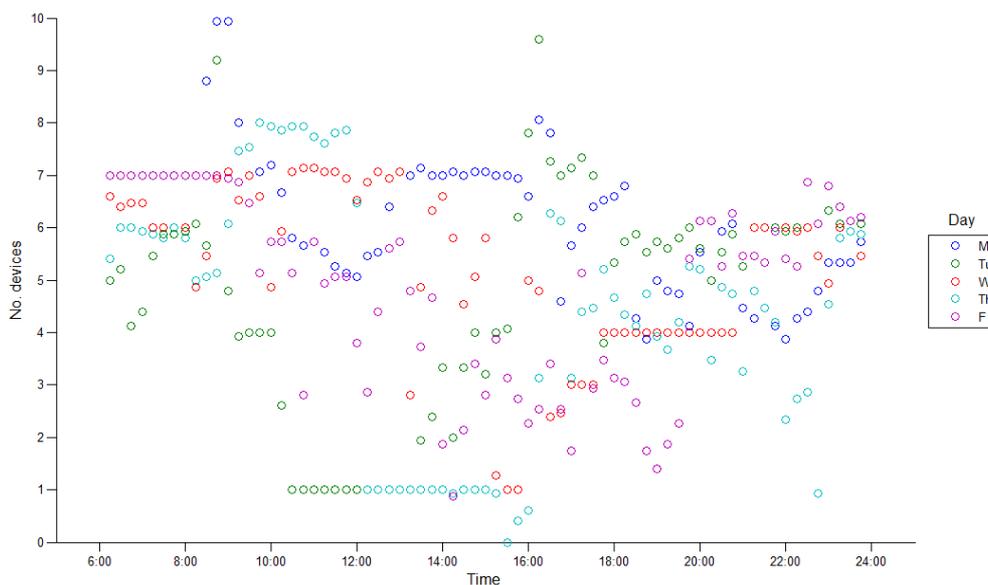


Figure 3. A typical user's weekday observations

Figure 3 illustrates the number of unique devices observed by an individual during a working week (Monday-Friday). Each day is plotted as a separate set of readings with individual data points representing the average number of detected devices within a fifteen minute period plotted against the time of day that the observation was made.

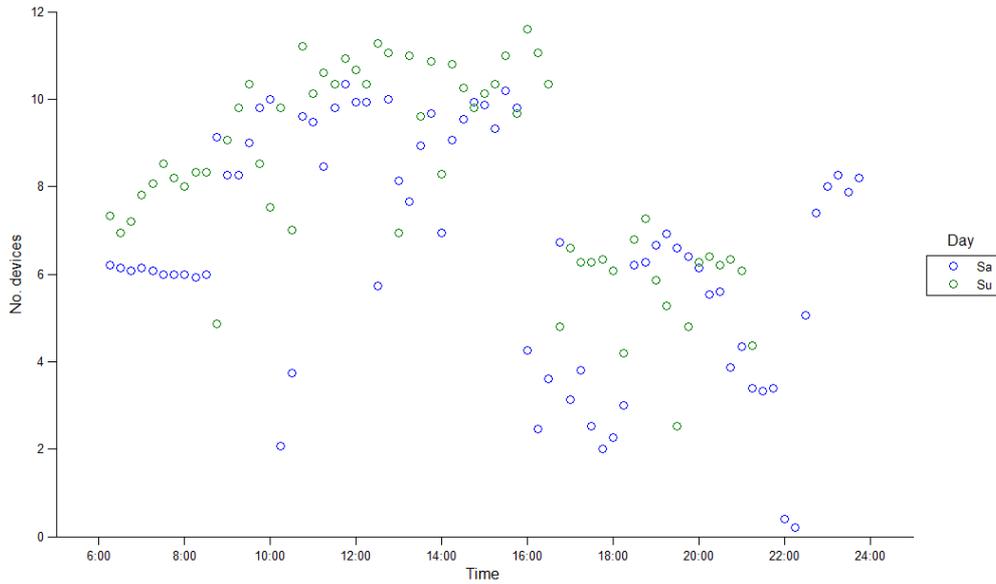


Figure 4. The same typical user's weekend observations

The weekday plot exhibits a maximum average of ten devices being detected in any given fifteen minute slot whilst at the weekend this figure peaks at twelve, suggesting that more static tags were located at home rather than at work. However, with such a high number of observations being recorded at both home and work it is apparent that the majority of tags were placed on portable possessions that the subject carried with them throughout the day.

During the workdays there appears a high degree of variation in the number of observed devices implying that this subject is active during their employment and even spends time out of the office. Time away from their usual location can be perceived from the data on Tuesday and Thursday between 10a.m. and 4p.m. where the average falls to a single unit.

With the observed variations, fluctuations and even periods of consistency it is possible to immediately conjecture that scope exists to leverage this information for use in security.

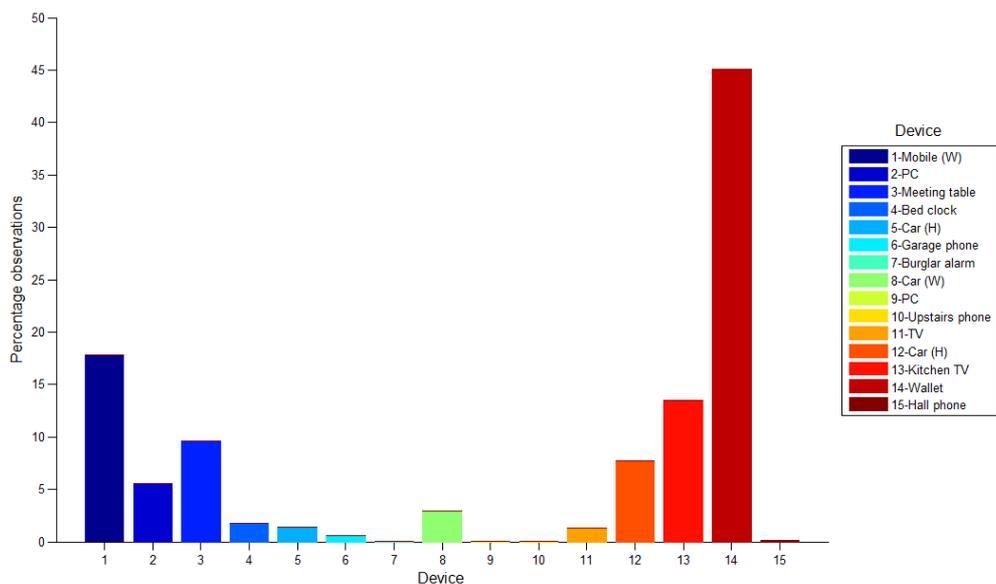


Figure 5. A single user's specific device observations

Figure 5 above illustrates a histogram that has been compiled from observations of specific devices for a user throughout the duration of their fourteen day experimental participation. It shows the percentage of observations that recorded each of their fifteen RFID tags, cross-referenced to identify the specific devices or items of equipment. Clearly from this diagram, there is one personal item that was detected far more often than any other. The subject's wallet was observed during approximately 45% of all recordings executed during the two week experiment. So do inert devices or personal items provide greater security leverage than intelligent ones? For the same user, by plotting days' observations in isolation (Figures 6 and 7) it is possible to examine more clearly how the user's routine affects the devices that are detected. These diagrams illustrate the continuity of presence for each possession or item of equipment across the day, when contact is established and when it is lost. Additionally other user's devices are also shown (Other devices) indicating when they are also detected. Intuitively, these foreign device contacts mainly appear on the weekday plot (Figure 6) because the other members of the experimental group were all work colleagues but there is a single set of blips visible at approximately 16:15 at the weekend, suggesting that the subject briefly visited their work premises.

It is interesting to note that in both examples nearly the entire observation window from 6a.m. to 12p.m. has at least one device within detection range at any given moment. Indeed, closer examination appears to suggest that the inert devices are present most consistently throughout the day, supporting the potential for security leverage.

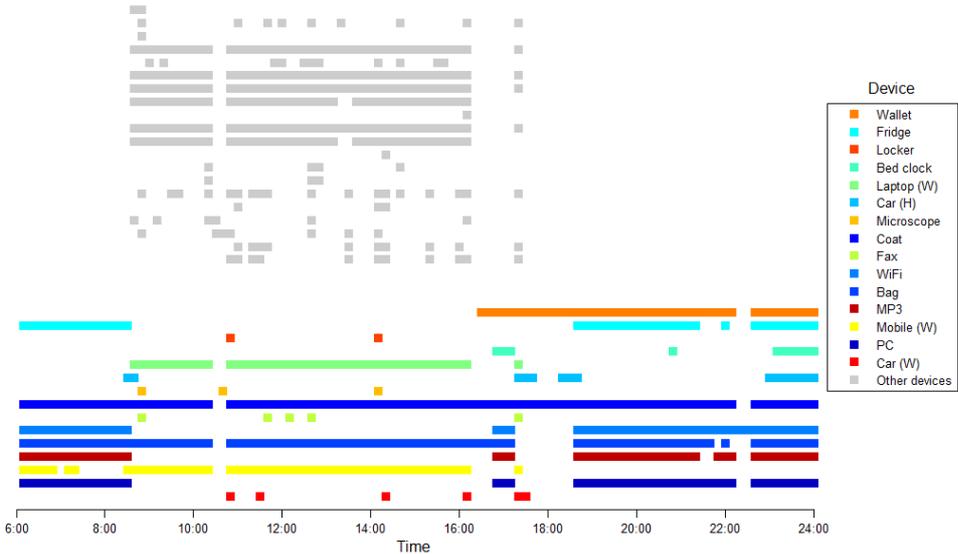


Figure 6. A user's isolated single weekday activity

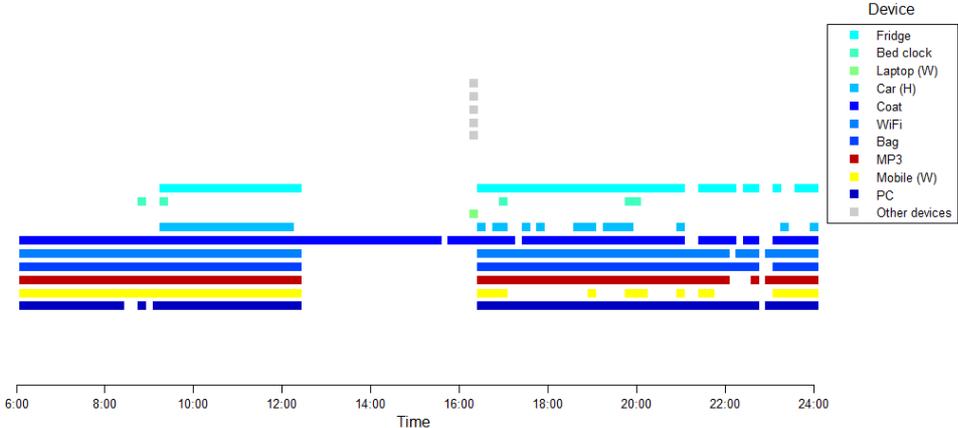


Figure 7. The same user's isolated single weekend day activity

The discussion above has concentrated upon and examined the data from just a single user. It would require a study of many subjects to ascertain if this is unequivocally true or false, a volume of data that is not currently available. However within the current sample set high percentages of experimental detection are attributed to inert personal items when they were selected by an individual; indeed coats, work bags and hand bags all topped the frequency chart for particular participants. Intuitively it cannot be stated that they provide a greater security potential but equally it is important they should be utilised where possible because of their persistence and inconspicuous presence.

## CONFIDENCE

### Confidence of identity

The concept of an Authentication Aura utilises confidence of the user's identity in two ways. When a device is activated and the initial security check (if there is one) is passed, the confidence of the device in the user's identity at that moment in time is high. The authentication has been passed and usually an implicit trust is made by the device in giving the user unrestricted access to the services and data it holds. This level of trust remains unwavering and unchallenged unless barriers such as a PIN protected screen saver/lock are implemented. Rather than continuing in this way the Aura concept erodes the user identity confidence over time; the longer it has been since an authentication was undertaken the lower the confidence will be. This degrading value will then be assessed and utilised to restrict some of the processes and applications available for use; eventually at a prescribed threshold unobtrusive re-authentication will be executed to reaffirm the user's identity. It is of course rather simplistic to simply erode the confidence and so to counteract this effect the concept incorporates communicated authentication details from other trusted devices to positively boost the devices identity confidence. Thus at a point in time the device has a confidence in the user's identity that is a combination of time since last authentication, the authentication method used and information received from surrounding devices. The Aura concept's calculation of user identity confidence is encapsulated by Equation 1.

$$C_x = \left[ F_1(t_x, m_x) + \left( \sum_{i=1}^n F_2(t_i, m_i) \right) \right] \begin{matrix} \text{max } 100 \\ \text{min } 0 \end{matrix}$$

*Equation 1. Formula for calculating a device's user identity confidence*

In the equation:

- $x$  signifies the user device on which the confidence  $C$  is being calculated.  $C$  is bounded within the range 0.0 to 100.0 inclusively.
- Function  $F_1$  calculates the amount of confidence using  $t$  the time since authentication was carried out on the given device ( $x$ ) and  $m$  the authentication method that was used.
- $n$  represents the number of devices (both intelligent and dumb) that constitute the current Authentication Aura.
- Function  $F_2$  yields the contribution to confidence that each Aura member ( $i = 1..n$ ) makes to the receiving device  $x$ . Similarly to  $F_1$  this function utilises both time since authentication ( $t$ ) and the method used ( $m$ ) in its calculation.

With confidence eroding and a re-authentication threshold in situ the influence of the surrounding Aura members will delay and even potentially postpone the need for the reaffirmation process to be undertaken. If the framework and process model are designed with an appropriate logical path, it may indeed be the case that initial activation authentication be by-passed because a suitably high level of confidence can be drawn from the surrounding trusted devices.

It is appropriate to examine the potential of the confidence contribution to establish if there is sufficient evidence to progress this concept and hone the method by which function  $F_2$  might be invoked.

### Contribution from Aura members

It is vital to establish or at least explore how the function ( $F_2$  in Equation 1) might be conceived and operate. Previous work has indicated that inherited confidence should be influenced by and adapt to location, the types of devices active within the Aura and the authentication methods they use (Hocking et al., 2010); these should thus

be incorporated into the implemented function. To achieve this it is necessary to quantify scales of numeric values that can be implemented and then assessed to gauge performance.

As an initial first step, location can be allocated a simple tri-value range, home, work or other; equated to 3, 2 or 1 respectively. Apportioning values in this way will enable a variation in confidence contribution to be accomplished. It is reasonable to argue that whilst at home devices should operate with less heightened security and be more relaxed about the way in which they are being used. Similarly at work, although assured the operating environment is less safe than within the owner’s home. Finally being away from both home and work is the time when a device should be most wary and inherit least confidence from surrounding pieces of equipment. Initially for assessment purposes this three point scale can be used as a simple multiplier resulting in inherited confidence at home being 50% more significant than that received from the same devices at work and three times more whilst in other unrecognised locations.

In addition to location, it is imperative that the significance of the device is somehow incorporated into the contribution formula. As highlighted earlier in this paper some devices are more often detectable and less visible, a combination which arguably makes them of greater significance. With this being a mathematical calculation it seems sensible to allocate a ranking value (in the range 1..10) to each item of equipment owned by a user and use this within the formula, this will be referred to as the device’s rank. It is proposed that a rank of 1 should indicate the most significant pieces of equipment whilst 10 the least. This value can then be used as a divisor to reduce the relative contribution of each device.

To establish the latent potential of drawing confidence from surrounding devices it is initially advantageous to keep the function as simple as possible. Therefore, although Equation 1 indicated that the specific confidence of any communicating device would be used currently a rigid maximum value will be set for each. To initiate investigation this will be fixed at 15%. In a fully operational model this would be allocated on a device by device basis and then reduced by the time that has elapsed since authentication and the method used.

Thus the initial formula for  $F_2$  and the contribution made by device  $i$  becomes:-

$$c_i = \left(\frac{15}{r_i}\right) \times l$$

*Equation 2. Formula for F2 to test the potential of confidence contribution made by each device*

Where ...

- $i$  signifies the contributing device.
- $r$  is the significance rank of device  $i$  (in the range 1..10).
- $l$  is the location multiplier (in the range 1..3).

Thus a device whose presence is regarded as being most significant (i.e. has a rank of 1) that is detected whilst the user is at home (location multiplier equal to 3) contributes 45% to the confidence of the host device. However, in the same location a device of medium significance (rank 5) would only contribute 9% and one of least significance (rank 10) just 4.5%.

To aid in the clarity of this brief investigation a single day’s data for one user will be isolated and plotted so a subjective appraisal can be made.

Equipment	Rank	Equipment	Rank	Equipment	Rank
Wallet	2	Car (Home)	3	Bag	4
Fridge	4	Microscope	5	MP3	6
Locker	6	Coat	4	PC	6
Bed clock	4	Fax	9	Car (Work)	5
Laptop (Work)	8	WiFi (Home)	5	Mobile (Work)	5

*Table 2. Table of selected equipment and allocated rankings*

The user chose to tag the fifteen items of equipment shown in the table above, enabling them to be detected during the experiment. The table also indicates the allocated ranking to each device:



## REFERENCES

- Albrechtsen, E. (2007) 'A Qualitative Study of Users' View on Information Security', *Computers and Security*, vol. 26, no. 4, pp. 276-289
- Clarke, N. L. and Furnell, S. M. (2005), 'Authentication of users on mobile telephones – a survey of attitudes and opinions', *Computers & Security*, vol. 24, no. 7, pp. 519-527
- CPP (2010), "'IFraud" Fuels Rise In Scam Phone Claims', *CPP Group*, available: <http://www.cppgroupplc.com/news/press-release.shtml>  
[accessed: 26 Feb 10]
- Design Council (2010), 'Design Out Crime: Hot Product Crime', *Design Council*, available: <http://www.designcouncil.org.uk/Design-Council/Files/Landing-pages/Design-Out-Crime/Hot-Product-crime/>  
[accessed: 02 Mar 10]
- Hocking C.G., Furnell S.M., Clarke N.L. and Reynolds P.L. (2010), 'A distributed and cooperative user authentication framework', *6th International Conference on Information Assurance and Security (IAS 2010)*, Atlanta, USA, 23-25 August 2010, pp. 304-310
- Home Office (2009), 'Reducing Crime: Robbery', *Home Office website*, available: <http://www.homeoffice.gov.uk/crime-victims/reducing-crime/robbery/>  
[accessed: 27 Feb 10]
- In-stat (2009), 'Hotspot Usage is Increasingly Shifting Away From Notebooks and Laptops and Toward Handhelds', *In-stat*, available: <http://www.instat.com/newmk.asp?ID=2695&SourceID=00000352000000000000>  
[accessed: 18 Jan 09]
- In-stat (2011), 'Hotspot Usage to Reach 120 Billion Connects by 2015', *In-stat*, available: <http://www.instat.com/press.asp?ID=3246&sku=IN1105002WS>  
[accessed: 15 Sep 11]
- O'Gorman, L. (2003) 'Comparing Passwords, Tokens, and Biometrics for User Authentication', *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2019-2040
- Rohde, L. (2001) 'UK Government Asks Industry to Fight Mobile Phone Theft', *Infoworld*, vol. 23, no. 5, p. 76
- Vu, K-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B-L., Cook, J. and Schultz, E. E. (2007), 'Improving password security and memorability to protect personal and organizational information', *International Journal of Human-Computer Studies*, vol. 65, no. 8, pp. 744–757

Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

journal homepage: [www.elsevier.com/locate/cose](http://www.elsevier.com/locate/cose)Computers  
&  
Security

# Co-operative user identity verification using an Authentication Aura



CrossMark

C.G. Hocking<sup>a,1</sup>, S.M. Furnell<sup>a,b,\*,1</sup>, N.L. Clarke<sup>a,b,1</sup>, P.L. Reynolds<sup>a,1</sup><sup>a</sup>Centre for Security, Communications and Network Research, Plymouth University, Plymouth PL4 8AA, UK<sup>b</sup>Security Research Institute, Edith Cowan University, Perth, Western Australia, Australia

## ARTICLE INFO

### Article history:

Received 20 May 2013

Received in revised form

30 August 2013

Accepted 2 September 2013

### Keywords:

Authentication

Identification

Mobile

Security

Identity

Authentication Aura

## ABSTRACT

IT usage today is typified by users that operate across multiple devices, including traditional desktop PCs, laptops, tablets and smartphones. As a consequence, users can regularly find themselves having a variety of devices open concurrently, and with even the most basic security in place, there is a resultant need to repeatedly authenticate, which can potentially represent a source of hindrance and frustration for the user. Building upon previous work by the authors that proposed a novel approach to user authentication, called an Authentication Aura, this paper investigates the latent security potential contained in surrounding devices in everyday life and how this may be used to augment security. An experiment has been undertaken to ascertain the technological infrastructure, devices and inert objects that surround individuals throughout the day to establish whether or not these items might be utilised within an authentication solution. The experiment involved twenty volunteers, over a 14-day period, and resulted in a dataset of 1.23 million recorded observations. Using the data provided by the experiment as a basis for a simulation, it investigated how confidence in the user's identity is influenced by these familiar everyday possessions and how their own authentication status can be 'leveraged' to negate the need to repeatedly manually authenticate. The simulation suggests a potential reduction of 74.04% in the daily number of required authentications for a user operating a device once every 30 min, with a 10-min screen lock in place. Ultimately, it confirms that during device activation it is possible to remove the need to authenticate with the Authentication Aura providing sufficient confidence.

© 2013 Elsevier Ltd. All rights reserved.

## 1. Introduction

Authentication of the user's identity by any device provides the first line of defence in maintaining data confidentiality following theft or loss. Establishing, as far as possible, that the user is whom they claim to be provides a device with the accepted degree of confidence to allow access and service utilisation. However, although steps have been taken to

ensure the devices are only accessed by authorised individuals, the usual point of entry username and password has been rendered susceptible to abuse through the inability or unwillingness of individuals to protect and administer this sensitive information correctly (Dobyns, 2012; Albrechtsen, 2007; Clarke and Furnell, 2005). With the accepted fragility of this ubiquitous point of entry authentication, research has been widespread in attempting to improve upon this current

\* Corresponding author. Tel.: +44 1752586234.

E-mail address: [sfurnell@plymouth.ac.uk](mailto:sfurnell@plymouth.ac.uk) (S.M. Furnell).

<sup>1</sup> [info@cscan.org](mailto:info@cscan.org)

situation (Jansen, 2003; O’Gorman, 2003; Furnell et al., 2008; Vu et al., 2007). However, in the event where several devices are carried simultaneously, there will always be a degree of repeated intrusive authentication, a process that can become laborious and inconvenient; an issue that is of particular note when one considers the general complacency of users around security issues on mobile devices (Mylonas et al., 2013), which could render it easily abandoned if it is perceived as too burdensome. If a user has previously authenticated upon a device then it may be feasible to use the confidence arising from this to provide automated access to other devices within a close proximity to the device on which they have just authenticated. Alternatively, authentication judgements made across several devices could also be used to deliver a collective confidence level – increasing the level of identity confidence that any one unilateral device could obtain.

The aim of this paper is to further investigate the potential of such a distributed and co-operative approach to device security. First, a summary of this novel approach is presented, establishing the premise and discussing the types of devices and personal items that might be incorporated. The investigation then proceeds to explain a series of experiments that have been undertaken to assess the practical feasibility, based upon the presence of devices and infrastructure surrounding them throughout the day, examining the observed results. Following this a simulation has been performed based upon the gathered experimental data, the results have been plotted, revealing supportive evidence for the proposed approach. The paper concludes with a discussion of the results and observes how theft of a device operating with this security might perform whilst in an impostor’s possession.

---

## 2. A distributed approach

In current systems, each authentication measurement is treated as discrete and independent, and users may have to remember a variety of information and/or carry a variety of physical tokens with them, in order to achieve authentication in the different contexts (Tanvi et al., 2011). When considered from a holistic perspective, this can be seen to be inconvenient, and potentially over-complex. For example, if a user has just submitted to a biometric authentication on their desktop PC, is there then any real benefit to be gained from the same user then authenticating to a mobile phone via a weaker, PIN-based method? Given that the two devices can be in communication with each other anyway (e.g. via wireless networking), there is clear potential to remove the need for the user to authenticate to each one.

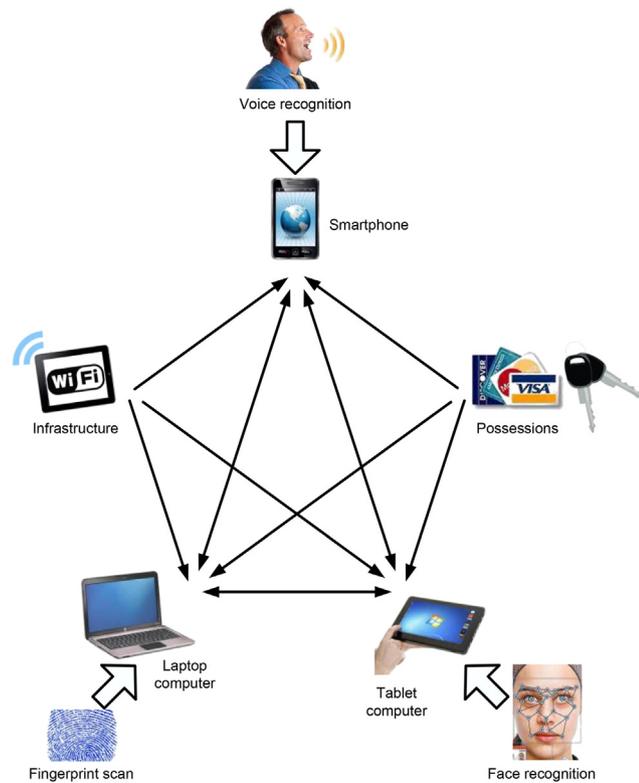
The Authentication Aura proposes a distributed approach that can improve the situation by bringing together a range of authentication methods (e.g. based upon secret knowledge, physical tokens, and biometrics) within a flexible framework that can operate across multiple devices and services within a user’s Personal Area Network (Hocking et al., 2010, 2011). The intention is not to simply achieve a single sign-on, whereby authentication to one device automatically authenticates the user to all others for an unlimited period. Instead, by intelligently combining authentication measures from the different devices and techniques used within this network, the concept

of an ‘Authentication Aura’ can be established. When access to a new device or service is requested, the strength of the user’s Aura will determine whether they will be granted access automatically, or be required to perform an explicit authentication. This strength will vary depending upon when the user last performed an authentication, and with which technique it was achieved (e.g. a measure obtained from a physiological biometric could well be weighted higher than that from a password) (Hocking et al., 2010, 2011; AuthenticationWorld, 2006; Clarke and Furnell, 2007). This distributed and collaborative environment seeks to improve the level of authentication security and improve the convenience for users.

On the majority of personal devices, as an individual authenticates, the piece of equipment establishes a confidence in the user’s identity. In most scenarios this is Boolean, in that the user is either believed to be whom they claim to be (they pass the authentication process) or they are not (they fail). As a consequence, the confidence is either set at total (100%) and universal application access granted, or it is none and the user is barred. The Authentication Aura uses a continuous identity confidence measure following validated access which can in turn be utilised to control the availability of device functionality. High confidence will permit the use of expensive applications and access to sensitive data, whilst reduced confidence can be used as a cue to block the use of these functions (Clarke, 2011). Then when confidence erodes to a suitably low level, or a high-level action is attempted with insufficient confidence, re-authentication of the user will be necessary to ensure continuing availability of use (Furnell et al., 2008; Hocking et al., 2010, 2011; Clarke and Furnell, 2007).

Information relating to location, time since and method of authentication can be communicated between trusted devices (which, in a full implementation, could utilise encrypted communications between devices based upon a prior pairing process). The Authentication Aura utilises each set of details, and the presence of other detected possessions, to calculate a positive confidence contribution. With a suitably strong ‘Aura’ users should be able to achieve device access without the need for an explicit/intrusive authentication. For instance, if a user with a number of present and active devices then switches to another item of equipment, there ought to be sufficient confidence available to enable the newly activated item to grant access immediately without additional intervention. With users currently performing many authentications per day, the savings that can be achieved will greatly reduce the overhead and potential inconvenience they experience.

The Aura utilises both intelligent and dumb devices. Intelligent devices are those that have computational capabilities and are able to interact with the user and one another, whilst dumb possessions are those that do not currently possess this ability. For some intelligent devices it might be possible to undertake continuous authentication (such as voice recognition during telephone calls) to provide frequently reconfirmed identity details and a valuable confidence contribution, whilst others might simply act as tokens, their physical presence at a location being the only information of use. Fig. 1 illustrates how the information might then be relayed amongst a group of commonly owned devices and where relevant, some of the authentication techniques that



**Fig. 1 – The potential intra-device relationship and authentication techniques.**

could be employed. Note that the three intelligent devices receive and provide information (signified by the arrows with two-way information flows), whereas the possessions and infrastructure act as providers only (signified by one-way flows). As such, the possessions and infrastructure elements do not have any reciprocal activity with other devices, whereas intelligent devices are able to perform mutual verifications.

With devices, technical infrastructure, possessions and other factors playing such a pivotal role in the Authentication Aura's approach, a key step towards evaluating the viability is to assess the degree to which such information would actually be available to be leveraged during normal day-to-day usage. As such, experiments have been carried out to assess the amount of time individuals spend within detectable range of these contributing items.

### 3. Experiment

The concept of an Authentication Aura relies upon the intercommunication of information between intelligent devices, supplemented by the detection of dumb items within the user's surrounding environment. However, to date there is no evidence to suggest the interactions exist in such a volume as to be useful. This section details the motivation, methodology, and results of an experiment that has sought to support this theory and assess the potential contribution to be made by incorporating these factors into the authentication process.

#### 3.1. Motivation and approach

The purpose of the experiment is two-fold:

- To initially gauge the viability of this concept through the identification of whether sufficient interactions (i.e. devices coming into close proximity with each other) exist to be useful within the Aura.
- To subsequently use the dataset to model the Aura framework and evaluate the security and usability attributes.

Unfortunately, no datasets currently exist that provide information regarding the interaction of technologies in close proximity. Furthermore, as the devices (both intelligent and dumb) would not necessarily currently have the required functionality, a simulated environment was constructed by placing RFID tags on/in physical equipment such as mobile phones, laptops, cars, houses and wallets. It is considered that the use of such tags could also be representative of a future deployment scenario, with more objects likely to have RFID tags within them by default (Sakr, 2011; RSA Laboratories, 2012). As an aside here, it is recognised that RFID tags have known security issues and in a full implementation of the Authentication Aura approach the intelligent devices would utilise more active communication approaches (e.g. Wi-Fi, Bluetooth), which could in turn be encrypted. Dumb devices/objects might still be detected via RFID tags, but their influence on the authentication decision process is relatively small, and would only really work as a supplement to the strength acquired from the presence and interaction with intelligent devices.

#### 3.2. Methodology

The experiment involved twenty participants, grouped into 4 groups of 5, with each group collecting interaction data for a 14-day period. Each participant was given 15 RFID tags (battery-powered rather than passive, in order to increase the detection range), which they were then asked to place upon items within their home and work environments. Whilst it would be preferable to have had a larger population sample, the nature of the tasks involved (i.e. placing tags on items and ensuring the PDA RFID reader remains charged and in their possession) and the prolonged period (14 days) of data capture placed a practical limit upon this. It was felt that having a smaller population with data collected over a longer period of time would be more beneficial to the experimental hypothesis than merely collecting data for a few days.

Volunteers were grouped based upon whether they had pre-existing relationships (i.e. that they worked together). This enabled a degree of crossover within their daytime activity allowing each subject's recording equipment to detect other participants' tags. In a fully operational Aura environment additional confidence could be derived from the presence of familiar devices belonging to friends or colleagues even though the same user does not specifically own them. As such selecting groups in this way would provide an additional dimension to the results data that could be analysed to assess this theory.

Software was written and deployed to the PDAs that recorded all detectable tag identities within range, their signal strength and time stamp, at 1 min intervals. The individual's tags were placed upon or attached to items of interest representing intelligent and dumb devices, personal possessions and infrastructure. A cross-reference list of tag identities and locations was recorded, enabling the identification of relevant items during later analysis. The items that were specifically given to experiment participants as suggested locations for the placement of tags were as follows:

- |                    |                      |
|--------------------|----------------------|
| • Mobile phone     | • Wallet/purse       |
| • Work PC          | • MP3 player         |
| • Home PC/Laptop   | • Work bag/briefcase |
| • Work Wi-Fi point | • Home telephone     |
| • Home Wi-Fi Point | • Bedside clock      |
| • TV (s)           | • Fridge             |
| • Car interior     | • Hi-Fi              |
| • Car keys         |                      |

### 3.3. Results

With observations continuously recorded from the PDAs during the collection period the experiment yielded 1440 sets of readings each day. With each reading potentially capturing multiple tags, this resulted in a dataset with 1.23 million samples within the population. Overall, during the hours of 6am–12pm, all participants were close to devices that would contribute positively towards their Aura confidence on average 97% of the time. With tags being split between work and home, movement between these locations is easily identifiable, as well as periods away from

either. This is an extremely encouraging proportion that clearly demonstrates that technologies do and can interact on a regular basis.

In order to further investigate the nature of these interactions, an analysis of individual participant interactions would be useful. However, given the scope of the paper, it is not possible to do this for each and every participant, so an analysis of a random participant is presented below as an illustration.

The histogram in Fig. 2 illustrates the observations of specific devices for a user throughout the duration of their 14-day experimental participation. It shows the percentage of time (between 6am and 12pm) for the entire 14 days, that the user spent in the presence of each of their selected items of equipment. From this diagram, one can see that there is one personal item that was detected far more often than any other. The subject's wallet was observed during approximately 45% of all recordings executed during the two week experiment. So with inert devices or personal items being discretely carried for large proportions of the day and throughout differing locations they have the potential to provide significant security leverage and possibly more than intelligent ones which are often overtly visible. One point of caution here, however, might be that some items become naturally paired for a large proportion of the time (e.g. as a result of being carried together in a bag), and thus it would be important to guard against a false assurance being gained from this. For example, if a wallet/purse and phone were routinely carried together in a bag, and the bag were to be stolen, then the phone is no longer in the possession of the owner, yet still close to the wallet/purse for a false sense of security to arise. As such, it would be appropriate for the system to learn about items that are always (or almost always) in close proximity to each other, and thus come to regard them as a single/aggregated object for Aura purposes.

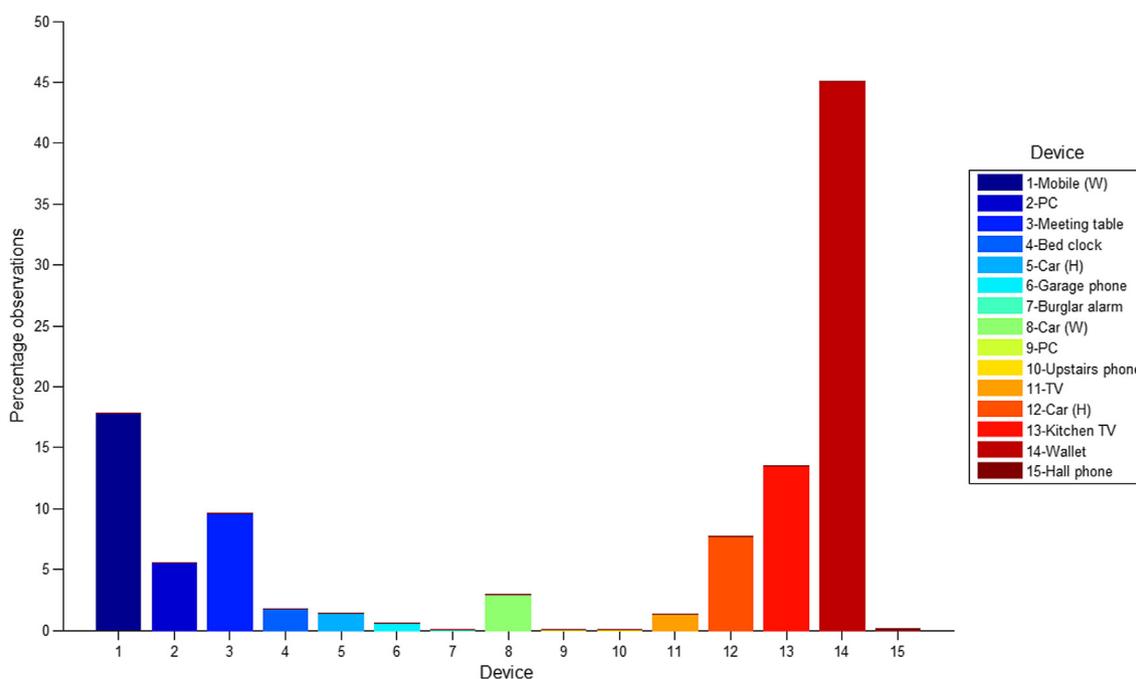


Fig. 2 – A randomly selected user's specific device observations.

By plotting daily observations in isolation (Figs. 3 and 4) it is possible to examine more clearly how the same user's routine affects the devices that are detected. These diagrams illustrate the continuity of presence for each possession or item of equipment across the day, when contact is established and when it is lost. Additionally, devices belonging to other users (Other devices) and infrastructure are also shown indicating when they are detected. These foreign device contacts only appear on the weekday plot (Fig. 3) because the other members of the experimental group were all work colleagues. Although specifics of movement are unknown, the data provides an indication of what action the participant has taken. For instance, it appears that the user left work shortly after 5pm and returned home, and in the evening between 6pm and 8pm the subject was travelling in their car having left their wallet behind. Although statements of this kind can correctly raise concerns of privacy issues (Dritsas et al., 2006), it is important to clarify that the Aura approach will not be attempting to use data in this manner, and a full implementation would have to take steps to ensure third parties were also prevented from doing so. It is interesting to note that, in both examples, nearly the entire observation window from 6am to 12pm has at least one device within detection range at any given moment. Indeed, analysis of the entire dataset reveals that, when all twenty subjects are considered as a whole, only 7254 of the 237,473 observations (i.e. 3.06% of all polled detections) failed to identify one or more devices. It can also be observed that some items serve to mirror each other's detection (because of being situated in close proximity). For instance, in Fig. 4 one of the subject's cars must have been parked at home in the garage during the recorded day as the sporadic detection pattern for this is virtually identical to their garage phone.

Closer examination of the dataset appears to suggest that inert devices are detected most consistently throughout the day, supporting their proposed potential for inclusion in the approach. Indeed coats, work bags and hand bags all topped the frequency chart for particular participants. However, when the frequency profile of the 1.23 million recorded observations is compared with the proportions of tagged device type it is virtually identical in distribution as shown in Table 1. The only differences being a 2% increase in the proportion of intelligent devices detected and a corresponding 2% reduction in the detection of dumb devices. This certainly demonstrates the clear potential for both categories of device to make a contribution to the Aura, based upon the frequency with which users are likely to encounter them.

#### 4. AURA confidence

Central to the Aura approach to security is the computation of confidence in the identity of the user interacting with a device at a given point in time. This section consequently explores the calculation of identity confidence and how it can be used to influence service availability on Aura empowered devices.

##### 4.1. Confidence of identity

The Authentication Aura utilises confidence in the user's identity differently to the Boolean manner in which traditional authentication employs it. Currently, when a device is activated and the initial security check (if there is one) is passed, the confidence (of the device) in the user's identity at that moment in time is absolute, irrespective of the authentication technique that has been invoked. The authentication has been passed and usually an implicit trust is made by the

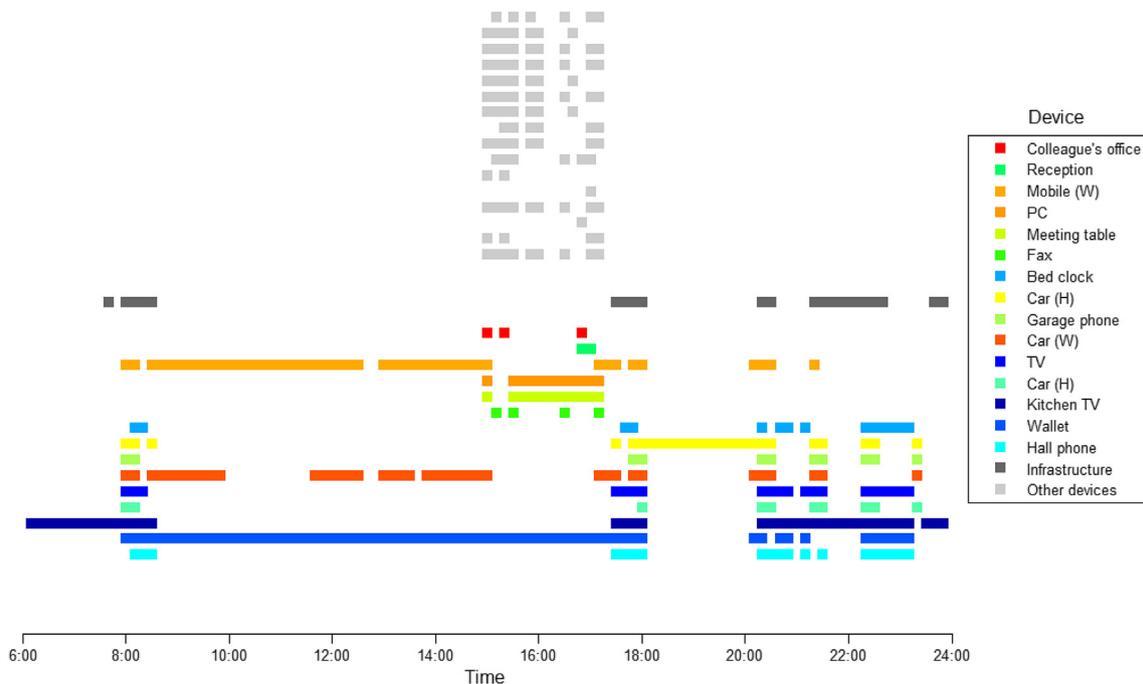


Fig. 3 – A user's isolated single weekday activity.

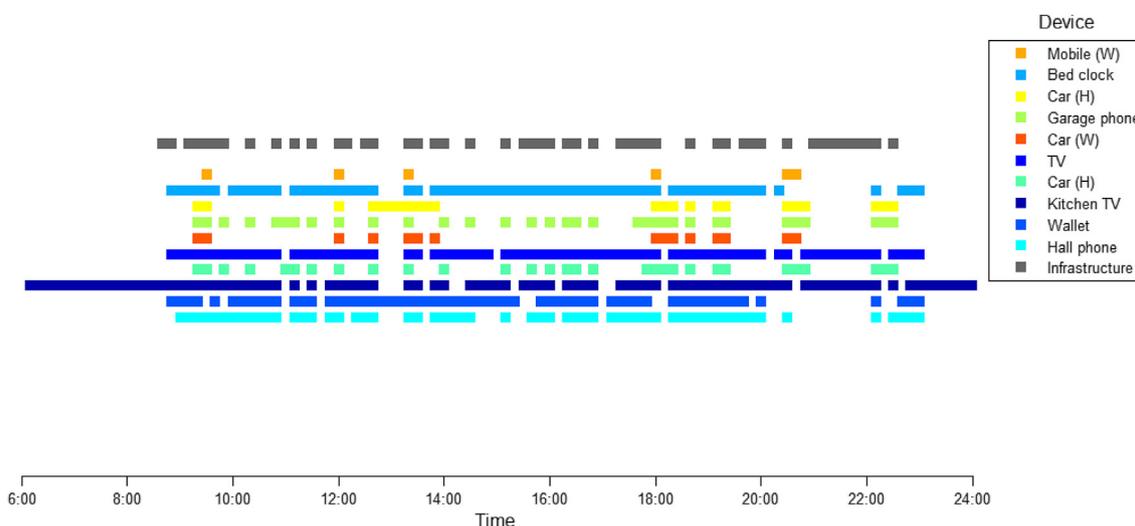


Fig. 4 – The same user’s isolated single weekend day activity.

device in giving the user unrestricted access to the services and data it holds. This level of trust remains unwavering and unchallenged unless barriers such as a PIN or password protected screen saver/lock are implemented.

Initial assessment of confidence in the user’s identity is established by the Aura in one of two ways. Upon activation of a piece of intelligent equipment, the surrounding locale is polled for trusted and recognised devices to establish a confidence level. If recent and high-level authentication has been performed on one or more nearby devices, the inherited confidence can be established and may well be sufficient to postpone intrusive authentication. If the contribution from the Aura devices is insufficient to achieve this state, the second method is invoked and explicit authentication is required from the user to directly establish the confidence in their identity. Upon completion of either of these processes and with the confidence level set, the device will proceed to operate within the Aura framework.

A notable difference to the traditional approach to authentication is that the Aura continuously monitors the confidence in the user identity, basing its calculation upon the authentication method used, the user’s location and the elapsed time since the last authentication. Whilst at home and in a trusted location the threat to a device is deemed less than if it is in a foreign and unfamiliar environment, and the longer the time since authentication, the lower the confidence. To counteract the effect of these factors, the Aura incorporates communicated authentication details from other trusted devices to positively boost the device’s identity confidence and stave-off the point at which the user is asked for unnecessary re-authentication. This value will then be assessed and utilised to restrict some of the processes and

applications available for use. Research has already been undertaken to establish how threats to mobile devices should be assessed and restriction of application usage determined based upon a sliding scale of confidence (Ledermuller and Clarke, 2011). If and when a prescribed threshold is reached, re-authentication will be executed to reaffirm the user’s identity; non-intrusively where possible. To reflect the different types of authentication being employed it is important to incorporate consideration of their strength and robustness within the Aura framework. This is achieved by associating a maximum level of contribution with each type of authentication method. For instance an iris scan (extremely robust) would be allocated a high-level tariff (e.g. 5 out of 5) and an associated 100% maximum Aura confidence, whereas PIN-based authentication might attract a tariff of 1 and maximum confidence of 60%. Thus, at any point in time, the device has an *Aura Confidence* in the user’s identity that is a combination of time since last authentication, the authentication method used, the current location, and information received from surrounding intelligent and dumb devices. One approach to the Aura’s calculation of user identity confidence is presented in Equation (1), reflecting the elements outlined above. Each of the three functions will be explained fully in the succeeding section.

Equation (1): Formula for calculating a device’s user identity confidence

$$AC_x = \left[ F_1(t_x, m_x, l) + \left( \sum_{i=1}^n F_2(t_i, m_i) \right) + \left[ \left( \sum_{j=1}^d F_3(r_j) \right) \right]_{\min 0}^{\max a} \right]_{\min 0}^{\max 100} \tag{1}$$

In the equation: x signifies the user device on which the Aura Confidence AC is being calculated. AC is bounded within the range 0.0–100.0 inclusively. Function  $F_1$  calculates the amount of core confidence using t the time since authentication was carried out on the given device (x), m the authentication method that was used and the location l of the user (home, work or away), n represents the number of intelligent devices and d the number of dumb that constitute the current

Table 1 – Comparison of proportions of tagged items and recorded observations.

	Infrastructure (%)	Intelligent (%)	Dumb (%)
Tagged items	5	19	76
Observations	5	21	74

Authentication Aura. Function  $F_2$  yields the contribution to confidence that each intelligent Aura member ( $i = 1 \dots n$ ) makes to the receiving device  $x$ . This function utilises time since authentication ( $t$ ) on the contributing and the method used ( $m$ ).

The confidence contribution assessment of dumb and inert items to the receiving device  $x$  is calculated by function  $F_3$ . Each of these Aura members' ( $j = 1 \dots d$ ) addition is simply based upon their rank ( $r$ ), a numeric indicator used to represent their significance. The total dumb device contribution is bounded at an upper limit  $a$  to block excessive influence being gained from this element of the Aura.

#### 4.2. Core confidence $F_1$

The calculation of the core confidence incorporates the erosion of certainty in the user's identity since the last authentication was made on the host device  $x$ , the centre of the Aura. Currently, the proposed function to calculate this at each time interval is

Equation (2): Core confidence calculation

$$\text{Intelligent contribution} = \left( \frac{\text{Contribution portion} \times \text{Authentication method}}{\text{Time since authentication}} \right) \quad (3)$$

$$\begin{aligned} \text{Core confidence} &= \text{Last core confidence} \\ &- (\text{Period degradation} \times \text{Location multiplier}) \end{aligned} \quad (2)$$

The *Last core confidence* is initially derived from a local authentication, if present. Its value and subsequent weight being dependent upon the authentication technique utilised. The *period degradation* value will control how rapidly confidence is eroded. If confidence is eroded every minute then this value is likely to be a fraction of a percentage point but can be altered during analysis to investigate how this affects the operation of the Aura.

This is further influenced by the *location multiplier*, a tri-value argument that is set dependent upon the device's current location, home, work or away. The premise for this approach being certain locations can derive a higher level of trust than others. Subsequent analysis will need to specifically determine appropriate values for these but it should be noted that home is where the device is likely to be safest (a low value), work is next and then away is the environment in which the device is at greatest risk (high). The location is detected via the presence of known static possessions and infrastructure.

An iterative approach is used to maintain the history of location; that is, when a user moves between location if the equation calculated its confidence just based upon the current locale an enormous drop in this value would be experienced when moving from home to away, or a falsely large increase witnessed when travelling in the opposite direction. However, it should be noted that the calculation of *core confidence* is unbounded and can become negative, eventually overriding any contribution from other devices.

#### 4.3. Contribution from intelligent Aura members $F_2$

As outlined earlier, the contribution made by each intelligent device is a function based upon the method of authentication last performed on that device and the time since the authentication was made. It is important to note that the contribution of such devices cannot be based upon their current overall confidence because they are members of the Aura, and as such will be calculating their own value inclusive of a contribution from the host device. If this were done, a ping-pong effect would be created as values were traded back and forth, falsely elevating the confidence of each participating device. Each intelligent device is allocated a percentage proportion upon which its contribution is calculated, introducing a degree of flexibility and customisation. Of course, in the simplest form all devices can be treated equally but by incorporating this approach it allows for future device dependent enhancement. Thus function  $F_2$  is proposed as follows:

Equation (3): Intelligent device contribution

For the sake of discussion, *contribution portion* might be set to a value of 20% and *authentication method* in the range 1–5. An *authentication method* of value 5 would indicate an extremely secure and robust (resistant to circumvention) method of authentication and 1 the least secure method possible. *Time since authentication* is not a strict time such as the number of seconds or minutes but a degradation multiplier based upon the time. For example, this argument might be the number of 10-min intervals since authentication. Thus for an *authentication method* of 3 (an averagely secure method) that was performed 1 h 30 min ago (9 10-min periods) and providing the device has been continuously present in communicable range, the confidence contribution would be  $((20 \times 3) / 9) = 6.66\%$ . Adjusting the value of the *contribution portion* will of course correspondingly alter the amount of contribution made by each intelligent device.

#### 4.4. Contribution from dumb Aura members $F_3$

Dumb pieces of equipment that are unable to authenticate or communicate with other members of the Aura will simply act as tokens and contribute by their presence. The amount by which they contribute is simply dependent upon their rank, an allocated value between 1 and 10, the lower the rank the greater the security significance of the item. For example, in the earlier histogram (Fig. 2) because the subject's wallet is so often detected, yet hidden, it is conceivable that this item would be allocated a rank of 1 or 2, whilst the meeting table is far less personal and would therefore be ranked at a much higher level, perhaps 9. At this time it is anticipated that the equation for the contribution of the inert devices is

Equation (4): Dumb device contribution

$$\text{Token contribution} = \frac{\text{Dumb contribution portion}}{\text{Rank}} \quad (4)$$

Within Equation (4) the *dumb contribution portion* provides the basis of the calculation. Token devices when detected will contribute a static confidence percentage and so to get a balance between these and the intelligent devices it is proposed to allocate a value such as 15% to the *dumb contribution portion*. Thus a significant item (wallet) with a rank of 2 when detected would add 7.5% to the Aura's confidence total. The sum of all of the contributions from dumb devices will have an upper bound threshold applied to ensure Aura confidence is not maintained at an artificially high level by a large number of these devices that can easily be appropriated by an impostor. If, for instance, an upper bound of 30% was applied, in the above example it would require four such items to be concurrently removed to maintain this maximum contribution. Even if this were achieved, at this level only a very limited service would be available and with the fundamental *core confidence* eventually becoming negative its effect would be eradicated and the device rendered unusable.

When intelligent devices are present but have not been through an authentication process it is proposed that they will be treated as dumb devices. Without authentication they would be incapable of making a contribution and so, by treating them in this way, at least their detected presence will be used positively.

Another point to note relates to scenario in which a participating device becomes lost or stolen. In this case, the user would ideally need to ensure they removed the device from the trusted list, in order to ensure the device did not have the on-going ability to participate within the Aura and gain further access. Over time, a device operating outside the Aura would have progressively locked itself down in any case, and re-detection of such a device within the proximity of other intelligent Aura members could be used to alert the legitimate user and help them to locate and recover the lost item.

## 5. Simulation and validation

In order to assess the effectiveness of the proposed Aura, and to model the aforementioned formulae to understand the impact the variables have upon the authentication security, a simulation based upon the observed experimental data has been undertaken.

### 5.1. Simulating typical usage

A script was written to calculate the Aura for an intelligent device based upon the observed data for a particular user. As devices became visible and then disappeared their influence was incorporated and used to offset a degrading confidence. The simulation was performed upon all users, running from 8am until midnight, but because of the sheer volume of data, this was evaluated in 10-min periods. Table 2 lists the fifteen items of equipment that an illustrative user chose to tag, enabling them to be identified during the experiment and also the ranking allocated to each device. The subjective rankings

**Table 2 – Tagged equipment and associated rankings.**

Equipment	Rank
Wallet	2
Fridge	4
Locker	6
Bed clock	4
Laptop (Work)	8
Car (Home)	3
Microscope	5
Coat	4
Fax	9
Wi-Fi (Home)	5
Bag	4
MP3	6
PC	6
Car (Work)	5
Mobile (Work)	5

were based upon visibility, mobility and how likely the item was to remain in the user's possession. For instance, the subject's fridge is static and unlikely to move, and there is little chance of it changing ownership; however the fax is a publicly visible work machine that is non-specific to the subject and available to multiple people. The intelligent devices have also been ranked in case they are treated as a dumb device (as discussed in the previous section).

For the purposes of the simulation it has been necessary to set some initial values that will be used and these are shown in Table 3. It should be noted that these values are merely for the purposes of simulation rather than being definitive and will in practice be set based upon an independent assessment. During the simulation it was assumed that the user attempted to access a low risk, low tariff application (e.g. texting on a mobile phone) once every 30 min. Whilst this model is not reflective of normal user behaviour it does provide a worst-case scenario from which to understand the performance of the framework. Furthermore, controlling the application variable assists in understanding the impact of the Aura attribute directly rather than any affect the application access might play. In reality, it is likely that user interactions with their device are batched rather than once every 30 min and as such the performance of the framework would be better than what is presented here. This application is deemed to be available at a confidence level at or above 20%, the chosen re-authentication threshold. If the confidence level was below the 20% threshold at point of operation, authentication was

**Table 3 – List of parameter values used in the simulation.**

Variable	Value
Authentication method tariff	3
Re-authentication threshold	20%
Device access frequency	30 min
Location multipliers: home, work, away	2.5, 5, 10
Intelligent device contribution factor	20%
Dumb device contribution factor	15%
Cumulative dumb device upper bound	30%
Period degradation factor	2%

assumed to be requested and successfully completed with an average level 3 method (such as a mixed case and alpha-numeric password of more than eight characters) and so confidence was set to the associated maximum threshold of 80%. It should be noted that in reality this figure would vary upon differing authentication techniques being invoked.

The location multipliers were set at home = 2.5, work = 5 and away = 10 (reflecting the progressively less trusted nature of each environment), thus for each 10-min time segment confidence was reduced by the 2% degradation factor multiplied by the location multiplier. For dumb devices the contribution factor was set at 15% with their cumulative total bounded at 30%, and the contribution portion for intelligent devices trialled at 20%.

For comparison, Fig. 5 illustrates the performance expected from a mobile device employing current PIN-based protection, with a 10-min screen lock and an assumption of access being required every 30 min. It should be noted, at the moment the screen lock is invoked the host device assumes the identity of the user to be valid, a well-documented weakness of this approach to security (Muncaster and Turk, 2006). In this and all succeeding plots the y-axis represents the percentage of Aura confidence, with the time of day being plotted along the x-axis. Additionally, plus (+) symbols have been overlaid to indicate the point at which access to the device was made and squares have been used to show the points when the user was required to authenticate. Each authentication is represented by two squares, the lower indicates the time and confidence at which authentication was invoked whilst the upper illustrates the confidence allocated immediately after the assumed successful authentication. It should be noted that in several situations and especially in Fig. 5, a plus and a square co-exist at the same point in time and have consequently been plotted one on top of the other.

From this control plot the simulation indicates that the user would be required to undergo an authentication process 32 times during the 16-h period from 8am until midnight. Also, employing a traditional Boolean approach to security, when authentication is passed confidence is set to 100% and remains unchanged until the screen lock is invoked and confidence drops to 0%. This gives the graph the box-wave appearance that is exhibited in the diagram.

As an initial experiment Figs. 6 and 7 have been shown to illustrate how introducing the proposed equation, at different locations, with the discussed parameters but without the positive contribution from detected devices, influences the observed identity confidence over time. Once again, re-authentication is demanded when service access is attempted at a confidence level below the threshold and this cut-off is drawn in a colour dependant upon the user's location.

Without any external Aura influence, in the 'away' example Fig. 6, the confidence degrades at a rate of 20% for every 10-min period since authentication, the 2% degradation factor multiplied by the location weighting (10 for away). Thus it takes 30 min to degrade from the authentication level of 80% to 20% and 40 min to drop below this re-authentication threshold. As a result, in this test simulation authentication is required every 60 min, leading to the 16 authentications exhibited by this default graph between 8am and the 12pm cut-off. It should be noted that the nature of these authentications from the control set and the model are useful for comparing and understanding how many times an authentication is required. They are not, however, directly comparable in terms of the security they are providing, with the PIN-based approach being significantly weaker than the approaches utilised within the Aura.

Introducing the observed experimental data as shown in Fig. 8 and allocating the device rankings outlined earlier in

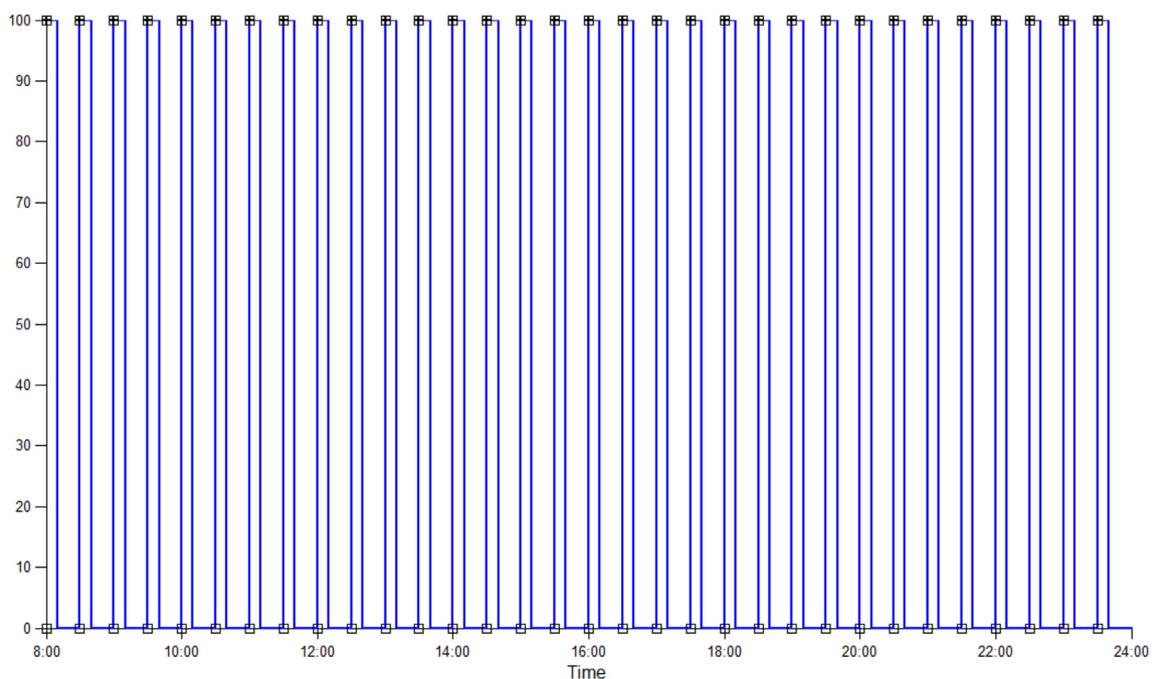


Fig. 5 – Control plot of user identity confidence on a device with a 10-min screen lock.

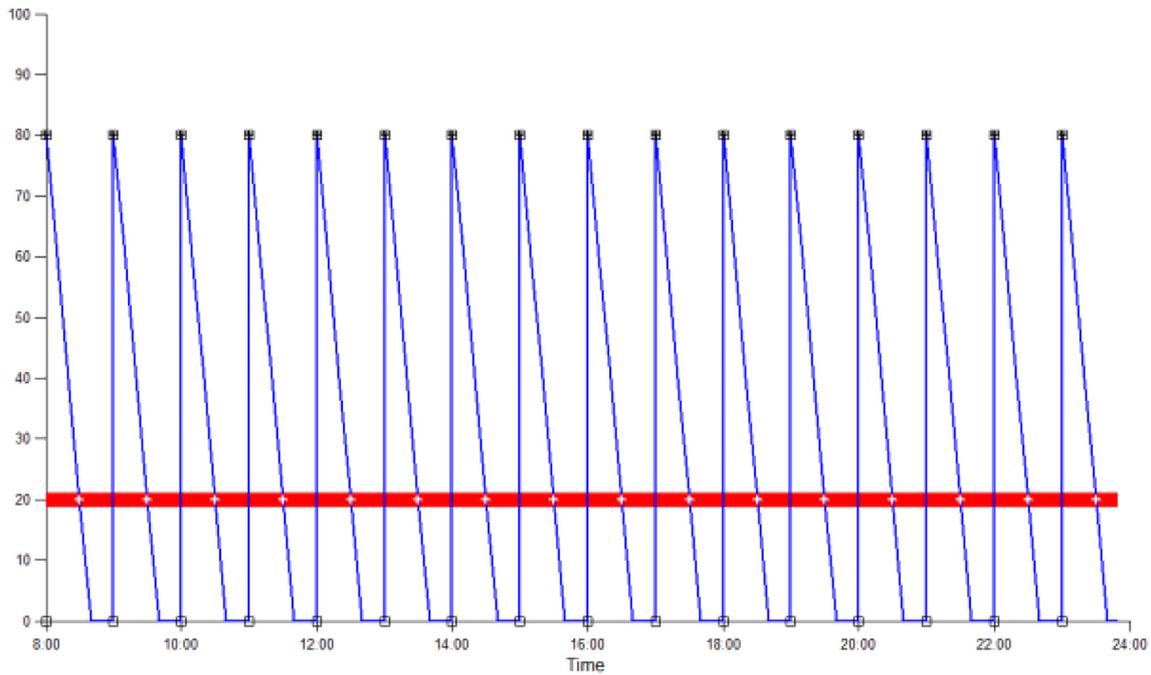


Fig. 6 – Degrading confidence whilst away.

Table 2 it is possible to fully simulate the Aura's action which has a significant effect as presented in Fig. 9.

Immediately it is noticeable that the detected devices provide the necessary information to ascertain the location of the user at any given time. The default location is away but this graph indicates the extended periods that are spent both at home and in a work environment (as highlighted by the colour band at the 20% threshold). Interestingly, as discussed

previously, upon activation of the core device initial authentication is delayed for a period of time. Although initially the Aura only contributes approximately 24%, a level at which services should be extremely restricted, it is a level at which the first simulated access can function and is a good indicator of the influence that can be harnessed. This influence is further illustrated by the confidence rising above the parameterised 80% level immediately upon each authentication.

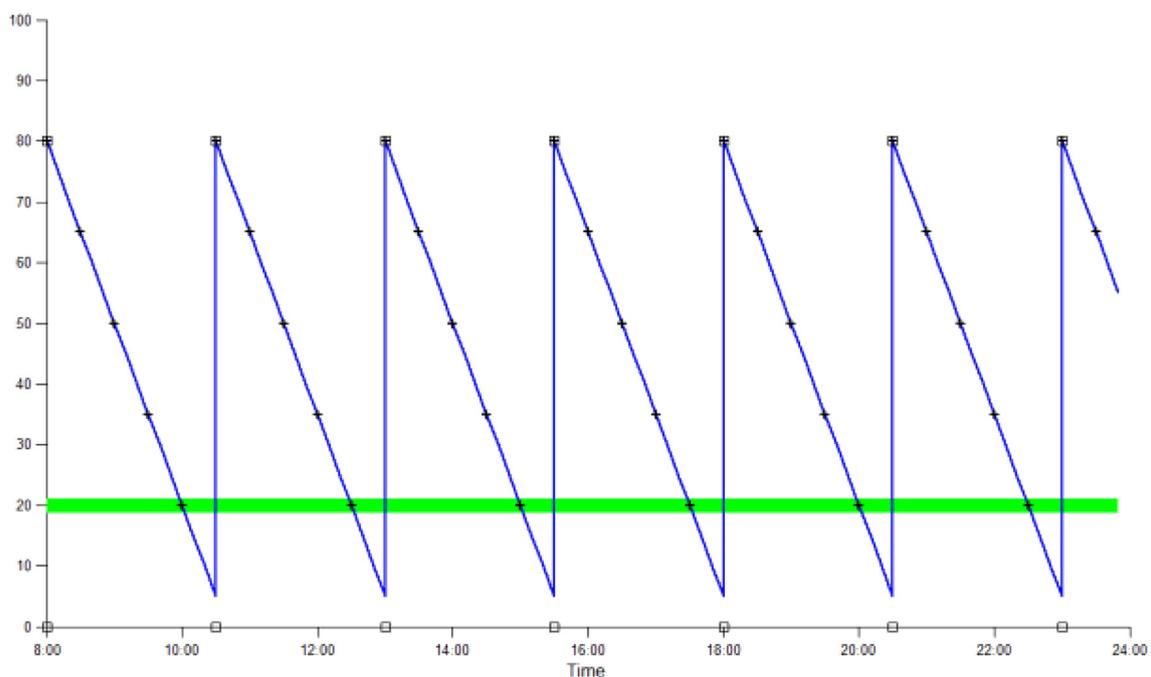


Fig. 7 – Degrading confidence whilst at home.

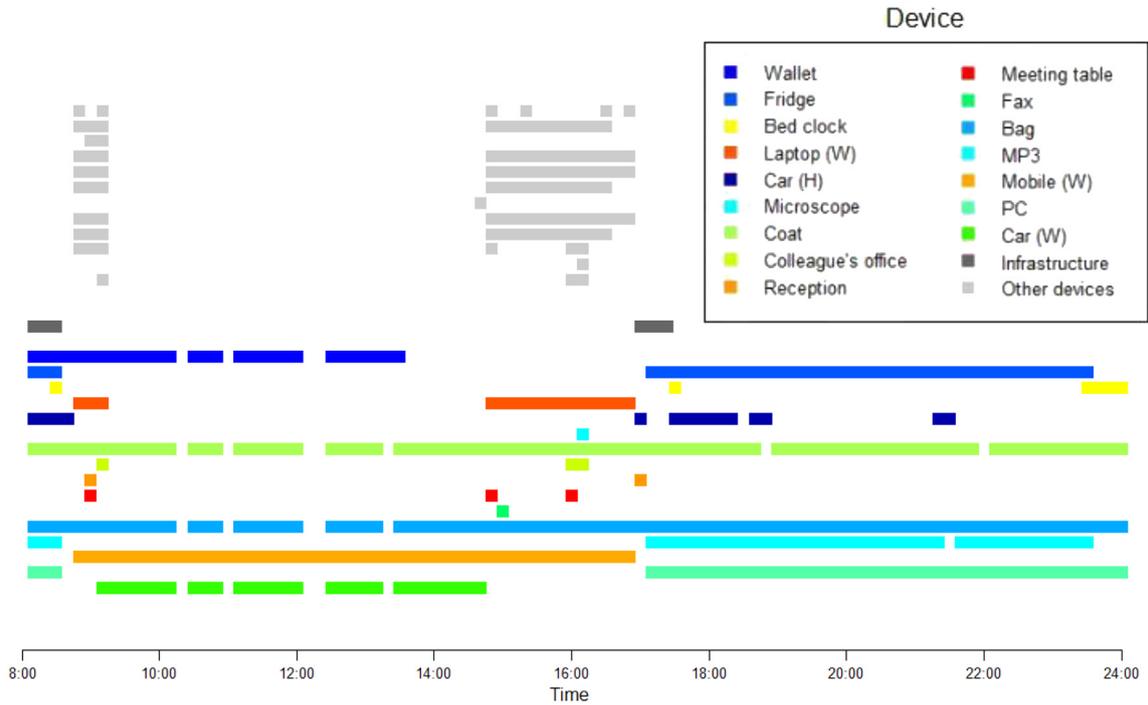


Fig. 8 – User’s devices detected during the day upon which the simulation graph below is based.

Location of the user and the core device clearly affects the rate of decline in confidence; with the user returning home just before 5pm, beyond this point the gradient of the plot significantly reduces, reflecting the relaxation of degradation

expressed within the Aura equation. At approximately 2.30pm the user moves within detectable proximity of their laptop and the added assurance of this intelligent item alone reverses the confidence erosion, reflected by a spike in the graph

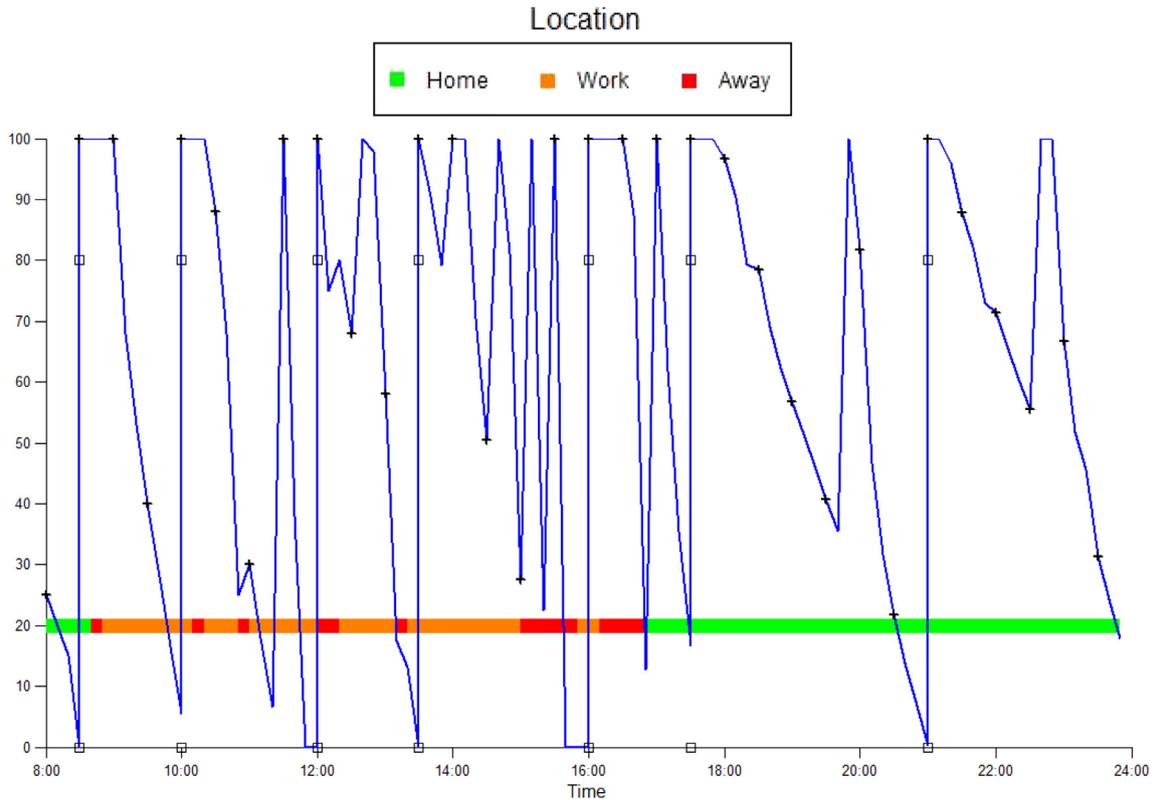


Fig. 9 – Aura influenced results for the same user on the same day.

at this point. This further supports the applicability of the Aura's approach and with the future expected to provide us with greater numbers of intelligent devices, the potential for security leverage is only likely to increase. Overall the number of authentications across the 14 h of utilised experimental data for this user on the simulated day is reduced to 7, 22% of the baseline 32. When the simulation was run for all candidates across all days and the number of authentications recorded, the total number of simulated authentications was 26% of the baseline total; an average of 8.4 authentications per day with an observed standard deviation of 2.9.

For comparison purposes, Fig. 10 illustrates a different user's simulated weekend day activity based upon their own specific devices and personal items but using identical parameters and thresholds. From this, it is clear to see that apart from an hour in the early afternoon the user spent their entire day at home. In this location the Aura is most relaxed with degradation at its slowest. During the plotted 14 h only 5 authentications are required, only 16% of the baseline 32. The home reference graph (Fig. 7) suggests that without the Aura's influence re-authentication will be expected every 2.5 h. In the weekend graph however, this period extends to as much as 4 h between 9.30am and 1.30pm as the detected devices maintain the confidence at an operable level. There are six points during the day at which the confidence is capped and then sustained at its maximum level of 100%. Additional contributions from the Aura push the confidence from the simulated authentication threshold of 80% to above the 100% for over 60 min before the erosion finally draws the level back below the cap.

Alteration of the simulated parameters of course influences this performance, Figs. 11–13 illustrate five variations of the same user and day as Fig. 9 with different values of intelligent device contribution.

In the examples above, the main effect of varying the intelligent device contribution parameter is to reduce the

number of authentications during the day from nine in Fig. 11 to seven in Fig. 13. Logically, the overall confidence percentage is maintained at a higher level for longer and is slower to degrade. With this occurring the user would have more high-level applications and functionality available for their use for greater periods of time. For comparison, Figs. 14–16 present three graphs, each with a different authentication level. They are based on the same user and day, with an intelligent device contribution value of 20.

Varying the authentication level is of course for illustration purposes because in a real-life implementation the tariff of the authentication method will depend on devices' capabilities and in-built technology. As discussed earlier, at the weakest level (1) the associated confidence percentage will only rise to 60% upon authentication and with the strongest method (5) it will be 100%. In the figures the main variations are that the number of authentications decreases from eleven to six and at the lowest level the framework fails to maintain the confidence percentage at 100%. Interestingly, in the weakest model, Fig. 16, although the simulation authenticated at 60%, the affect of the Aura pushed the confidence up to the maximum. This suggests that if utilised, an Authentication Aura approach to security would enable a low-end device that was limited in authentication ability in its own right to perform at a much higher level than would currently be possible.

Finally, the period of time spent at home in the evening does not exhibit a significant influence, however during the day when the user is at work and away from the office, confidence unsurprisingly erodes much more rapidly with a lower tariff.

The investigation and discussion of varying parameters for each day in minute detail is beyond the scope of this paper, however it is possible to observe how changing some of them immediately impacts upon the performance of the

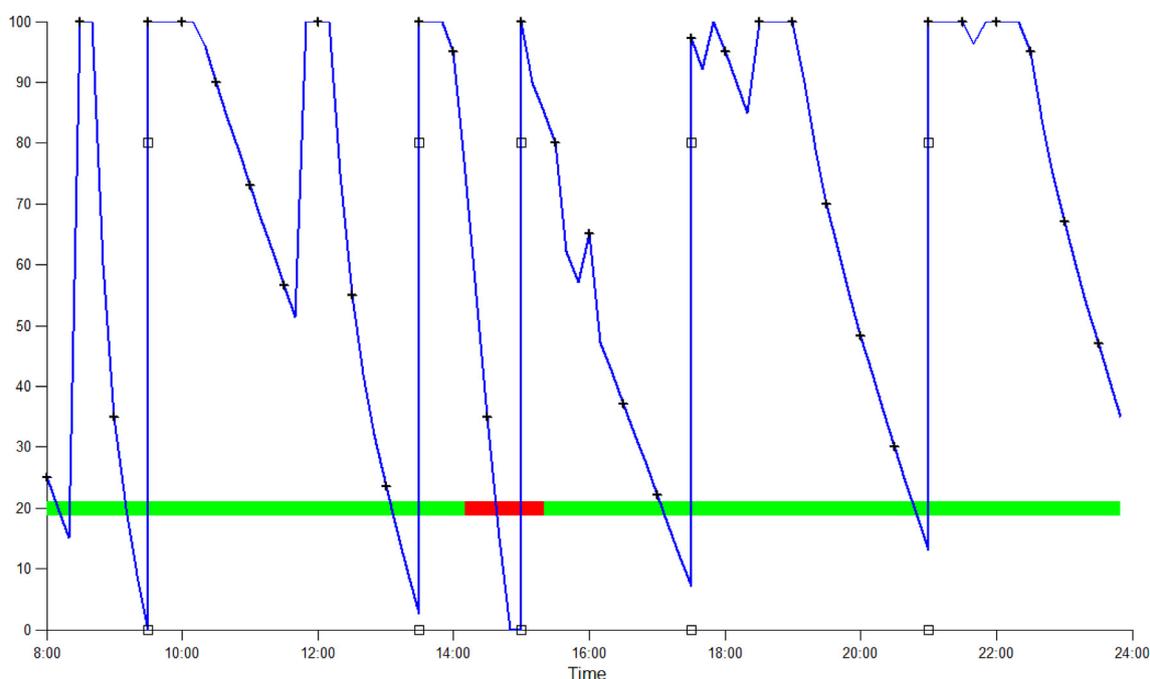


Fig. 10 – A user's weekend Aura profile.

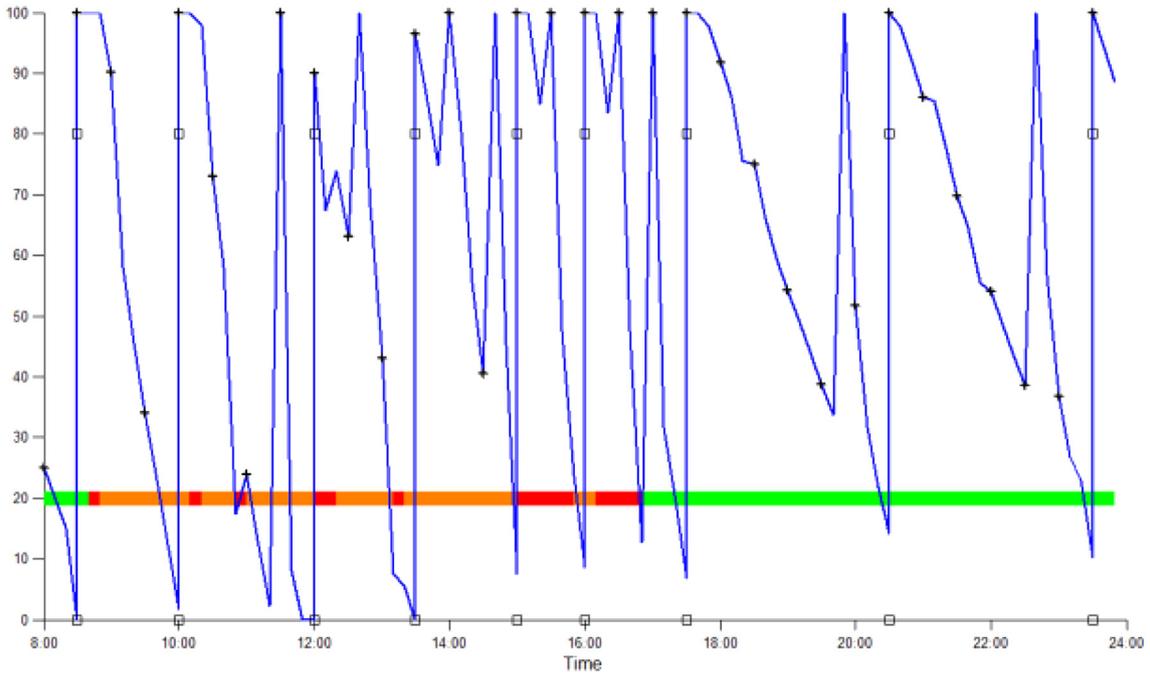


Fig. 11 – Intelligent device contribution 10.

authentication Aura approach to device security. As previously highlighted, altering the intelligent device contribution and simulated level of authentication security both reduce the number of observed authentications whilst maintaining higher levels of confidence for longer. This will permit a user of a mobile device to have access to more applications for longer, making the item of equipment more usable. However, influencing the framework in this way has the potential to make this approach less robust to theft.

### 5.2. Simulating a device theft

This simulation was re-run for the original user and day as illustrated in Figs. 8 and 9 and at 2:01pm any detection of the user’s coat, bag, work’s mobile phone and work’s vehicle (the items that were present) was blocked. The resultant plot of the Aura’s confidence is shown in Fig. 17.

Upon theft the Aura immediately reverts to the default location of away and it can be seen that without the influence

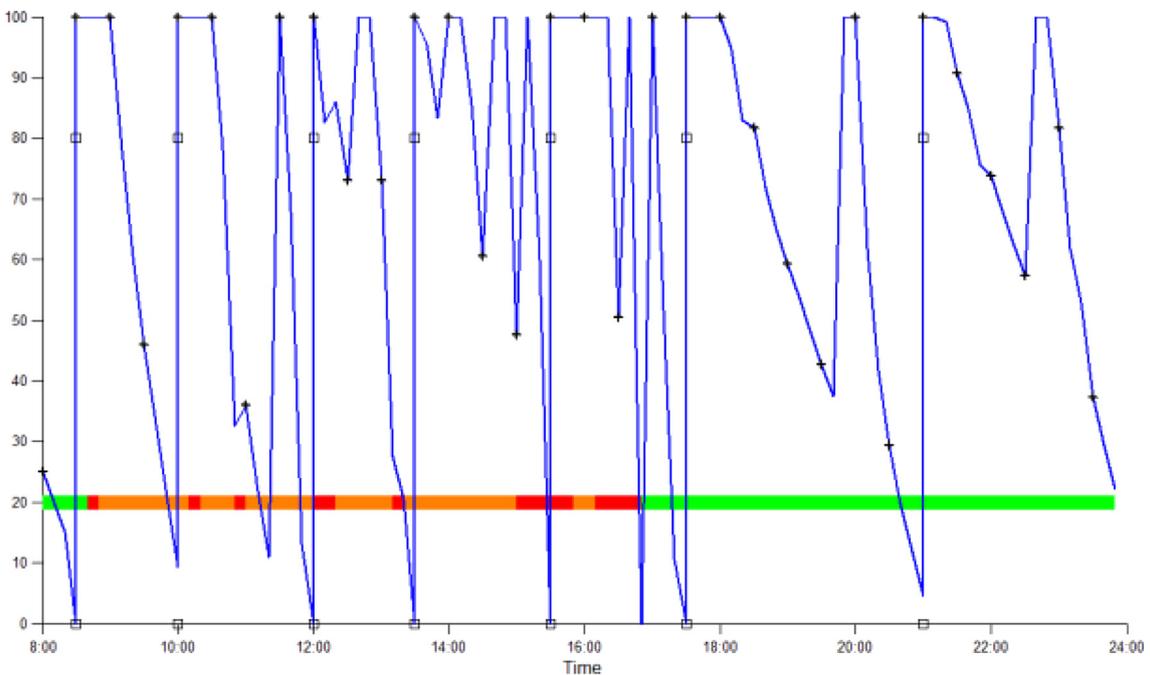


Fig. 12 – Intelligent device contribution 30.

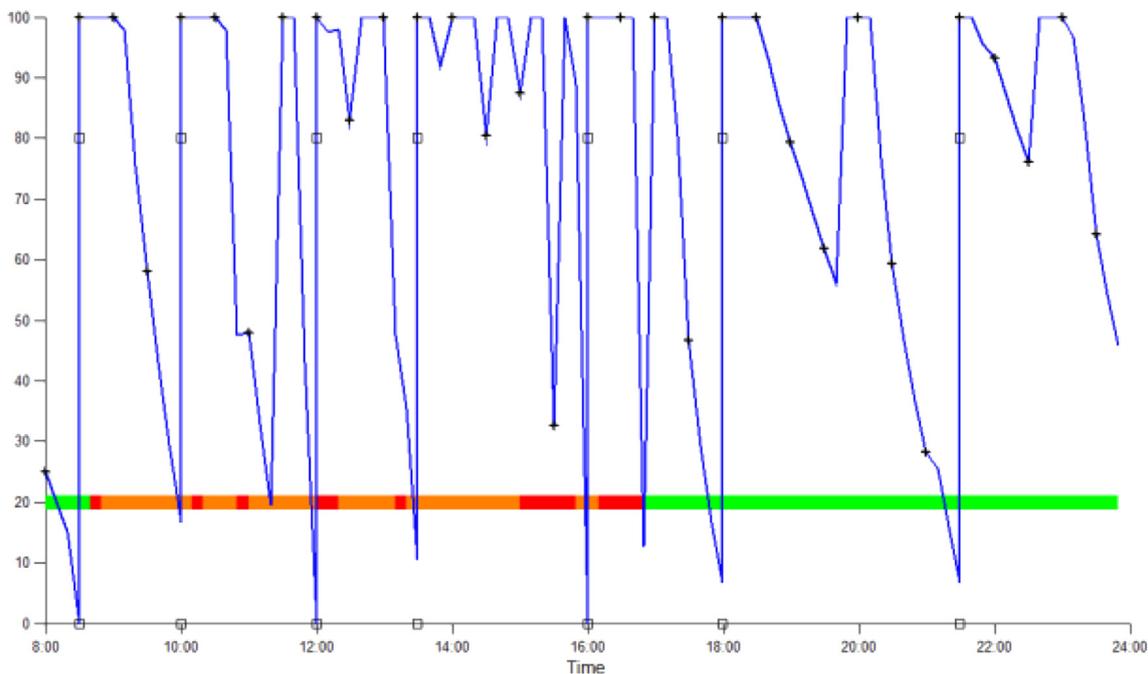


Fig. 13 – Intelligent device contribution 50.

of known devices within 12 min the confidence has fallen below 20% and it takes 25 min in total for the confidence to plummet from maximum confidence (100%) and flatten out at zero. As the Aura reaches this point all potential services and applications would have been barred and without re-authentication, the simulated device rendered unusable. It should be remembered that for the simulations within this

paper the Aura calculations have been re-run every 10 min. In a real-life application it is anticipated that this will occur more frequently and so the response to theft would be quicker. Even so, in comparison to an unlocked and unprotected mobile phone, this is a significant improvement over being blocked only when the battery’s charge is spent and the device shuts down.

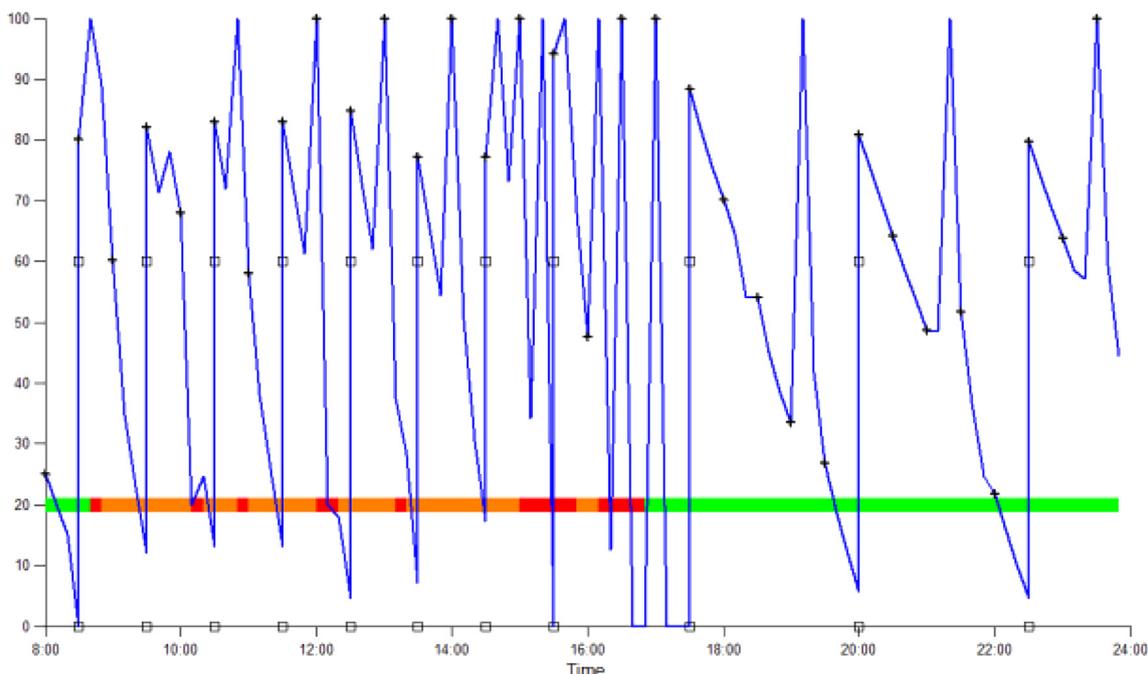


Fig. 14 – Authentication level parameter set to 1.

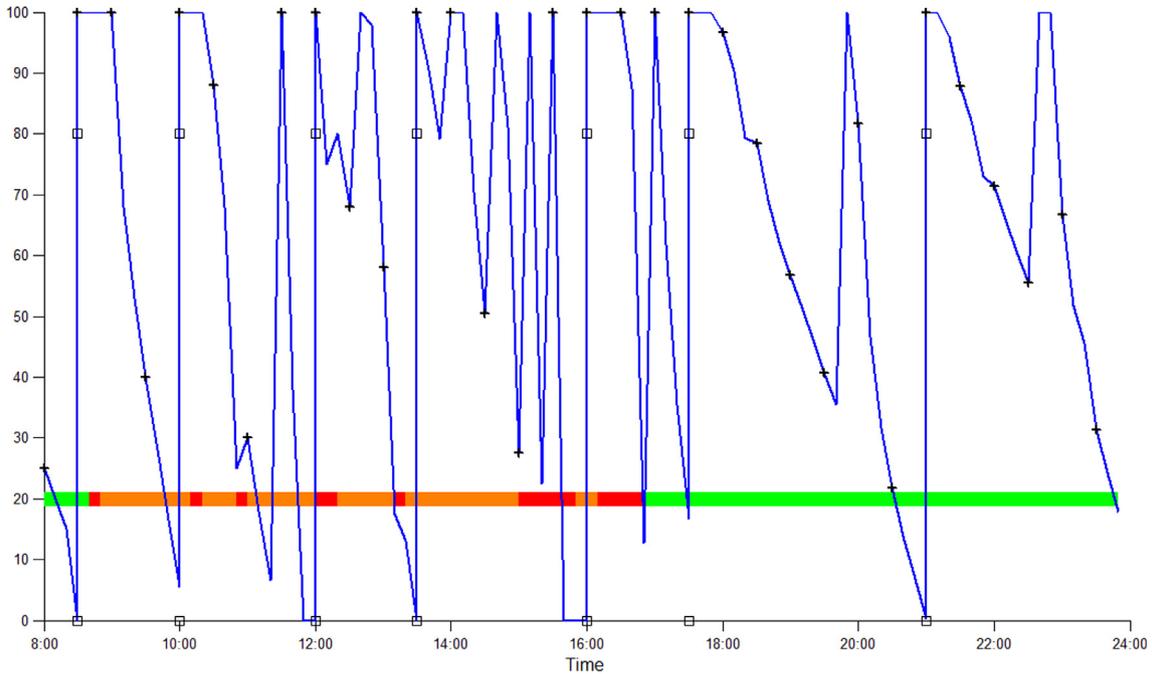


Fig. 15 – Authentication level parameter set to 3.

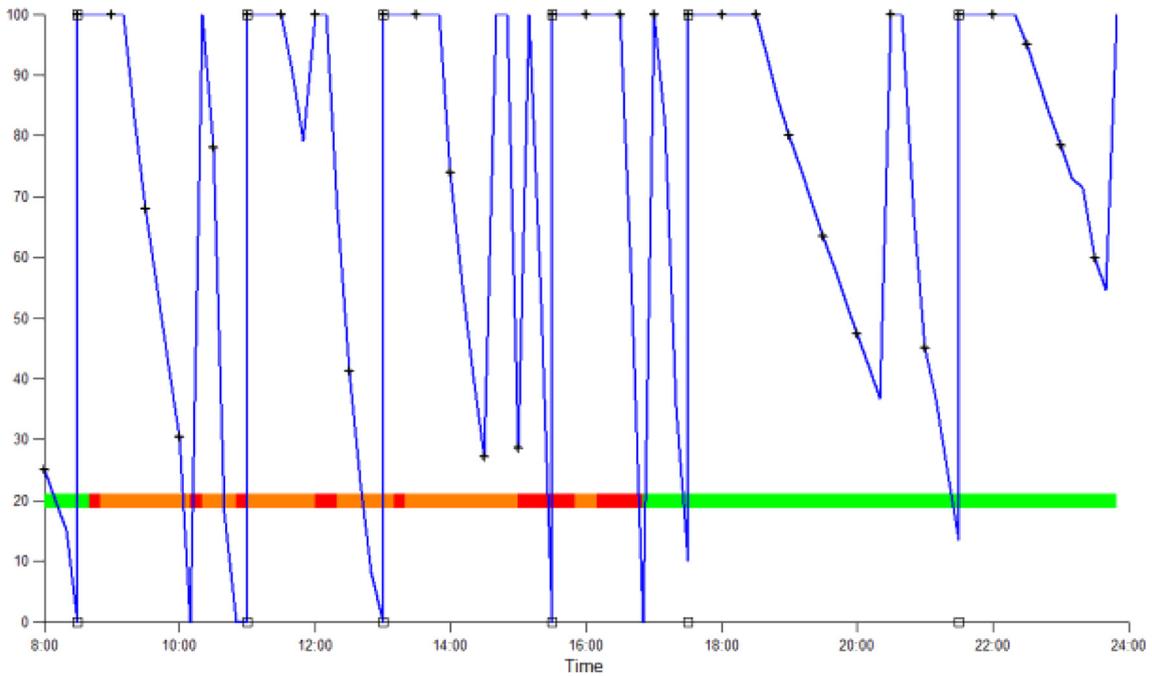


Fig. 16 – Authentication level parameter set to 5.

## 6. Conclusion

From an authentication perspective, our increasing utilisation of IT multiple devices has only served to increase the burden placed upon end users, who consequently find themselves having to prove their identity to an increasing range of devices on a fairly frequent basis. The concept of the Authentication Aura aims to use the very fact of having multiple devices to the opposite effect; reducing the burden on the user while aiming to improve the overall level of authentication

confidence in the process (taking it beyond a point of entry mechanism into a more continuous mode based upon cooperation between the user's devices).

The investigation into inherited confidence has demonstrated that there is indeed scope for an approach such as the Authentication Aura methodology to positively contribute towards device security. The simulation results have indicated the advantage that this technique can offer when identity confidence measures are coupled with a positive influence from known devices. Awareness of surroundings and other objects can also be leveraged both unilaterally and

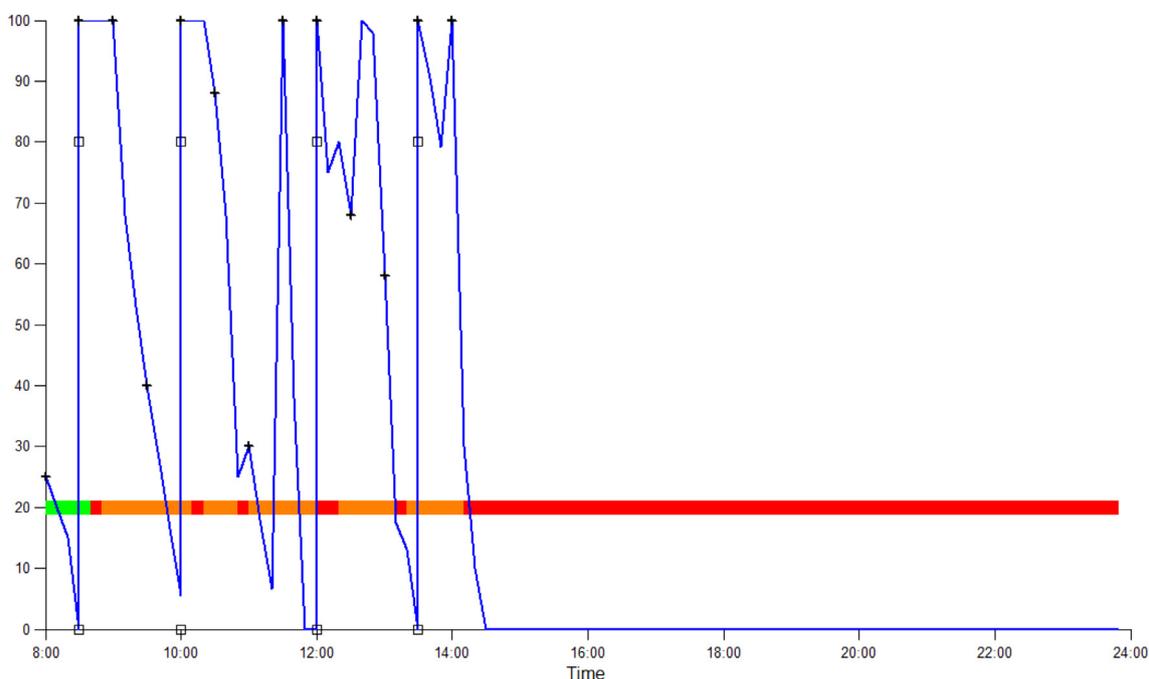


Fig. 17 – A simulated theft illustrating the Aura's response.

within a co-operative set of devices to further boost identity confidence and even circumvent the need for authentication. Significant value can also be drawn from considering dumb possessions that we might not readily expect, especially those that are not immediately visible but are carried on a daily basis. With the placement of RFID tags in clothing being proposed, even what we are unconsciously wearing might contribute to security in the future.

A significant 74% reduction in the number of daily authentications required by a smartphone user when compared with one who accesses their device once every 30 min, with a 10-min PIN-protected screen lock in place, was also observed. Reducing this repetitive and onerous task, whilst maintaining a high level of security, should be of interest to purchasers and producers of such devices alike.

An additional benefit of such an approach is the reaction to theft, and the short timescale the Aura takes to block application usage and render the device unusable. Governments and renowned design agencies are calling for the greater protection of mobile devices; the results suggest that implementing an Authentication Aura has the potential to meet such demands.

Utilising the findings of the simulation as a foundation for the next stage of investigation it is now possible to develop a working prototype based upon the concepts outlined in this paper. Functioning agent software will now be written and tested to further establish the validity of this method and if there are practical or operational restrictions that are currently unforeseen. Beyond this, it is acknowledged that there is also a need to consider the threat model that would apply to the Aura approach, including identifying and managing any potential for gaming of the system in order to prevent manipulation and misuse in order to fool or circumvent the controls. This will consequently form part of the future

work once the viability of the underlying authentication concept has been more fully validated.

## Acknowledgements

The research presented in this paper has been undertaken with funding and support from Orange-France Telecom.

## REFERENCES

- Albrechtsen EA. Qualitative study of users' view on information security. *Comput Secur* 2007;26(4):276–89.
- AuthenticationWorld. Authentication strength. *Authentication world.com*. <http://www.authenticationworld.com/Authentication-Strength/> [accessed 18.05.13].
- Clarke NL. Transparent user authentication: biometrics, RFID and behavioural profiling. Springer; 2011.
- Clarke NL, Furnell SM. Authentication of users on mobile telephones – a survey of attitudes and opinions. *Comput Secur* 2005;24(7):519–27.
- Clarke NL, Furnell SM. Advanced user authentication for mobile devices. *Comput Secur* 2007;26(2):109–19.
- Dobyns N. Mobile device safety and security. *Tech Insights*; 23 October 2012. <http://www.wiu.edu/coehs/techinsights/blog/?p=1250> [accessed 12.04.13].
- Dritsas S, Gritzalis D, Lambrinoudakis C. Protecting privacy and anonymity in pervasive computing: trends and perspectives. *Telematics Informat J* 2006;23(3):196–210.
- Furnell SM, Clarke NL, Karatzouni S. Beyond the PIN: enhancing user authentication for mobile devices. *Comput Fraud & Secur* 2008;2008(8):12–7.
- Hocking CG, Furnell SM, Clarke NL, Reynolds PL. A distributed and cooperative user authentication framework. In: *Proc. of 6th*

- international conference on information assurance and security (IAS 2010). Atlanta, USA; 23–25 August 2010. p. 304–10.
- Hocking CG, Furnell SM, Clarke NL, Reynolds PL. A preliminary investigation of distributed and cooperative user authentication. In Proc. of the 9th Australian information security management conference (SECAU 2011). Perth, Australia; 5–7 December 2011.
- Jansen WA. Authenticating users on handheld devices. In: Proc. of Canadian information technology security symposium; 2003.
- Ledermuller T, Clarke NL. Risk assessment for mobile devices. In: Proc. of privacy and security in digital business – 8th international conference (TrustBus 2011). Toulouse, France; 30 August–2 September 2011. p. 210–21.
- Muncaster J, Turk M. Continuous multimodal authentication using dynamic Bayesian networks. In: Proc. of 2nd workshop on multimodal user authentication. Toulouse, France; 11–12 May 2006.
- Mylonas A, Kastania A, Gritzalis D. Delegate the smartphone user? Security awareness in smartphone platforms. *Comput Secur* 2013;34(3):47–66.
- O’Gorman L. Comparing passwords, tokens, and biometrics for user authentication. *Proc IEEE* 2003;91(12):2019–40.
- RSA Laboratories. RFID, a vision of the future. RSA Laboratories; 2012. <http://www.rsa.com/rsalabs/node.asp?id=2117> [accessed 18.05.13].
- Sakr S. RFID: radio tags set to combat the counterfeiters. BBC News Online. <http://www.bbc.co.uk/news/business-12358919>; 6 February 2011 [accessed 18.05.13].
- Tanvi P, Sonal G, Kumar SM. Token based authentication using mobile phone. In: Proc. international conference on communication systems and network technologies (CSNT) 2011. Katra, Jammu, India; 3–5 June 2011. p. 85–88.
- Vu KL, Proctor RW, Bhargav-Spantzel A, Tai B, Cook J, Schultz EE. Improving password security and memorability to protect personal and organizational information. *Int J Hum Comput Stud* 2007;65(8):744–57.
- Chris Hocking** achieved a BSc (Hons) in mathematics and statistics from the University of London, Goldsmiths College in 1986. After an eighteen-year career in industry he returned to education attaining an MSc in web technologies and security from the University of Plymouth in 2007. Since this time Chris has been a PhD researcher within the Centre for Security, Communications & Network Research at Plymouth University. His research is focused upon the topic of transparent and non-intrusive user authentication. Chris’s research is being undertaken with financial sponsorship from Orange/France Telecom.
- Prof. Steven Furnell** is the head of the Centre for Security, Communications & Network Research at Plymouth University, and an Adjunct Professor with Edith Cowan University in Western Australia. His interests include security management and culture, computer crime, user authentication, and security usability. He is the author of over 230 papers in refereed international journals and conference proceedings, as well as books including *Cyber-crime: Vandalising the Information Society* (2001) and *Computer Insecurity: Risking the System* (2005). Further details can be found at [www.plymouth.ac.uk/cscan](http://www.plymouth.ac.uk/cscan), with a variety of security podcasts also available via [www.cscan.org/podcasts](http://www.cscan.org/podcasts).
- Dr Clarke** is an Associate Professor in Information Security and Digital Forensics at Plymouth University. Dr Clarke is also an adjunct Associate Professor at Edith Cowan University, Western Australia. His research interests reside in the area of biometrics, forensics and intrusion detection. Dr Clarke has over 100 outputs including journal papers, conference papers, books, edited books, book chapters and patents. He is a chartered engineer, a fellow of the British Computing Society and a senior member of the IEEE. Dr Clarke is the author of *Computer Forensics: A Pocket Guide* published by IT Governance and *Transparent Authentication* published by Springer.
- Prof. Paul Reynolds** is a technical specialist in Internet based mobile telecommunications. He has a doctorate in Advance Telecommunications and among other things he has: directed the European Union’s funded research into distributed computing for mobile telecommunications; designed mobile telecommunication networks for eight countries; been the technical leader of the Mobile Wireless Internet Forum and of two major European Union research projects; and, been the chairman of EU’s Group responsible for leadership of Europe wide next generation mobile telecommunications. Since 1993 he has authored 11 patents, and over 40 published technical papers, in the area of telecommunications.

## **Appendix D. Experiment Instructions**

---

These instructions were given to each of the volunteers who agreed to perform the research experiment. They were explained in detail prior to each subject signing an agreement confirming their willingness to partake.

**UNIVERSITY OF PLYMOUTH**  
**FACULTY OF SCIENCE AND TECHNOLOGY**

CONSENT TO PARTICIPATE IN RESEARCH PROJECT

---

Name of Principal Investigator

**Chris Hocking**

---

Title of Research

**Authentication Aura**

---

Brief statement of purpose of work

This research experiment aims to establish if security of mobile devices such as laptop computers and mobile phones can be improved by making them aware of their environment and other devices that are close to them at any given time. To help achieve this it is necessary to carry out a continuous survey over a two week period to ascertain what equipment is close to the participant and in what environment they are. Mini radio transmitters/beacons (15 per person) will be issued to each volunteer and they will be required to position these throughout their working and home environment. Each one will represent a single device. A small data gathering device will then be carried constantly for the duration of the experiment which will record all nearby radio beacons on a minute by minute basis.

---

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations).

Under these circumstances, I agree to participate in the research.

Name: .....

Signature: .....

Date: .....

# Experiment Instructions

## Introduction

Thank you for agreeing to take part in this experiment. This PhD research work is being undertaken to investigate how security of mobile devices (such as laptops and phones) can be improved.

To participate in this study you will have been issued with a Dell Personal Digital Assistant (PDA), charging cable and a number of small blue plastic blocks with adhesive tape on one side. This equipment has been selected as a convenient and portable means of gathering information about your surroundings on a 24x7 basis for two weeks.

The supplied blue plastic blocks are Radio Frequency Identity (RFID) tags that constantly transmit a unique 8 digit alphanumeric code. Within 10m or so, the PDA can hear the transmitted code and record the presence of the tag. If more than one tag is present, the PDA will hear and note all codes simultaneously.

You will be required to position the tags on or close to pieces of everyday equipment that you will find in your home, workplace or even car. Although adhesive tape is present on the back of each tag it is preferable that this remains untouched, allowing the tags to be easily recovered and reused during follow-on experiments. The aim of this experiment is to then allow the PDA to constantly monitor your surroundings and record the equipment that is near to you at any given moment. With a significant number of participating volunteers, the observed data can be analysed to investigate if this concept holds potential to improve our everyday information and device security.

**Although the tags constantly transmit data via a dedicated radio frequency, they will not interfere with any other household equipment or indeed pose a health risk to anyone undertaking this experiment.**

Upon completion of the experiment the equipment will be collected and the data extracted from the PDA into a database for analysis. No subject will be linked to the data they have returned and at no point will they be required to supply their name or any other identifying information. The data will remain entirely anonymous at all times and not distributed to any outside parties.

If for any reason you wish to terminate the experiment early, this can be done at anytime without obligation. Any data that has been gathered will be completely and securely removed from the PDA and extracted from any related databases.

Once the experimental database is populated with data from all the consenting participants, trend analysis and device proximity investigative work will be undertaken. It is hoped to produce results that will be significant enough to warrant publication to a broad scientific community. As such, it is anticipated that this work will be published on the internet and throughout appropriate scientific media.

When this tranche of research work is finalised, all associated databases will be destroyed and any supplied paperwork shredded.

## Guidance

### The Personal Digital Assistant (PDA)

Figure 1 below highlights the elements and controls of the PDA that will be referred to in this document. Some of them you will refer to often but most you will only use in extreme circumstances should the need arise. If the experiment concludes without incident, it will run continuously for two weeks and the only intervention that will be required is to charge the PDA to ensure it remains active at all times.

On-off button

this button illuminates when the PDA is active. It will glow green when the PDA is fully charged, orange during regular use and will start to flash when the battery power is getting critically low. If you observe this state during the experiment please recharge the unit as soon as possible. In the event of a complete power failure please note the date and time on the provided Power Failures sheet, connect the PDA to the mains and reset it to recommence operation as described in the Resetting the PDA section on page 4.

Do not turn off the PDA during the duration of the experiment.

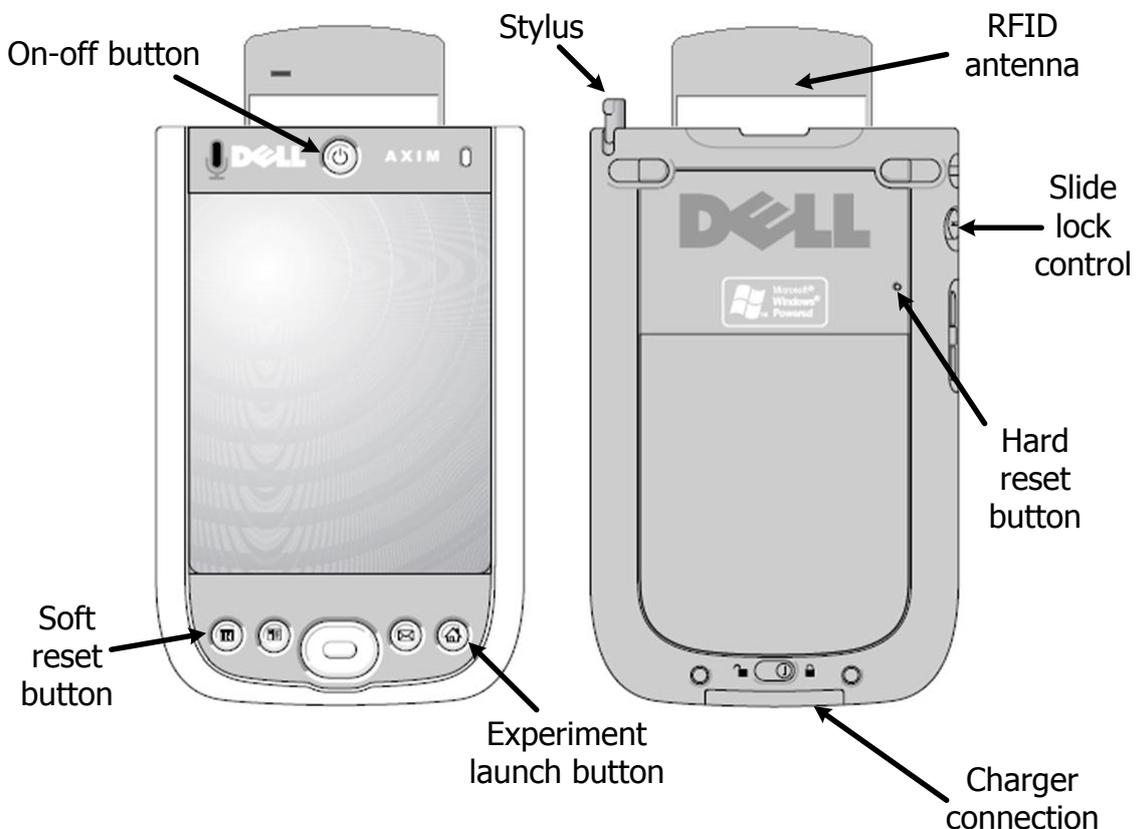


Figure 1. Anatomy of the PDA

Stylus	used to perform a <i>hard reset</i> of the unit. See Resetting the PDA on page 4.
RFID antenna	this receives the communication from the tags.
Slide lock control	allows the unit to be locked inhibiting the function of any other PDA controls. Sliding the control to the up position will lock the unit, sliding it down will enable all other buttons to be used. Following the commencement of the experiment slide this control to the locked position; only unlock the PDA in exceptional circumstances.
Charger connection	the point at which the mains charger is connected. Refer to Charging the PDA below.
Experiment launch button	this button will start the application to commence the experiment. If during the launch of the application a message is displayed that suggests “The program is from an unknown publisher...” and asks if you want to proceed, do so by touching the “Yes” button in the bottom left hand corner of the PDA’s display. Once the application has started running apply the slide lock control immediately.
Soft reset button	refer to Resetting the PDA on page 4.

### Charging the PDA

It is imperative that the PDA remains active during the course of the experiment. Although it has been fitted with an extended life battery pack, it will require charging once a day. Connect the PDA to a wall socket using the charging cable as shown in Figure 2 below.

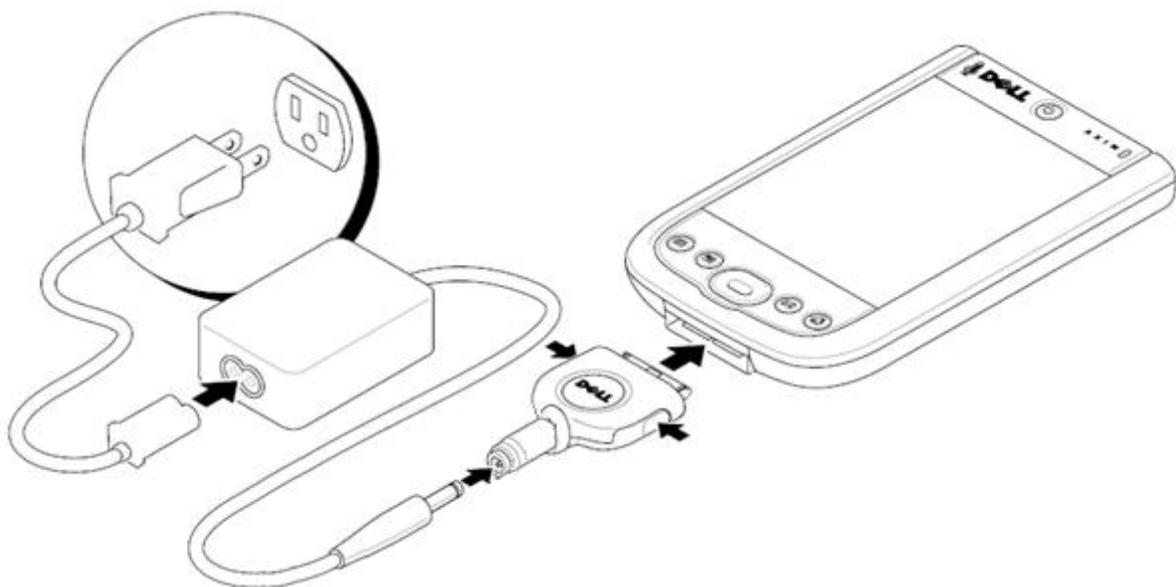


Figure 2. Connecting the PDA to the mains for charging

If possible leave the unit connected to the mains until it is fully charged at which point the on-off button will glow green. This process will take approximately 3 hours.

It is best if the unit is charged overnight but if charging has to take place during the day please try to ensure it is during a period of little activity when you are not moving around within your environment and will be stationary in close proximity to the PDA. If you move away from the unit and fail to take it with you, the integrity of the recorded data will be compromised and the experiment tainted.

### Tag location

To ensure that the experiment is as successful as possible it is necessary to position the tags in places that will yield the maximum coverage whilst giving the most meaningful results. Below is a list of devices and items that should be tagged where at all possible. If for some reason an item cannot be tagged or it is not owned please make a brief note in the provided comments sheet.

Mobile phone	Work PC	Home PC / Laptop	Work Wi-Fi point
Home Wi-Fi Point	TV (s)	Car interior	Car keys
Wallet/purse	mp3 player	Work bag/briefcase	Home telephone
Bedside clock	Fridge	Hi-Fi	Coat pocket

If there are surplus after installing the tags following the list above, please use your own imagination to place any remaining tags in locations you frequent often (whilst carrying your mobile phone i.e. a toilet or bathroom is not deemed a significant location! ☺) or alternatively on frequently used pieces of electronic equipment. Make sure you complete the Tag Inventory sheet as accurately as possible.

It is important to note that large amounts of metal or concrete will impinge upon the tags ability to communicate with the PDA so please try to avoid placing tags in positions where this likely to occur.

### Resetting the PDA

Should the PDA become inoperable or the battery drain completely it may be necessary to rest the unit to enable it to function again.

In most cases a *soft reset* will be sufficient. With power available (either the on-off switch is glowing orange or the unit has been connected to the mains for charging) ensure the slide lock control is in the unlocked (down) position and then press the soft reset button as indicated in Figure 1. Anatomy of the PDA. If this is successful the display will momentarily switch off and then a blue desktop will appear. At this point, to ensure the unit is ready to recommence the experiment, press the on-off button to turn off the unit, wait for 5 seconds and then re-press the on-off button to switch it back on.

When the desktop reappears, initiate the experiment by depressing the Experiment launch button and then lock the PDA immediately.

Under extreme circumstances, even with the unit unlocked, the soft reset button may not function. In this event use the stylus to perform a hard rest as illustrated in Figure 3.

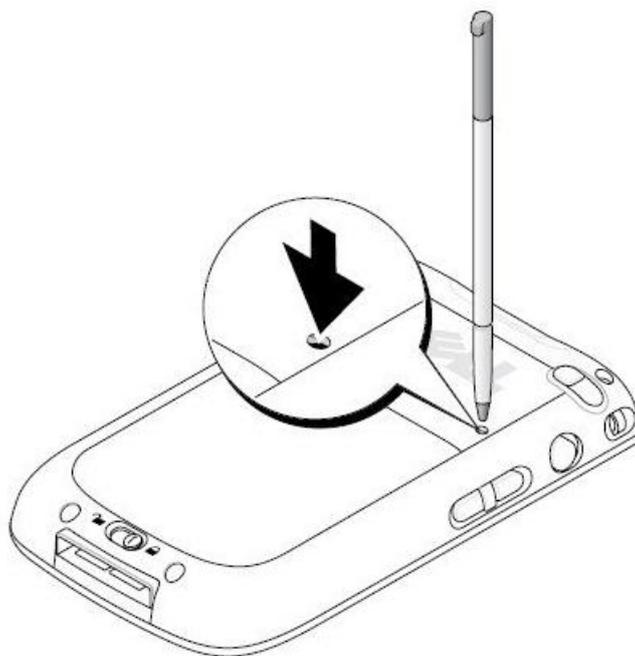


Figure 3. Performing a hard reset

Once this has been done, follow the steps to switch the unit off and on, and then launch the experiment as described above. Remember to lock the unit once it is active.

In the event that you have to perform a soft or hard reset, please note the occasion on the Power Failures sheet attached to the end of this document.

If you are unsure if it is necessary to reset the PDA please contact the experiment coordinator whose telephone number is shown in the Help section below.

### Commencing the experiment

Once all the tags have been installed ensure your PDA is charged, launch the experiment recording application and let it run for two complete weeks. Remember to recharge the PDA daily to ensure the continuity of the experiment and lock it to ensure it cannot be stopped inadvertently.

Each morning and regularly throughout the day please check that the on-off switch is still glowing orange to ensure the unit has not gone flat. In the event it has, please connect it to the mains as soon as possible and follow the instructions on Resetting the PDA.

### Help

Should you get into any difficulties or require further guidance (no matter how trivial) then please do not hesitate to contact Chris, the principal investigator coordinator, at any time.

Tel: 07812 768 799

If you are dissatisfied with the way the research is conducted, please contact the principal investigator in the first instance: tel. 07812 768 799. If you feel the problem has not been resolved please contact the secretary to the Faculty of Science and Technology Human Ethics Committee: Mrs Paula Simson 01752 584503.

## Tag Inventory

Please fill-in the table below as you are positioning the tags (blue plastic blocks) so upon completion of the experiment it will be possible to analyse the data in a meaningful way. Failure to do this accurately will render your participation in the experiment unusable, so please take care when entering the information.

Number	Tag id code (code written on tag)	Location (home, work, car, N/A)	Equipment description (e.g. mobile phone, work PC etc.)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

## Power Failures

Please record any time when the PDA experiences complete power failure and has to be reset. This will allow gaps in experimental data to be accounted for and enable analytical adjustments to be made. Please note details as accurately as possible and ensure the experiment is recommenced promptly.

---

Number	Date and time of complete PDA power failure / reset
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	

---



## **Appendix E. Ethical Approval Form**

---

This appendix contains the ethical approval form that was submitted prior to the experiment being performed. Without the consent of the ethics committee it would not have been possible to proceed with this area of the research.

**UNIVERSITY OF PLYMOUTH  
FACULTY OF SCIENCE AND TECHNOLOGY**

**Human Ethics Committee**

**APPLICATION FOR ETHICAL APPROVAL OF RESEARCH INVOLVING  
HUMAN PARTICIPANTS**

**All applicants should read the guidelines at the end of this application**

This is a WORD document. Please complete in WORD and extend space where necessary.

*All applications must be word processed. Handwritten applications **will** be returned.  
One signed hard-copy must be sent to Paula Simson. You may also send an unsigned electronic copy of your application to [paula.simson@plymouth.ac.uk](mailto:Paula.Simson@plymouth.ac.uk) as this will speed up the review process*

---

**1. TYPE OF PROJECT**

**1.1 What is the type of project? (Tick 1 only)**

**STAFF should tick one of the three options below:**

**Specific project**

Tick this box if you are seeking approval for a specific study, or set of studies, with methods that are explained fully in the following sections. This form of approval is appropriate for funded projects with a clear plan of work and limited duration.

**Thematic programme of research**

Tick this box if you are seeking approval for a programme of work using a single paradigm. This form of approval is appropriate for pilot work, or routine work that is ethically straightforward. Note, the maximum period of approval for thematic ethical clearance is 3 years.

**Practical / Laboratory Class**

Tick this box if you are seeking approval for a teaching activity which involves student involvement in the role of an experimental participant.

**1.2 Tick 1 only**

**POSTGRADUATE STUDENTS should tick one of the options below:**

Taught Masters Project

M.Phil / PhD by research

**UNDERGRADUATE STUDENTS should tick one of the two options below:**

Student research project

Practical / Laboratory class where you are acting as the experimenter

**2. APPLICATION**

<p><b>2.1 TITLE of Research project</b></p> <p>Authentication aura</p>
<p><b>2.2 General summary of the proposed research for which ethical clearance is sought, briefly outlining the aims and objectives and providing details of interventions/procedures involving participants (no jargon)</b></p> <p>This research experiment aims to establish if security of mobile devices such as laptop computers and mobile phones can be improved by making them aware of their environment and other devices that are close to them at any given time. To help achieve this it is necessary to carry out a continuous survey over a two week period to ascertain what equipment is close to the participant and in what environment they are. Mini radio transmitters/beacons (15 per person) will be issued to each volunteer and they will be required to position these throughout their working and home environment. Each one will represent a single device. A small data gathering device will then be carried constantly for the duration of the experiment which will record all nearby radio beacons on a minute by minute basis.</p>
<p><b>2.3 Physical site(s) where research will be carried out</b></p> <p>Within the University/working environment and at the willing participants home.</p>
<p><b>2.4 External Institutions involved in the research (e.g. other university, hospital, prison etc.)</b></p> <p>None</p>
<p><b>2.5 Name, telephone number, e-mail address and position of lead person for this project (plus full details of Project Supervisor if applicable)</b></p> <p>Lead person: Chris Hocking, +44 (0) 7812768799, christopher.hocking@plymouth.ac.uk, PhD research student</p> <p>Project Supervisor: Prof. Steven Furnell, +44 (0)1752 586234, sfurnell@cscan.org, School of Computing and Mathematics - Head of School</p>

<b>2.8 Start and end date for research for which ethical clearance is sought (NB maximum period is 3 years)</b>	
Start date: 01.01.2011	End date: 31.03.2011
<b>2.9 Name(s) of funding source(s) if any</b>	
Orange/France Telecom	
<b>2.10 Has funding already been received?</b>	
Yes	
<b>2.11 Has this same project received ethical approval from another Ethics Committee?</b>	
No	
<b>2.12 If yes, do you want Chairman's action?</b>	
N/A	
<b><i>If yes, please include other application and approval letter and STOP HERE. If no, please continue</i></b>	

**3. PROCEDURE**

<p><b>3.1 Describe procedures that participants will engage in, Please do not use jargon</b></p> <p>Each participant will be issued with 15 mini radio transmitters/beacons and asked to position these on pieces of equipment that they regularly come into contact with at home, work and in the car. Each one is numbered and they will record on paper the position of each beacon. They will then carry a Personal Digital Assistant (PDA) with them at all times for 14 days, charging their PDA daily. Each minute the PDA will listen to the close environment sensing all beacons that are within range and recording the identities of those found. The gathered data will be saved on the PDA for later analysis.</p>
<p><b>3.2 How long will the procedures take? Give details</b></p> <p>Positioning the beacons and filling in the appropriate paperwork will take 1 hour. Carrying the PDA will be continuous for 14 days.</p>
<p><b>3.3 Does your research involve deception?</b></p> <p>No.</p>
<p><b>3.4 If yes, please explain why the following conditions apply to your research:</b></p>
<p><b>a) Deception is completely unavoidable if the purpose of the research is to be met</b></p>
<p><b>b) The research objective has strong scientific merit</b></p>
<p><b>c) Any potential harm arising from the proposed deception can be effectively neutralised or reversed by the proposed debriefing procedures (see section below)</b></p>
<p><b>3.5 Describe how you will debrief your participants</b></p> <p>Participants will be verbally debriefed at the end of the experiment. This final debrief will repeat the nature and purpose of the study, confidentiality and include contact information should the individuals have any further questions.</p>
<p><b>3.6 Are there any ethical issues (e.g. sensitive material)?</b></p> <p>No.</p>
<p><b>3.7 If yes, please explain. You may be asked to provide ethically sensitive material. See also section 11</b></p>

#### 4. BREAKDOWN OF PARTICIPANTS

##### 4.1 Summary of participants

<b>Type of participant</b>	<b>Number of participants</b>
<i>Non-vulnerable Adults</i>	20
<i>Minors (&lt; 16 years)</i>	
<i>Minors (16-18 years)</i>	
<i>Vulnerable Participants (other than by virtue of being a minor)</i>	
<i>Other (please specify)</i>	
<b>TOTAL</b>	20

<b>4.2 How were the sample sizes determined?</b>
Funding for 5 sets of equipment has been received and it was decided to run 4 contiguous experiment groups, each with 5 volunteers.
<b>4.3 How will subjects be recruited?</b>
Via personal contacts.
<b>4.4 Will subjects be financially rewarded? If yes, please give details.</b>
No.

## 5. NON-VULNERABLE ADULTS

<b>5.1 Are some or all of the participants non-vulnerable adults?</b>
All participants are non-vulnerable adults.
<b>5.2 How will participants be recruited? Name any other institution(s) involved</b>
Via personal contacts.
<b>5.3 Inclusion / exclusion criteria</b>
Participants should be over 18 and students or employees who are willing to participate.
<b>5.4 How will participants give informed consent?</b>
Each potential candidate will be approached and briefed about the experiment. Only if they consent by signing an appropriate form will they be issued with the relevant equipment.
<b>5.5 Consent form(s) attached</b>
Yes – at end of information sheets.
<b>If no, why not?</b>
<b>5.6 Information sheet(s) attached</b>
Yes.
<b>If no, why not?</b>
<b>5.7 How will participants be made aware of their right to withdraw at any time?</b>
By an information sheet that will be issued with the equipment as part of the experiment.
<b>5.8 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?</b>
No personal, sensitive or identifiable data will be collected from participants. Users will be issued with a sequential number (1..20) but no cross reference between this and their identity will be held. Experimental results will be stored securely on the University's servers and on a password protected laptop computer. Upon completion of the research all information will be securely destroyed.



<b>6.8 Consent form(s) for parent / legal guardian attached</b>
No <input type="checkbox"/> Yes <input type="checkbox"/>
<i>If no, why not?</i>
<b>6.9 Information sheet(s) for parent / legal guardian attached</b>
No <input type="checkbox"/> Yes <input type="checkbox"/>
<i>If no, why not?</i>
<b>6.10 How will minors be made aware of their right to withdraw at any time?</b>
<b>6.11 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?</b>

**7. MINORS 16-18 YEARS OLD**

<b>7.1 Are some or all of the participants between the ages of 16 and 18?</b>
No.
<i>If yes, please consult special guidelines for working with minors. If no, please continue.</i>
<b>7.2 How will minors be recruited? (See guidelines). Name any other institution(s) involved</b>
<b>7.3 Inclusion / exclusion criteria</b>
<b>7.4 How will minors give informed consent? (See guidelines)</b>
<b>7.5 Consent form(s) for minor attached</b>
No <input type="checkbox"/> Yes <input type="checkbox"/>
<i>If no, why not?</i>
<b>7.6 Information sheet(s) for minor attached</b>
No <input type="checkbox"/> Yes <input type="checkbox"/>
<i>If no, why not?</i>
<b>7.7 Consent form(s) for parent / legal guardian attached</b>
No <input type="checkbox"/> Yes <input type="checkbox"/>

<b><i>If no, why not?</i></b>
<b><i>7.8 Information sheet(s) for parent / legal guardian attached</i></b>
No <input type="checkbox"/> Yes <input type="checkbox"/>
<b><i>If no, why not?</i></b>
<b><i>7.9 How will minors be made aware of their right to withdraw at any time?</i></b>
<b><i>7.10 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?</i></b>

### 8. VULNERABLE GROUPS

<b>8.1 Are some or all of the participants vulnerable? (See guidelines)</b>
No.
<i>If yes, please consult special guidelines for working with vulnerable groups. If no, please continue.</i>
<b>8.2 Describe vulnerability (apart from possibly being a minor)</b>
<b>8.3 How will vulnerable participants be recruited? Name any other institution(s) involved</b>
<b>8.4 Inclusion / exclusion criteria</b>
<b>8.5 How will participants give informed consent?</b>
<b>8.6 Consent form(s) for vulnerable person attached</b>
No <input type="checkbox"/> Yes <input type="checkbox"/>
<i>If no, why not?</i>
<b>8.7 Information sheet(s) for vulnerable person attached</b>
No <input type="checkbox"/> Yes <input type="checkbox"/>
<i>If no, why not?</i>
<b>8.8 Consent form(s) for parent / legal guardian attached</b>
No <input type="checkbox"/> Yes <input type="checkbox"/>

<b><i>If no, why not?</i></b>
<b><i>8.9 Information sheet(s) for parent / legal guardian attached</i></b>
No <input type="checkbox"/> Yes <input type="checkbox"/>
<b><i>If no, why not?</i></b>
<b><i>8.10 How will participants be made aware of their right to withdraw at any time?</i></b>
<b><i>8.11 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?</i></b>

**9. EXTERNAL CLEARANCES**

**Investigators working with children and vulnerable adults legally require clearance from the Criminal Records Bureau (CRB)**

<b>9.1 Do ALL experimenters in contact with children and vulnerable adults have <u>current</u> CRB clearance? Please include photocopies.</b>
<b>9.2 If no, explain</b>
<b>9.3 If your research involves external institutions (school, social service, prison, hospital etc) please provide cover letter(s) from institutional heads permitting you to carry out research on their clients, and where applicable, on their site(s). Are these included?</b>
<b>If not, why not?</b>

**10. PHYSICAL RISK ASSESSMENT**

<b>10.1 Will participants be at risk of physical harm (e.g. from electrodes, other equipment)? (See guidelines)</b>
No.
<b>10.2 If yes, please describe</b>
<b>10.3 What measures have been taken to minimise risk? Include risk assessment proformas.</b>
<b>10.4 How will you handle participants who appear to have been harmed?</b>

**11. PSYCHOLOGICAL RISK ASSESSMENT**

<b>11.1 Will participants be at risk of psychological harm (e.g. viewing explicit or emotionally sensitive material, being stressed, recounting traumatic events)? (See guidelines)</b>
No.
<b>11.2 If yes, please describe</b>
<b>11.3 What measures have been taken to minimise risk?</b>
<b>11.4 How will you handle participants who appear to have been harmed?</b>

**12. RESEARCH OVER THE INTERNET**

**12.1 Will research be carried out over the internet?**

No.

**12.2 If yes, please explain protocol in detail, explaining how informed consent will be given, right to withdraw maintained, and confidentiality maintained. Give details of how you will guard against abuse by participants or others (see guidelines)**

**13. CONFLICTS OF INTEREST & THIRD PARTY INTERESTS**

<b>13.1 Do any of the experimenters have a conflict of interest? (See guidelines)</b>
No.
<b>13.2 If yes, please describe</b>
<b>13.3 Are there any third parties involved? (See guidelines)</b>
No.
<b>13.4 If yes, please describe</b>
<b>13.5 Do any of the third parties have a conflict of interest?</b>
No <input type="checkbox"/> Yes <input type="checkbox"/>
<b>13.6 If yes, please describe</b>

**14. ADDITIONAL INFORMATION**

**14.1 [Optional] Give details of any professional bodies whose ethical policies apply to this research**

--

**14.2 [Optional] Please give any additional information that you wish to be considered in this application**

--

**15. ETHICAL PROTOCOL & DECLARATION**

To the best of our knowledge and belief, this research conforms to the ethical principles laid down by the University of Plymouth and by any professional body specified in section 14 above.

This research conforms to the University's Ethical Principles for Research Involving Human Participants with regard to openness and honesty, protection from harm, right to withdraw, debriefing, confidentiality, and informed consent

**Sign below where appropriate:**

**STAFF / RESEARCH POSTGRADUATES**

	<b>Signature</b>	<b>Date</b>
Principal Investigator:	_____	_____
Other researchers:	_____	_____
	_____	_____
	_____	_____

**Staff and Research Postgraduates should send the completed and signed copy of this form to Paula Simson, Secretary to the Science and Technology Human Research Ethics Committee, A106 Portland Square.**

**UG / TAUGHT POSTGRADUATES**

	<b>Signature</b>	<b>Date</b>
Student:	_____	_____
Supervisor / Advisor:	_____	_____

**Undergraduate and Taught Postgraduate students should pass on the completed and signed copy of this form to their School Representative on the Science and Technology Human Ethics Committee.**

	<b>Signature</b>	<b>Date</b>
School Representative on Science and Technology Faculty Human Ethics Committee	_____	_____

**Faculty of Science and Technology Human Research Ethics Committee List of School Representatives**

School of Psychology	Prof Chris Harris (Chair) Prof Judy Edworthy
School of Geography, Earth and Environmental Sciences	Dr Rupert Hodder Dr Sanzidur Rahman
School of Biomedical & Biological Sciences	Dr David J. Price
School of Marine Science & Engineering	Dr Matthew Barlow
School of Computing & Mathematics	Mr Martin Beck
External Representative	Dr Jane Grose
Lay Member	Rev. David Evans

**Committee Secretary: Mrs Paula Simson**

**email: [paula.simson@plymouth.ac.uk](mailto:paula.simson@plymouth.ac.uk)**

**tel: 01752 584503**

## Appendix F. Data Disc Index

---

Supplied with this thesis is a supplementary data disc containing the experiment data and diagrams that were produced during the simulation and subsequent analysis. For clarity an index of the disc is outlined below.

Simulation IDC=10 (Baseline	Intelligent Device Contribution of 10
Simulation IDC=30	Intelligent Device Contribution of 20)
Simulation IDC=40	Intelligent Device Contribution of 30
Simulation IDC=50	Intelligent Device Contribution of 40
	Intelligent Device Contribution of 50
Simulation TDC=0pt75 (Baseline	Token Device Contribution of 0.75
Simulation TDC=2pt25	Token Device Contribution of 1.5)
Simulation TDC=3pt0	Token Device Contribution of 2.25
	Token Device Contribution of 3.0
Simulation MTC=10	Maximum Token Contribution of 10
Simulation MTC=20 (Baseline	Maximum Token Contribution of 20
Simulation MTC=40	Maximum Token Contribution of 30)
Simulation MTC=50	Maximum Token Contribution of 40
	Maximum Token Contribution of 50
Simulation Baseline High Location Multipliers	Location weightings of 2.5, 10 and 30
Simulation Baseline	Location weightings of 2.5, 5 and 10
(Baseline	Authentication Threshold set at 20%)
Simulation AT=60	Authentication Threshold set at 60%
Simulation AT=Var	Authentication Threshold varies with location to 20%, 40% and 60%