2006

Non-Intrusive Subscriber Authentication for Next Generation Mobile Communication Systems

RODWELL, PHILIP MAURICE

http://hdl.handle.net/10026.1/2072

http://dx.doi.org/10.24382/1406
University of Plymouth

Non-Intrusive Subscriber Authentication for Next Generation Mobile Communication Systems

by

PHILIP MAURICE RODWELL

A thesis submitted to the University of Plymouth in partial fulfilment

for the degree of:

DOCTOR OF PHILOSOPHY

School of Computing, Communication & Electronics

In collaboration with

Orange Personal Communication Services Ltd.

January 2006

Abstract

Non-Intrusive Subscriber Authentication for Next Generation Mobile Communication Systems

Philip Maurice Rodwell *B.Eng.(Hons)*

The last decade has witnessed massive growth in both the technological development, and the consumer adoption of mobile devices such as mobile handsets and PDAs. The recent introduction of wideband mobile networks has enabled the deployment of new services with access to traditionally well protected personal data, such as banking details or medical records. Secure user access to this data has however remained a function of the mobile device's authentication system, which is only protected from masquerade abuse by the traditional PIN, originally designed to protect against telephony abuse.

This thesis presents novel research in relation to advanced subscriber authentication for mobile devices. The research began by assessing the threat of masquerade attacks on such devices by way of a survey of end users. This revealed that the current methods of mobile authentication remain extensively unused, leaving terminals highly vulnerable to masquerade attack. Further investigation revealed that, in the context of the more advanced wideband enabled services, users are receptive to many advanced authentication techniques and principles, including the discipline of biometrics which naturally lends itself to the area of advanced subscriber based authentication.

To address the requirement for a more personal authentication capable of being applied in a continuous context, a novel non-intrusive biometric authentication technique was conceived, drawn from the discrete disciplines of biometrics and Auditory Evoked Responses. The technique forms a hybrid multi-modal biometric where variations in the behavioural stimulus of the human voice (due to the propagation effects of acoustic waves within the human head), are used to verify the identity of a user. The resulting approach is known as the Head Authentication Technique (HAT).

Evaluation of the HAT authentication process is realised in two stages. Firstly, the generic authentication procedures of registration and verification are automated within a prototype implementation. Secondly, a HAT demonstrator is used to evaluate the authentication process through a series of experimental trials involving a representative user community. The results from the trials confirm that multiple HAT samples from the same user exhibit a high degree of correlation, yet samples between users exhibit a high degree of discrepancy. Statistical analysis of the prototypes performance realised early system error rates of: FNMR = 6% and FMR = 0.025%. The results clearly demonstrate the authentication capabilities of this novel biometric approach and the contribution this new work can make to the protection of subscriber data in next generation mobile networks.

...for Neeta.

Contents

List of Figures

List of Tables

Notes

Acknowledgments

This research PhD was made possible through the industrial sponsorship of Orange PCS Ltd.[1], and the resources of the Network Research Group at the University of Plymouth[2].

I am deeply indebted to my Director of Studies, and manager of the Network Research Group, Dr. Steven Furnell; whose patience and support, beyond his professional calling, enabled the author to realise an academic achievement far beyond his own vision. A consummate professional and a yardstick by which any Supervisor can be measured.

Thanks must also go to my industrial supervisor, Professor Paul Reynolds, whose original vision set down the foundations for the research and with whose professional experience and expertise the head authentication patents were drafted. A man whose intolerance of adverbs is matched only by his generosity and wit.

Thanks go to Dr. Howard Taylor (Chief audiologist, Derriford hospital, circa 2002) for our discussions on the principles of sound, the anatomy of the human ear and for conducting the audiology (otoacoustic) trials (Section 5.2.3.4). Special mention also goes to my colleagues within the University of Plymouth, notably: Dr. Zaki Achmed for his non-impulsive finite responses to my questions on digital filters; Dr. Nathan Clarke for his cooperation conducting the security survey and discussions on neural-networks; Dr. Paul Dowland for his encyclopaedic knowledge of software engineering and willingness to share it; Dr. Licha Mued for sharing the psychological burden of a research PhD; and Dr. Harjit Singh for his enlightened sole and spirit for research: Akal.

[1] Orange Personal Communications Services Limited, Bradley Stoke, Bristol, UK.
[2] University of Plymouth, Drake Circus, Plymouth, UK.

To my wife I dedicate this work, for her patience and unerring support through the PhD years; no words can ever express my love and gratitude, and no gesture repay her devotion and sacrifice. I would also like to thank my parents for their life investment in me, most recently for my mother's time and family support during the latter writing up phase of the research.

Finally to my children, who have become as much a part of this journey as the research itself: As you take your first steps into the world of academia, I hope that you are inspired by the wealth of knowledge that awaits you and tempted by the new discoveries that await your generation.

Phil Rodwell

Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award.

This research was funded by Orange Personal Communications Services Ltd., and is solely the work of the author.

Relevant conferences were regularly attended, where work was frequently presented, and a number of external establishments visited for consultation purposes. Details of publications are listed in the thesis appendices.

Thesis word count (Abstract and Chapters 1 through 8) : 48,000 words (approx.).

Signed: .....

Date: 4th MAY 2006

Use of Conventions

Within the context of this document the following conventions apply:

Chapter/Section numbering

Syntax: <Chapter #>.<Section #>[.<sub-Section #>][.<sub-Section #>][.<Char>]

- Where <Chapter #> is defined by: 1 # 8
- Where <[sub-]Section #> is any number
- Where <Char> is a lower-case letter in the series: a, b, c…z

Cross-reference(s)

Syntax: ([see] Chapter # | Section #. #[.#. #])

- Where Chapter # is defined by: 1 # 8
- Where Section # is any number
- Where the optional [see] denotes a subject covered later in the thesis.

Figures and Tables

Syntax: Figure | Table <Chapter #|A> - <Figure #>

- Where <Chapter #> is defined by: 1 # 8 or A (denotes Appendix)
- Where <Figure #> is any number

Footnote(s)

Footnote numbering is page independent.

Internet Links

Syntax: (Link: <name>).

- Where <name> is an index to a reference in the list of Internet Links at the end of the thesis.

Reference citation(s) (Harvard)

Syntax: (<Surname> <year>).

- Where <Surname> is an index to a reference in the list of References at the end of the thesis.

Glossary of Abbreviations

#G	-	# Generation (of mobile communications) (see Table 2-1)
3GPP	-	Third Generation Partnership Project
ABR	-	Auditory Brainstem Response
ADSL	-	Asynchronous Digital Subscriber Line
AER	-	Auditory Evoked Response
AuC	-	Authentication Centre (ref. SIM)
bps	-	bits-per-second (ref. PCM)
CCD	-	Charge Coupled Device (digital camera light sensor)
CCTV	-	Closed Circuit Television
CDMA	-	Code Division Multiple Access
CEIR	-	Central Equipment Identity Register (ref. IMEI)
CEPT	-	Conference of European Posts and Telegraphs
CHEOAE	-	CHirp Evoked OtoAcoustic Emissions (ref. OAE)
CPU	-	Central Processing Unit (a microprocessor)
DECT	-	Digital Enhanced Cordless Telephone (range < 300m)
DPOAE	-	Distortion Product OtoAcoustic Emissions (ref. OAE)
EDGE	-	Enhanced Data rates for GSM Evolution
EEPROM	-	Electrically Erasable Programmable ROM (ref. SIM)
EER	-	Equal Error Rate
EIR	-	Equipment Identity Register (ref. IMEI)
ENT	-	Ear Nose and Throat (Medical field)
EOAE	-	Evoked OtoAcoustic Emissions (ref. OAE)
ESN	-	Electronic Serial Number
ETSI	-	European Telecommunications Standards Institute

FAR	-	False Acceptance Rate (see also Glossary of Terms)
FIR	-	Finite Impulse Response (ref. Digital filters)
FMR	-	False Match Rate (see also Glossary of Terms)
FNMR	-	False Non-Match Rate (see also Glossary of Terms)
FRR	-	False Rejection Rate (see also Glossary of Terms)
G3G	-	Global 3rd Generation
GPRS	-	General Packet Radio Service
GSM	-	Global System for Mobile communications *originally: Groupe Speciale Mobile (French)*
HAT	-	Head Authentication Technique
HCI	-	Human-Computer Interface
HSCSD	-	High Speed Circuit Switched Data
HSDPA	-	High Speed Downlink Packet Access
IMEI	-	International Mobile Equipment Identity
IMSI	-	International Mobile Subscriber Identity
INCITS	-	International Committee for IT Standards
ISO	-	International Organization for Standardization
ITU	-	International Telecommunications Union
LBS	-	Location Based Services
MMI	-	Man-Machine Interface (an outdated term referring to an HCI)
MMS	-	Multimedia Message Service
MWIF	-	Mobile Wireless Internet Forum
OAE	-	OtoAcoustic Emission (ref. AER)
OHG	-	Operator Harmonisation Group
OMA	-	Open Mobile Alliance
PCM	-	Pulse Code Modulation (digital sampling technique)

PCS	-	Personal Communications System
PDA	-	Personal Digital Assistant (electronic filofax)
PCN	-	Personal Communications Network
PIN	-	Personal Identification Number
PoE	-	Point of Entry
QoS	-	Quality of Service
RAM	-	Random Access Memory (ref. SIM)
RCA	-	Radio Control Authority
RFID	-	Radio Frequency IDentification (electronic tagging)
RIFF	-	Resource Interchange File Format (Appendix D)
RMS	-	Root Mean Square
ROM	-	Read Only Memory (ref. EEPROM)
SIM	-	Subscriber Identity Module
SMS	-	Short Message Service
SOAE	-	Spontaneous OtoAcoustic Emissions (ref. OAE)
TACS	-	Total Access Communication System (1G Analogue)
TEOAE	-	Transient Evoked OtoAcoustic Emissions (ref. OAE)
TDMA	-	Time Division Multiple Access (2G/GSM)
TMSI	-	Temporary Mobile Station Identifier
UMTS	-	Universal Mobile Telecommunications System
		3G mobile technology for Europe, Japan and North America
WAP	-	Wireless Access Protocol
wav	-	File extension for wavefile format (ref. RIFF, Appendix D)
W-CDMA	-	Wideband - Code Division Multiple Access

Glossary of Terms

Within the context of this document the following definitions are assumed:

Authentication

The act of proving the validity of the *claimed identity* of a user on a system.

(See also the definition of 'Biometric Authentication' in thesis sub-Section 4.2.4.)

Broadband

A bandwidth defined by: 2 Mbps < *Broadband* < 1 Gbps.

Biometric Password

An authorisation code derived from a users distinctive *Physiological* or *Behavioural* characteristics; known as biometric markers.

Continuous

A discrete action occurring indefinitely at either a fixed or variable time interval.

Cordless Handset

A low range mobile telephony device specifically for use in the home. E.g. DECT

Equal Error Rate

The common threshold value where the FAR and FRR of a system are equal.

False Acceptance Rate

The probability that an impostor will falsely pass system authentication: Also known as a *Type II* error (see also FMR).

False Match Rate

Alternative to 'False Acceptance Rate'. Used to avoid confusion in scenarios that reject the claimant if their biometric template matches that of an enrolee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection' (Link: iAfB/ICSA).

False Non-Match Rate

Alternative to 'False Rejection Rate'. Used to avoid confusion in scenarios that reject the claimant if their biometric template matches that of an enrolee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection' (Link: iAfB/ICSA).

False Rejection Rate

The probability that an authorised user will falsely fail system authentication: also known as a *Type I* error (see also FNMR).

Identification

The act of determining the identity of an *unknown* user on a system.

(See also the definition of 'Biometric Identification' in thesis sub-Section 4.2.4.)

Mobile Device

Any hand-held mobile communications device, including though not exclusively: mobile handsets, Personal Digital Assistants (PDA), laptop & palmtop computers.

Mobile Handset

A mobile (cellular) device, designed primarily, though not exclusively, for telephony.

Mobile Terminal

A wireless interface to a distributed communications network: not necessarily a mobile handset.

Mobility

The convenience of accessibility of a distributed communications network via:

- *Terminal* – The ability of a mobile terminal to roam within a distributed network
- *Personal* – The ability of a mobile user to roam within a distributed network.

Non-Intrusive

A service or procedure that is transparent in operation to the system user.

Smartphone

Any electronic handheld device that integrates the functionality of a mobile handset with a personal digital assistant or other information appliance.

Subscriber

The legitimate registered user of: a mobile device, mobile network or mobile service.

User

Any person capable of utilising a mobile device; not necessarily the registered user.

Verification

See Authentication.

Wideband

A bandwidth defined by: 9.6 Kbps < *Wideband* < 2 Mbps.

"Measure what is measurable, and make measurable what is not so."

Galileo Galilei

Chapter 1

Introduction and Overview

1 Introduction and Overview

This chapter introduces the PhD research area, identifies the research focus, specifies the research requirements and objectives and provides a complete systematic breakdown of the thesis with individual chapter summaries.

1.1 The Mobile Telephone

Within a single generation, a vision of personal communications proposed by luminaries such as Arthur C. Clarke (1945) & Carl Sagan (1978), has left the realms of conceptual theory and become an everyday reality; spearheaded by a multi-functional masterpiece of miniaturisation, endearingly referred to, as the 'mobile'.

With, the introduction of the domestic CD in 1985 (Philips 1985), digitised sound was perceived to enter homes en-masse for the first time and the term 'digital' firmly entered the vernacular of the general population. The adoption of digitisation of the human vocal spectrum for telephony application, brought management of the data stream within the control of advancing computer technology and the subsequent convergence of communications and computer technology was inevitable.

The introduction of the Global System for Mobile communications (GSM) in 1991 (CellularOnline 2006a) gave digital telephony the mobile medium it required to appeal to a new technology hungry generation. The implications to the consumer were that the once dumb *shackled* telephone has evolved into a mobile, internationally networked, computing device with excellent processing and storage capabilities. By the early years of the 21st Century, GSM based mobile communications devices represented 78% of the world's digital mobile market and numbered in excess of 1.6 billion (GSM World 2005);

outstripping even the sale of traditional personal computers which themselves experienced excellent annual growth in 2005 of 16% (Sharma 2005).

Figure 1-1 shows the generational evolution of the mobile handset over the last 15 years, from the modern day multi-functional network terminal back to the first rudimentary mobile telephone, as presented by one of Europe's biggest handset suppliers: Nokia.

Figure 1-1 : The evolution of the cellular mobile handset: Nokia brand

The primary selling point of post 2G mobile devices is the plethora of services the hardware enables. Having inherited many of the capabilities of the traditional Personal Digital Assistant (PDA), including: comprehensive address books, work planners and schedulers; current mobile devices offer many functions originally only available on a networked computer, including: email, internet, e-commerce and extensive multimedia capabilities. The latest 'smartphone' mobile devices have evolved into a new generation of combined hardware and services, enabling users to perform video-conferencing, watch live news, weather or sports broadcasts, locate bars and restaurants near to their location and pay for goods with virtual money, locate theatres near to their location and book tickets before receiving live directions to the venue (Link: BBC Mobile Services).

With around 1 in 4 of the world population now in possession of a mobile communications device (CellularOnline 2006b), along with the decentralisation of the modern business environment, current mobile service providers are competing for unprecedented access to hundreds of millions of customers, for whatever post telephony services they care to conceive. It is, however, a disturbing reality that as these services probe deeper into the world of personal consumer data, once the preserve of trusted red-brick institutions, the levels of data protection offered are emerging as secondary to the revenue such services can provide. In fact, in many cases, confidential information is usually only a 4 digit PoE PIN away from prying eyes (CellularOnline 2006c). Depending upon the security awareness of the user and the capabilities of the mobile device, even this basic defence itself, may be rendered ineffective (see Section 3.4.2). Alternate knowledge based security approaches such as ones mother's maiden name or even complex passwords can usually be bypassed fairly easily using established social engineering techniques (Granger 2001). A topical example being the current trend in phishing, the spoofing of legitimate service providers via unsolicited communications, maybe emails or phone calls, in order to persuade a targeted service subscriber to divulge sensitive security details to unscrupulous parties (Link: APWG). This information is then used by a 3rd party to masquerade as the legitimate service subscriber in order to defraud the system.

Mobile devices have consequently become the target of more than the opportunistic thief (Chopra 2002). In the UK alone, 2001 saw in excess of 700,000 mobile handsets stolen (Harrington & Mayhew 2001), leading the government to set-up a National Mobile Phone Crime Unit to specifically target the problem (NMPCU 2003). Even more valuable to criminals who target mobile devices is the data which these devices carry, and owing to their essential networking capabilities, the wider data and services which they have access to (see Section 2.3.6). Eugene Kaspersky, founder of Kaspersky

Labs recently warned that hackers will become increasingly interested as mobile phones proliferate and "...when they get cheap enough, smart phones will become a real problem. It will happen sooner or later" (Kaspersky 2006). In the UK in the year of 2004, identity theft was estimated at £1.3 billion (Home Office 2006) and it would be naive to believe that with no apparent end in sight to either the market penetration of mobile technology, or the advancement of the underlying technology itself, that the size of this problem is going to do anything other than increase.

The growth of mobile networks capacity with the introduction of next generation networks (Section 2.2.3) and services (Section 2.2.3.3) has placed even more emphasis on the mobile device to act as a gatekeeper to both local and network-centric data. The aim of the PhD is to research a novel biometric technique, specifically applicable to the mobile arena, capable of not only offering a more secure Point-of-Entry (PoE) authentication mechanism than the traditional PIN, but subsequently continuously monitoring the authentication status of the user beyond PoE. Continuous authentication, using existing biometric and non-biometric approaches is wholly impractical owing to the intrusive requirement of specific user interaction. Therefore, the proposed solution must be transparent in operation to the user; not interfere or impede normal interaction with the mobile device. In addition, if authentication was managed within the network, rather than the mobile device (Section 2.3.7.3) it has the potential to revolutionise personal mobility, enabling a new level of convenient network accessibility within the mobile community.

Apart from the security implications of subscriber's biometric signature data, the very nature of biometrics themselves, or the measuring of a person's physiology or behaviour (see Chapter 4), constitutes personal medical data and therefore itself should fall under the jurisdiction of established confidentiality data protection protocols.

1.2 Research Requirements

The goal of the research is to investigate, develop and evaluate a novel user authentication system for application in the new generation of personal mobile communication devices with enhanced services. This work is ultimately aimed at addressing authentication issues within the emerging wideband PDA/telephony hybrid devices of post 2nd Generation (2G) networks and encompassed under the umbrellas of 2nd generation wideband (2.5G) and 3rd generation (3G) networks: assigned UMTS (Link: 3GPP) in Europe. To this end, the aim is to develop a technique, which compliments existing mobile equipment and the knowledge-base of existing mobile users. The work draws upon the field of biometrics in order to realise an authentication system that enables transparent and continuous online monitoring; a significant improvement over the current 2nd generation one-time, PoE authentication system.

There are a number of objectives to the research as follows:

- **Research Assessment:** Review current security systems in place within GSM and UMTS based mobile networks and devices and assess the extent to which these systems meet the present and future security needs of the subscriber. Establish the need for improved authentication security within the developing market for advanced mobile services.
- **Conception:** Conceive an original idea for an improved mobile authentication technique addressing any deficiencies identified within the research assessment and drawn from the discipline of biometrics.
- **Development:** Realisation and development of the aforementioned technique to the point of a prototype demonstrator, which can subsequently be used for validation and evaluation of the technique.

- **Validation:** A *Proof of Concept* demonstration of the viability of the technique, for trial evaluation approval, using the prototype demonstrator and cross comparisons with a small sample set of volunteer users.
- **Evaluation:** Statistical evaluation of the technique via an extended trial involving a group of volunteers, over an extended period.

To gain a full understanding of the research requirements, it was necessary to perform a complete review of current mobile security systems, from the inception of GSM in 1991 to the recent introduction of 3rd generation UMTS networks. The review encompasses all aspects of mobile security in parallel with the impact of the offered services, which are the essence of the investment effort into misuse and abuse.

The research subsequently required the inspiration, development and validation of an original form of non-intrusive authentication suitable for continuous application within the mobile communications arena. In order to achieve the objective, development realised an approach incorporating the individual strengths of both physiological and behavioural biometric techniques: a hybrid approach which was later submitted to the UK and US patents offices (Rodwell 2001) and presented in Appendix I.

Upon successful completion of the development stage, the core research was realised within a prototype demonstration and validation tool. For evaluation purposes, the demonstrator was suitably modified for general use, via automating the authentication process and adding appropriate help information, before being released for an extended trial involving a group of volunteers, yielding real-world results. This is essential, if the practicality and effectiveness of the realised technique is to be considered in context.

1.3 Thesis Structure

The thesis can essentially be divided into three main research areas. The chapters covering each of these areas will now be introduced in detail:

- **PhD Research Foundations**

  Chapters 2, 3, 4 introduce and review the foundations to the PhD research.

- **PhD Research and Development**

  Chapters 5, 6, 7 cover respectively; conception, development and evaluation of the PhD core research proposal(s).

- **PhD Research Conclusions**

  Chapter 8 presents and discusses the research conclusions.

1.3.1 PhD Research Foundations

Chapter 2 discusses the results of a review of the evolution of current mobile communications technologies, with an in depth look at the security systems in place to protect users and their property. Current mobile security systems were originally conceived to protect 2nd generation mobile communications networks, specifically the Global System for Mobile communications (GSM), and have remained fundamentally unchanged through the subsequent generation(s) of mobile technology.

The security aspect of Chapter 2 focuses upon mobile subscriber authentication and the approaches employed by the network operators and the hardware manufactures. Security provisions within current mobile telephony based networks are primarily aimed at secure communication: subscriber authentication is achieved via use of a handset serial number and a token smart card containing subscription details; authentication is fundamentally between the token smart card and the mobile network. Subscriber authentication with the

mobile handset relies on a PoE knowledge-based approach, only usually performed at handset switch-on and therefore vulnerable to masquerade attack. Chapter 2 discusses these issues in detail, before identifying some potential technological areas from which solutions may be drawn to overcome essentially what are 1st generation security deficiencies within post 2nd generation and 3rd generation networks.

Chapter 3 presents the results of a public survey investigating mobile users' views towards existing mobile security and subscriber authentication. Participants were asked about their personal experience of mobile fraud or theft. They were also asked their opinion on the protection the mobile handset access control, the PoE four digit Personal Identification Number (PIN), provides for their network subscription. The survey goes on to explore participants usage of existing mobile services and their requirements for future services and the security risks which they may carry. Finally there are a selection of questions on participant's awareness and opinion on a selection of advanced security approaches to authentication, including biometrics and specific mobile related issues.

Introduced in Chapter 2, **Chapter 4** covers the topic of biometrics, including a comprehensive review of the state-of-the-art, and the scope, of current biometric approaches and systems. The chapter investigates market penetration of various biometric techniques and specific system applicability to the mobile arena. The chapter concludes with an extension to the security survey covered in Chapter 3 addressing specifically issues relating to biometrics and advanced authentication. Participants' views on various generic advanced security issues are explored, their awareness of current and emerging biometric techniques and their attitudes towards security issues affecting future mobile technology.

1.3.2 PhD Research and Development

Chapter 5 introduces the Head Authentication Technique (HAT), a proposed solution to the authentication deficiencies introduced in Chapter 2, discussing the technique from conception through to realisation. In order to place the proposed solution in context, a number of alternative approaches are also discussed, two of which are followed up in the research and the others rejected due to feasibility or practicality reasons. As mobile handsets are developed far beyond their simple telephony roots, it is accepted that in practical terms no single approach is appropriate in isolation to protect all mobile services, and that a multi-modal approach to authentication is expected to provide the most comprehensive solution. The successful application of such a system, especially in a continuously monitoring environment, will depend on a comprehensive mobile security framework, capable of managing multiple authentication techniques under differing scenarios.

Chapter 6 covers the finalised methodology of the Head Authentication Technique in detail, as realised through the HAT demonstration tool discussed in Chapter 7. The chapter discusses the HAT operational principles by cumulatively revealing and explaining the discrete stages of the HAT process, with the aid of comprehensive flow diagrams. The chapter also discusses some of the developmental processes which led to the final HAT methodology, explaining and defending the reasoning behind some of the key research direction choices with the aid of empirical data. There is also a section discussing an alternative HAT methodology partly developed in tandem alongside the principle choice, and characterised by a modified yet equally novel biometric data analysis algorithm, demonstrating some of the future research potential of the this novel biometric technique.

Chapter 7 covers the evaluation stage of the research project including the development and operation of a HAT demonstration tool. A group of twenty volunteers, including different sexes, ages and nationalities, was asked to authenticate themselves in a series of HAT trials using the developed demonstration tool. The HAT trials produced twenty sets of biometric HAT samples which were used for system evaluation through post trials analysis. A complete set of results is presented in Chapter 7, which includes a series of graphical outputs demonstrating the authentication performance of the HAT process including:

- how HAT audio spectra from the same user follows a common shape;
- how HAT audio spectra between different users follow a different shape;
- the calculations of the system false-acceptance and false rejection error rates;

1.3.3 PhD Research Conclusions

Finally **Chapter 8** summarises and reasserts the original research problem, before proposing a possible solution: HAT. The research is also critically assessed through sections on research achievements and limitations, effectively defining the operational envelope of the HAT process. The chapter proceeds to identify areas for future work, generally directions where the development of the HAT process was curbed due to available resources, before finally demonstrating the contribution that the research has made to the subject area of biometric authentication in the mobile arena.

A full list of **References** and **Internet Links**, followed by the appendices, containing significant **Public Outputs**, and the research **Patents** is included at the end of the thesis.

Chapter 2

Mobile Communications and Mobile Security

2 Mobile Communications and Mobile Security

This chapter reviews and discusses current mobile technology and the security authentication systems in place to protect users' mobile subscriptions; data link security being outside the scope of the thesis. The chapter highlights potential weaknesses in the current authentication methodology and their increasing relevance to the enhanced services of evolving 2nd generation wideband (GPRS, EDGE) networks, the recently introduced 3rd generation wideband (UMTS) networks and embryonic post 3rd generation broadband (HSDPA) networks.

2.1 Introduction

Cordless and cellular mobile communications devices function via the transmission and reception of signals within the radio frequency bands of the electromagnetic spectrum. Security for these devices must therefore protect three principal areas from compromise: the mobile subscriber, the mobile hardware and the radio link, in equal measure. Security provisions within the current, predominantly 2nd generation, GSM networks addresses each of these security issues as follows: to protect the subscriber from masquerade attack, subscriber authentication is performed via the use of a smart card token; to protect the mobile hardware from amongst other things, spoofing, mobile *terminal* authentication utilises an electronic serial number and to protect the mobile data on the radio link from eavesdropping, strong data encryption is employed.

All of the UK's, major network operators (at the time of writing: Orange, Vodafone, O_2 and T-Mobile, in order of market share), although still heavily involved with 2nd generation technologies, are all actively finalising post 2nd generation wideband

networks. Vodafone, Orange and T-Mobile, are in the process of enabling data communications across their 3rd generation UMTS networks, with Hutchison 3G being the first operator to market with a commercial system known as '3' in March 2003 (BBC News 2003). O2, in association with Nortel, recently completed live tests of their High Speed Download Packet Access (HSDPA) network, with extended commercial field trials scheduled for the second quarter of 2005 (Nortel 2005). Table 2-1 below, maps the history and evolution of mobile technology networks.

Generation		1G	2G	2.5G		2.75G	3G	3.xG
EU Acronym		*TACS*	*GSM*	*HSCSD*	*GPRS*	*EDGE*	*UMTS*	*HSDPA*
Coding Scheme		Analogue	Digital	Digital	Digital	Digital	Digital	Digital
Technology Characteristic		Analogue coding	Digital coding	Multiple time-slots	Packet switching	3G speed over 2G	Advanced Services	IP Core Network
Download Bandwidth (Kbps)	Max	×	9.6	< 115	< 171	< 384	< 2000	< 10000
	Real	×	~ 4	~ 12	~ 40	~ 100	~ 400	> 2000
Frequency (MHz)		900	900/1800	1800	900/1800	900/1800	2000	5000
Switching		Circuit	Circuit	Circuit	Packet	Packet	Packet	Packet
Services	Voice	✓	✓	✓	✓	✓	✓ *(Rich)*	✓ *(Rich)*
	SMS/MMS	×	✓	✓	✓	✓	✓	✓
	Internet	×	✓ *(WAP)*	✓ *(WAP)*	✓ *(WAP)*	✓	✓ *(Rich)*	✓ *(Rich)*
	mMedia	×	×	✓	✓	✓	✓	✓
	GPS enabled	×	×	×	×	×	✓	✓
Availability		1983	1992	2000	2001	2005	2004	> 2006

Table 2-1 : The evolution of cellular mobile communication technologies

The £22.5 billion investment in 3G licenses in the year 2000 (Brown *et al.* 2001), even before any investment in infrastructure (estimated to exceed the value of the 3G licenses, CNN 2001), demonstrates the commercial strength of the current mobile marketplace and the confidence existing major network operators have in the continued development of new mobile technology and the revenue streams that the enabled services will produce.

2.2 Mobile Communications Systems

The evolution on mobile communications technology has produced a rich heritage of revolution and innovation in communications. Table 2-1 introduces key technologies which have shaped the industry today and these will now be discussed in greater detail.

2.2.1 A Basic Mobile Communications Architecture

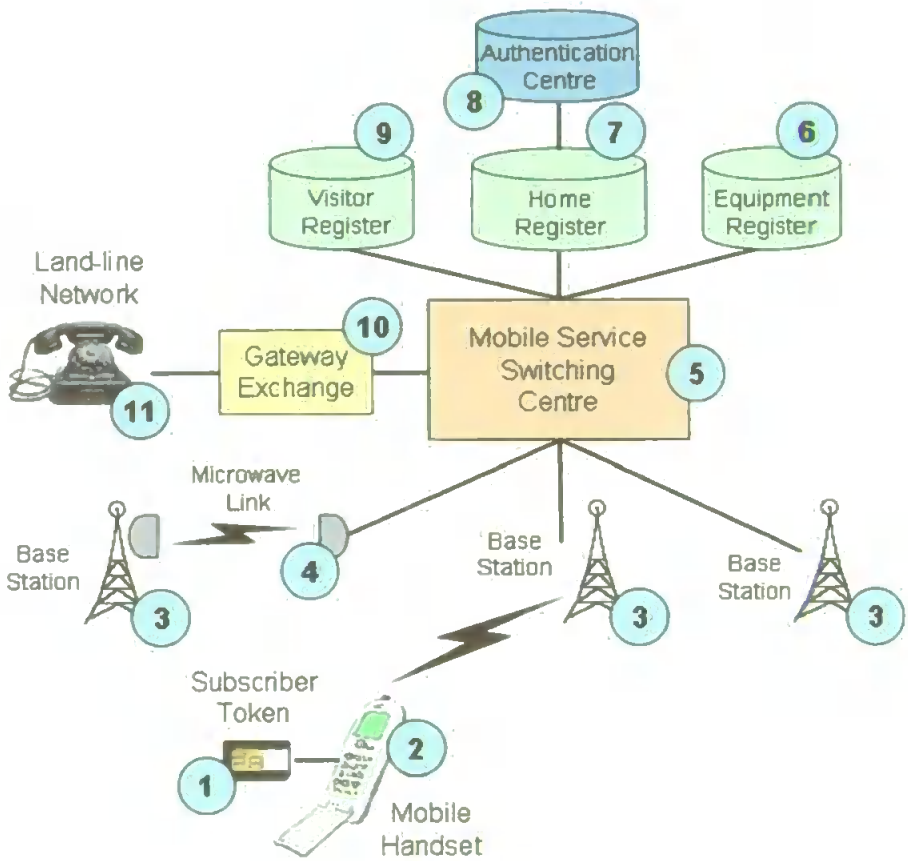


Figure 2-1 : Schematic of a basic mobile communications architecture

Figure 2-1 shows a basic architecture for a distributed mobile communications network similar to the cellular networks in use today and covered in Section 2.2.2. Although not comprehensive, the schematic and associated information provides those readers which require it, with a basic understanding of some of the key elements which come together to form a typical mobile network architecture.

Key to Figure 2-1

① **Subscriber Token**: Network subscriber authentication token (smart card, aka SIM).

② **Mobile Handset**: The physical *terminal* interface to the distributed mobile network.

③ **Base Station**: The interface between the radio link and the mobile network.

④ **Microwave Link**: Employed when base stations are cited in remote locations.

⑤ **Network Switching Centre**: The mobile network *telephone exchange*.

⑥ **Equipment Register**: Database of mobile handsets security status.

⑦ **Home Register**: Database of mobile network subscriptions.

⑧ **Authentication Centre**: Database of authentication and encryption parameters.

⑨ **Visitor Register**: Database for the temporary storage of visiting subscribers.

⑩ **Gateway Exchange**: Switches connections to landline network.

⑪ **Landline Network**: The Public Switched Telephone Network (PSTN)

There follows a simplified explanation and *walkthrough* of the generic mobile communications architecture shown in Figure 2-1. Although an in-depth explanation is beyond the scope of this text, further information on current mobile network architectures can be obtained from their respective governing bodies, which are identified in Section 2.2.2 for 2G and Section 2.2.3 for 3G systems.

The **Mobile Handset** ② containing, the **Subscriber Token** ① (ref. Section 2.3.1, The SIM Card) for network authentication, communicates with the distributed mobile networks' **Base-Stations** ③, over a secure radio link: Table 2-1 shows the link frequencies of current European mobile networks. The **Base-stations** ③ are connected to the **Mobile Service Switching Centre** ⑤, either via cable or **Microwave Link** ④, depending on location and terrain. The **Mobile Service Switching Centre** ⑤ contains a number of operational databases: the **Home Register** ⑦, the **Equipment Register** ⑥ and the **Visitor Register** ⑨. The **Equipment Register** ⑥ (see Section 2.3.2, The IMEI

Code) contains security information regarding the validity of the **Mobile Handset** ② such as, 'has it been reported stolen?' or 'is it compatible with the network?' The **Home Register** ⑦ (see Section: 2.3.5, Mobile Authentication Methodology), contains security information regarding the validity of the network subscription and works together with the **Authentication Centre** ⑧, to validate the subscription of the **Subscriber Token** ①. The **Visitor Register** ⑨ is a special database for the storage of temporary subscription data for persons visiting the network. If all security criteria are met, the **Mobile Service Switching Centre** ⑤ will complete the appropriate connection; either within the host network or transfer the link externally to the **Gateway Exchange** ①⓪, which will route the connection to the traditional **Landline Network** ①①.

2.2.2 2nd Generation Mobile Communications

Although 3rd generation mobile networks and their advanced services are now becoming available to the consumer, 2nd generation technology and its hybrid derivatives still predominate the European mobile marketplace; the most successful of these is GSM.

2.2.2.1 Introduction to GSM

The backbone of the European system for wide area mobile communications came into commercial existence in January 1992, when 'Oy Radiolinja Ab' of Finland, opened the first GSM network for business (CellularOnline 2006a), the standard having been ratified by the European Telecommunications Standards Institute (ETSI) some 3 years earlier, after taking over control from the original GSM working group. It was in fact in 1982, that the Conference of European Posts and Telegraphs (CEPT) first formed the study group known as the Groupe Spécial Mobile (GSM) to research and develop a pan-European public land mobile system: the GSM acronym later being changed, in 1987, to the now familiar and broader ranging: **Global System for Mobile Communications**.

GSM is a narrowband digital cellular radio network, originally developed for mobile telephony. It has experienced worldwide adoption since its introduction in 1992, with 32 networks by the following year and over 570 operational networks by 2004, covering 190 countries supporting 1.6 billion subscribers (GSM World 2005), representing 80% of the world's mobile market and one quarter of the world population. GSM currently provides almost complete coverage in Western Europe, and growing coverage in the Americas, Asia and elsewhere. Although GSM supports extensive international roaming, there are in fact three operational frequencies: 900MHz (Original GSM; Europe), 1800MHz (Personal Communications Network (PCN); Europe) & 1900MHz (Personal Communications System (PCS): North America), and a *tri-band* handset is required, along with a network operator agreement, in order to roam within the three international standards.

2.2.2.2 GSM Services

The first 2nd generation mobile handsets, circa early 1990s, only supported very basic mobile services: telephony, FAX, Short Message Service (SMS). As the technology matured and entered its second decade, the digital nature of GSM and its open standard, has allowed mobile networks operators to develop enhanced data services and enabling technologies like High Speed Circuit Switched Data (HSCSD) and the Wireless Application Protocol (WAP) (OMA 2005). Rudimentary data services, such as text messaging via Short Message Service (SMS), have proved popular, challenging the market dominance of voice based services and although light Internet browsing via WAP has not lived up to industry expectations (vnunet 2000), the trend is still towards Internet connectivity via wireless communications with mobile devices, such as laptop and palmtop computers, through Bluetooth (Link: Bluetooth).

2.2.2.3 GSM Derivative Technologies (2.5G)

The limited bandwidth of a single standard GSM link is 9.6 Kbps. Where this is sufficient for voice and rudimentary data services, the popularity and move towards enhanced data based services have driven the market to develop a number of wideband GSM derivative technologies, see Table 2-1:

- **High Speed Circuit Switched Data (HSCSD)** utilises multiple GSM TDMA time slots, to provide up to 115 Kbps.
- **General Packet Radio Service (GPRS)** offers bandwidths approaching 10 times the standard GSM rate: up to 171 Kbps.
- **Enhanced Data Rates for GSM Evolution (EDGE)** utilises a new air-interface modulation technique to offer data rates approaching 3rd generation performance over existing 2nd generation infrastructure: up to 384 Kbps.

2.2.3 3rd Generation Mobile Communications

As 2nd generation mobile networks entered their second decade, the growth in data services drove the industry to conceive the next generation of wideband networks to deliver advanced wideband services, via suitably enhanced handsets or network interface portals, including video telephony, always on rich Internet and multimedia. 3rd generation (3G) mobile networks offer data rates up to 200 times that of a basic 2nd generation network: the 3G service developed for Europe is known as UMTS.

2.2.3.1 3G Bodies and Standards

The governing body for both GSM and 3G in Europe, UMTS, is ETSI (European Telecommunications Standards Institute), formed in 1988. Along with other international bodies: ARIB (Japan), T1 (USA), TTA (Korea) and CWTS (China), a harmonising

project group was established, the 3rd Generation Partnership Project (Link: 3GPP), holding its first meeting in Sophia, France on 7th December 1998. 3GPP's aim was to co-operate in the production of globally applicable 3G mobile system standards, based on evolved GSM technology. In June 1999, OHG (Operator Harmonisation Group) proposed the evolution of 3GPP, along with the USA's 3GPP2 cdma2000 proposal group, into a harmonised G3G (Global 3G) standard. Another influential body was the Mobile Wireless Internet Forum (MWIF), an international harmonisation association, whose key goal was to influence 3GPP and 3GPP2 into the acceptance and adoption of a single open mobile architecture, independent of the access technology.

2.2.3.2 Introduction to UMTS

The term UMTS was first defined in 1986 as part of the Commission of European Communities (CEC) Research into Advanced Communications in Europe (RACE). Developed by the European Community as a commercial 3rd generation mobile technology, UMTS was adapted by the International Telecommunications Union (ITU) standards effort as part of IMT-2000 (International Mobile Telephone for the year 2000)[1] (ITU 2001). UMTS is based on the core network architecture of GSM, allowing current GSM network operators to protect their infrastructure investments and combines evolved current technologies with new developments in the field. UMTS frequencies were allocated at the World Radio Conference in Malaga (WRC-92) in February 1992. In addition to Europe, UMTS is the interpretation of 3G adopted by Japan and North America. One of UMTS's core developments was its packet-based wideband CDMA technology, allowing global roaming and always-on networking facilities. The technology offers data transmission rates far in excess of the 9.6 Kbps of basic 2nd generation GSM technology, providing up to (best case):

[1] IMT-2000 replaced the FLPMTS (Future Land Public Mobile Telecommunications System) initiative.

- 144 Kbps in macro cellular environments; Roaming: ~10km.
- 384 Kbps in micro cellular environments; Building: ~100m.
- 2000 Kbps in Pico cellular environments; Room: ~10m.

UMTS currently represents the ultimate evolution of commercially available public access mobile telephony aligned with associated mobile data services: Richardson (2000) summarised UMTS as "a revolution of the air-interface, by an evolution of the core network."

The final quarter of 2004 saw strong growth in the demand for UMTS 3G handsets in Europe, rising to 16 million subscribers across 60 networks, a 60% increase on the 10 million subscriber milestone set in September 2004 (UMTS Forum 2005).

2.2.3.3 3G (UMTS) Services

The availability of services that meet genuine market requirements are accepted as the key to the success of 3rd generation technology. "Unlike 2G, where services were specified within the standard, central to the concept of 3G are services' capabilities and toolkits – which enable the creation of customised, operator-specific services to drive new revenues streams" (Watson 2001). Further research commissioned by the UMTS Forum (2003) showed that, even at a conservative estimate, 3G services represent a cumulative revenue potential of one trillion US dollars for mobile services providers' between now and 2010. How big is the 3G services market expected to be by 2010? A total of 2.25 billion mobile subscribers (both 2G and 3G) are being forecast, of which more than 28% are predicted to be subscribers to 3G enabled networks.

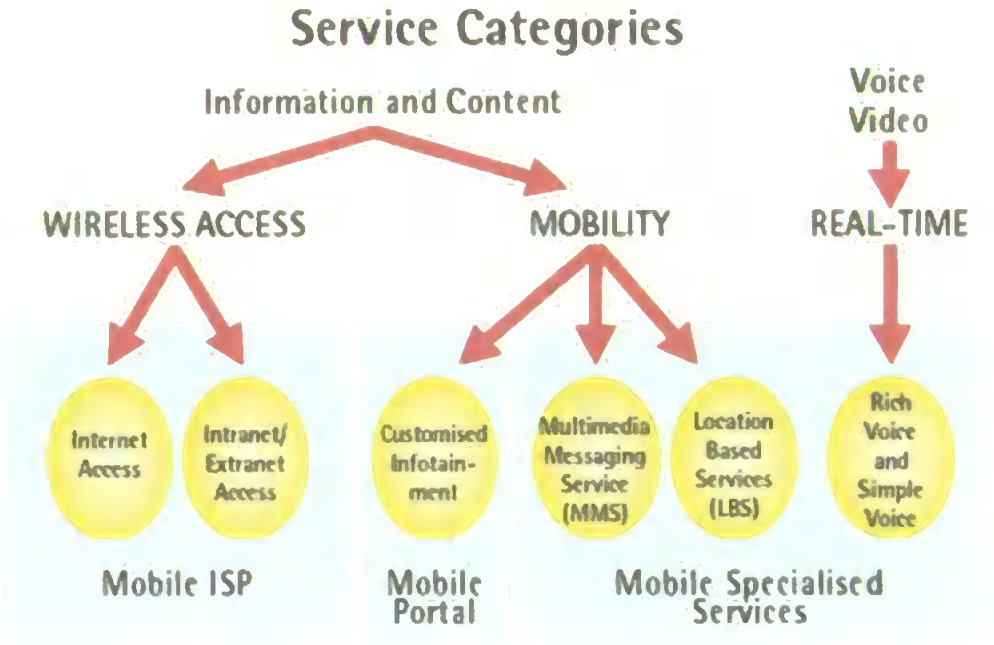


Figure 2-2 : 3G Services framework

What will 3G services be? Services are expected to evolve in fundamentally three different directions: Personal Communications; Wireless Internet and Mobile media. Out of these three areas, the UMTS Forum defines a clear structure of six service categories, illustrated in Figure 2-2, for discussing, planning and reporting on services and applications for 3G over the next ten years (UMTS Forum 2003). The services are:

- **Multimedia Content**

  These include: live video, ore-recorded video clips, music (mp3s) and games formatted for a mobile handset.

- **Multimedia Messaging**

  A development of the popular 2nd generation SMS text only service that enables: video clips, music or graphics to be sent to another mobile handset.

- **Internet Access**

  A *rich* Internet service, not the *light* browsing environment of the 2nd generation WAP service, which proved unpopular on introduction.

- **Instant Messaging**

  A mobile version of the popular real-time PC text messaging service.

- **Location Based Services**

  Utilising the global positioning capabilities of 3G. Services could include directions from the subscriber's current location to, for example, the nearest fuel filling station, cinema or restaurant.

- **Rich Voice**

  An enhanced rich voice telephony service. In addition to improved audio quality, services include: Presence, the ability to see if a user is currently 'on-line' to receive communications; 'Push-to-talk', a simultaneous group communications service, similar to the service offered by private radio networks.

Conservative forecasts predict that total service provider-retained revenues for 3G services in 2010 will reach US$322 billion. Of those revenues, 66 percent will come from 3G-enabled data services (VisionGain 2005). Figure 2-3 shows the predictive cumulative revenue potential for mobile services providers between now and 2010 is estimated to rise in excess of one trillion US dollars.

Services like e-mail and Web browsing are expected to have little direct revenue potential, as users will expect them to be included as part of their service package at no additional charge; their benefit comes mainly from their role as drivers of traffic. The single largest revenue opportunity is expected to come from multimedia based services by virtue of its low cost and mass-market appeal, contributing US$86 billion in 2010. It is also predicted that much of the additional revenue will be generated from increased mobile usage, driven by new services, rather than through new sources of revenue.

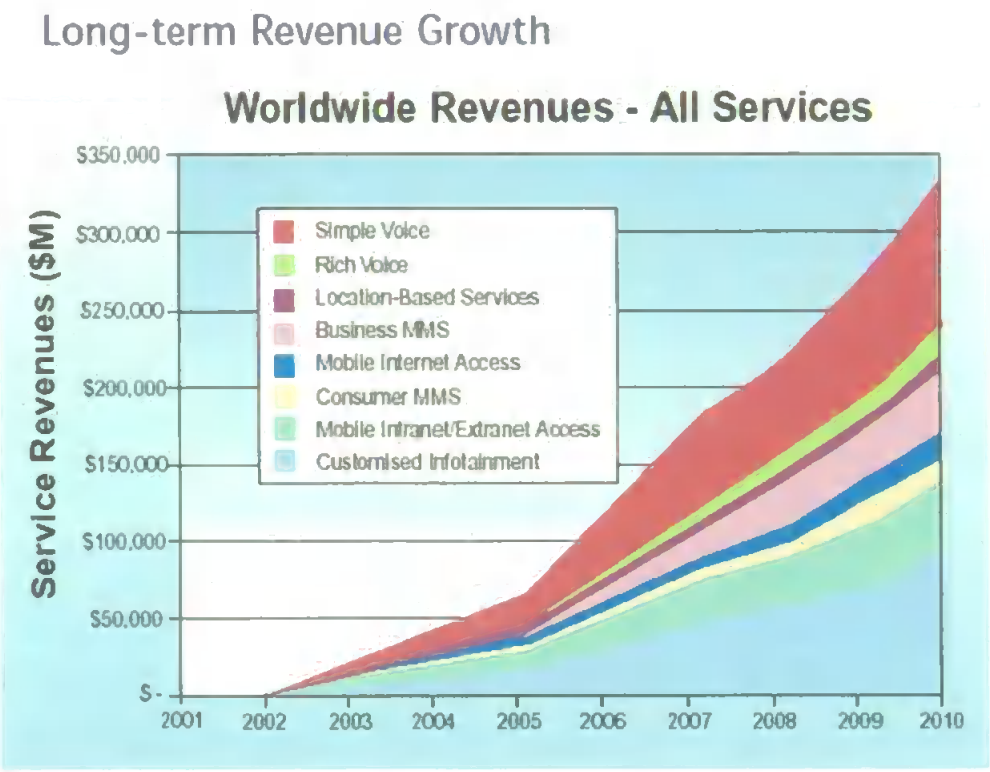


Figure 2-3 : Worldwide revenues forecast from all 3G services

2.2.4 Beyond 3rd Generation

It has been shown that mobile communications is evolving rapidly and the drive towards broadband mobile data communications shows no signs of slowing. Although the introduction of the first 3G mobile network marks a milestone in both data rates and offered services, when compared to the field of distributed computing networks, such as Wi-Fi, mobile telephony based technology is still over one hundred times slower. It is not unexpected therefore, that development of cutting edge mobile technology is continuing apace, before 3G has even firmly established itself within the market place. In order to further strengthen the presented case for enhanced authentication security, where enhanced services are intimately linked to enhanced data rates, two post 3G approaches currently in development are briefly acknowledged below.

2.2.4.1 High Speed Downlink Packet Access

High Speed Downlink Packet Access (HSDPA) is a packet-based data service based on an evolution of the core 3G architecture. HSDPA uses a new modulation technique which increases peak downlink data rates by to up to 5 times the peak data rate of the most advanced 3G networks; improving spectral efficiency. The Third Generation Partnership Projects (Link: 3GPP) standards, Release 4 specifications provide IP support enabling provision of services through an all-IP core network. The Release 5 specifications focuses on HSDPA to provide initially up to 10 Mbps to support packet-based multimedia services (3GPP 2005).

The increased bandwidth will enable network operators and service providers to offer their advanced services at lower costs, owing to the higher number of users supported by a single carrier and with greatly reduced delays over the air interface. This will also enable new time critical services, like streaming high-definition video.

In essence the benefits to the HSDPA user will be:

- Higher data rates
- Shorter service response times
- New services
- Better availability of existing services
- Improved overall quality of service

2.2.4.2 4th Generation

The Ministry of Internal Affairs and Communications (MIC), in addition to the ITU working group 8F, are actively addressing the issues for the 4th generation of mobile communications (4G), like the international coordination of frequencies, spectrum harmonisation and standardization. A coarse timetable has been set of establishing the necessary 4G technology for mobile communications systems by the end of 2005 and putting a system into practice by 2010.

One debate is currently tackling the issue of whether 4G will be an evolution of existing 3G standards or a revolutionary development. What is likely is that 4G will be a packet-switched technology offering bandwidths similar to the broadband distributed computer networks of the 2G mobile era. Based on Ethernet and wireless standards of around 100 Mbps, bandwidths 10,000 times that of current 2G technology are being proposed. This would enable the sending and receiving of high quality streaming video, even whilst roaming at high speed across cell boundaries, something even the most advanced currently proposed technologies, such as HSDPA, cannot do. Although 4G is broadly based on similar goals to 3G, with an emphasis on bandwidth enabled services rather than purely high data rates, one specific target area for improvement is interoperability between hardware and networks, via technologies such as 'software defined radio'. This will enable subscribers to freely roam across networks utilising various different mobile interfaces without suffering any loss in quality of service.

These proposals present a very strong case for not only an enhanced subscriber authentication system, but also a network-centric security system capable of enabling the proposed personal mobility criteria discussed in Section 2.3.7.3.

2.3 Mobile Security

Introduced in Section 2.1, GSM authentication is achieved on two separate levels, authentication of the mobile subscription and authentication of the mobile hardware, as follows:

- **Mobile subscriber authentication** is achieved through use of a token-based, *Subscriber Identity Module* held on a multi-standard smart card.
- **Mobile terminal authentication** is achieved via issuing the mobile terminal (handset) with an *International Mobile Equipment Identifier* at point of manufacture, uniquely identifying the hardware on the network.

These two approaches to mobile authentication form the minimum[1] standard for all post 2nd generation mobile handsets and they will now be reviewed and discussed in depth.

2.3.1 The SIM Card

The Mobile Station (MS) consists of the Mobile Equipment (ME, the handset) and a smart card containing a micro controller, the **Subscriber Identity Module** or SIM.

GSM was the first international mobile communication system to employ a smart card based SIM as a secure device for the authentication of a user subscription. The SIM contains subscription and security related data as well as user and/or network operator specific data. In addition the SIM can contain operator specific *applications* via the SIM Application Toolkit[2]: this service is completely separate from the GSM functionality of the SIM. A schematic breakdown of a generic SIM is included in Appendix A.

[1] Hardware manufactures and/or Network-operators may augment the minimum authentication standard with additional security measures, such as a biometric fingerprint scanner (see Section 4.3.1.1).
[2] The SIM Application Toolkit was originally integrated into the GSM standards in Release 96.

2.3.1.1 SIM Formats

SIMs shown actual size

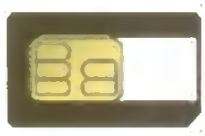


Figure 2-4 : Plug-in SIMs

The Sub Technical Committee SMG9, established in 1994 as the successor of the Subscriber Identity Module Expert Group (SIMEG) itself founded in 1988, defined three formats of SIM. The first and original specification was for an integrated circuit card, employing Surface Mount Device (SMD) packages and having a credit-card format: the ID-1 SIM. Aware of the inevitable size reduction developments of the ME, SMG9 also defined a second smaller *semi-permanent* plug-in SIM for those units unable to accept an ID-1 SIM. This SIM was obtained by removing the excess plastic from an ID-1 SIM. The plug-in SIM is 25mm x 20mm and normally installed behind the battery as opposed to being slotted externally.

An alternate specification proposed an integral SIM, a part of the ME itself. Although more reliable than the plug-in SIM owing to the removal of the SIM-ME interface, it introduced network operator security problems related to the utilisation of operator specific algorithms. It would be difficult, if not impossible, for network operators to use their own security algorithms and keep close control over secret keys and other operator specific security data without a dedicated security module. It was also believed that non-

specific mobiles would open the market for manufacturers reducing trade barriers. It is interesting however, that the USA took a different view for their PCN network, universally adopting the integral SIM.

Current market forces are also behind a drive for a Third Form Factor (3FF), which was recently approved at a plenary meeting of the ETSI Smart Card Platform project (ETSI 2003). Essentially, with the development of smaller and smaller handsets, the point will eventually be reached where the plug-in SIM card occupies too much volume in the mobile device, especially in those devices whose primary purpose is not mobile communications, i.e. miniature digital cameras or watches. The new card is proposed at half the size of the existing card, with the majority of the remaining excess plastic cut away, whilst leaving the contact area unchanged. In this way, the change will have minimal effect on the established standard and not affect existing chip size performance.

2.3.2 The IMEI Code

The **International Mobile Equipment Identity** (IMEI) is a unique 15-digit code assigned to every GSM and UMTS mobile handset at point of manufacturer, by the Global Decimal Administrator (GDA), identifying the Mobile Equipment (ME) or hardware as opposed to the subscriber to the network. It was initially produced for type approval reasons so that out of specification mobile handsets may be removed from a mobile network. The IMEI constitutes sensitive information, being the mobile handsets unique electronic serial number. This form of identification is analogous to the Electronic Serial Number (ESN) of 1st generation (1G) systems, such as AMPS. A historical[1] breakdown of the IMEI code is provided in Appendix B.

[1] The IMEI code has undergone some evolutionary changes since its introduction in 1992.

A list of all the mobile handset IMEIs on an operator network is stored in a central location known as the Equipment Identity Register (EIR). This enables, among other things, a handset reported stolen to be blocked from further use in the network; assuming that the networks infrastructure contain the necessary routines for checking the IMEI number against the central blocking register. The status returned in response to an IMEI query to the EIR is one of the following:

- **White Listed:** The handset is not considered suspicious

  The handset is allowed to connect to the network.

- **Grey Listed:** The handset is under observation for possible problems.

  The handset is allowed to connect to the network.

- **Black listed:** The handset has been reported stolen, or is not type approved.

  The handset is denied access to the network.

A Central Equipment Identity Register (CEIR) is operated by the GSM Association in Ireland, allowing GSM network operators to share their individual lists of IMEIs. (Link: GSM Association). The CEIR lists are automatically updated on a daily basis and at the same time local EIRs download the aggregated lists for their own use.

A handsets IMEI code is not kept secret from the user. It can normally be found on the retail packaging and on the handset itself, normally on a self-adhesive compliance label under the battery. It is also possible to display the IMEI by dialling the code *#06#.

2.3.2.1 IMEI Black Listing

A *black-list* contains the equipment identities, or IMEIs, of handsets barred from using the particular network: handsets reported lost, stolen or otherwise unsuitable for use. In October 2002, in an attempt to curb the rise in handset abuse, network operators started

sharing their black-lists within the GSM Associations CEIR in an attempt to curb the rise in handset abuse (GSM Association 2002).

2.3.2.2 Reprogramming the IMEI: The Mobile Reprogramming Act, 2002

It is not a secret that the IMEI of a mobile handset can be changed relatively easily. This is due to the fact that the GSM specification does not explicitly exclude re-programming of the IMEI by authorised individuals. This is quite serious from a security perspective, as this places the IMEI in firmware where it is ultimately vulnerable to abuse. This is in contrast to the data encryption/ciphering keys, which are masked directly into hardware at the point of manufacturer, denying any possibility of software alteration.

In an attempt to curb abuse of the system, standards for improved IMEI Security were drafted and agreed by manufacturers and ETSI members at the ETSI TC SMG#30 Plenary meeting (ETSI 1999). Their amendment policy statement proposing:

> "*The IMEI shall not be changed after the ME's final production process. It shall resist tampering i.e. manipulation and change, by any means (e.g. Physical, electrical and software)*".

This has led to **The Mobile Reprogramming Act 2002**, which came into force on 1st April 2002. The Act states that it is now a criminal offence to "Offer, change or reprogramme any mobile phone from any network which changes its designed purpose to allow it to unlock or to change the IMEI Number": the act carries a maximum penalty of 5 year imprisonment. The Act does not however include the unlocking of a mobile handset from a designated service provider, known as SIMLock deactivation, unless it includes changing the IMEI or other identifying features being changed or removed.

A brief search on the Internet however, demonstrates that it is still relatively easy to find IMEI firmware reprogramming utilities for mobile handsets, showing that the system is still openly abused, see Figure 2-5.

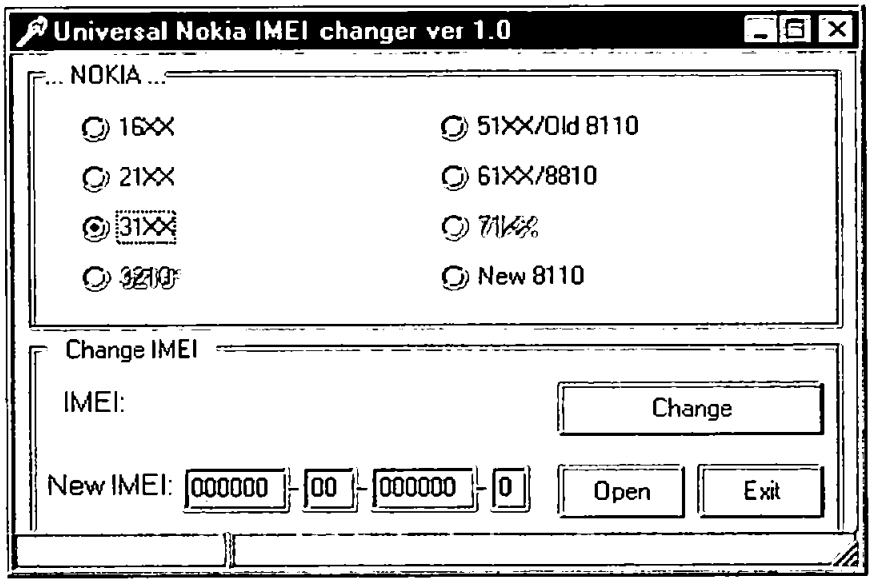


Figure 2-5 : Example of an IMEI reprogramming utility

2.3.2.3 Subscriber Identity Confidentiality (IMSI and TMSI)

Subscriber identity authentication allows mobile subscribers to originate calls, update their location, etc, without revealing their International Mobile Subscriber Identity (IMSI) to an eavesdropper on the radio link. It thus prevents location tracing of handsets by listening to the signalling exchanges on the radio path. All mobiles and networks must be capable of supporting the service, though its use is not mandatory.

Mobile Country Code (MCC)	Mobile Network Code (MNC)	Mobile Subscriber Identification Code (MSIC)
3 digits	*2 digits*	*10 digits*

Table 2-2: Format of the IMSI

In order to provide the subscriber identity confidentiality service it is necessary to ensure that the IMSI, or any information which allows an eavesdropper to derive the IMSI, is not normally transmitted 'in-clear' in any signalling message on the radio path. The mechanism used to provide this service is based on the use of a temporary mobile subscriber identity (TMSI), which is securely updated after each successful access to the system. Thus, in principle, the IMSI need only be transmitted in clear over the radio path at registration. In addition, the signalling elements which convey information about the IMSI are enciphered.

The TMSI updating mechanism functions in the following manner. For simplicity, assume the MS has been allocated a TMSI, denoted by $TMSI_o$, and the network knows the association between $TMSI_o$ and the subscriber's IMSI. The MS identifies itself to the network by sending $TMSI_o$. Immediately after authentication (assuming this takes place), the network generates a new TMSI, denoted $TMSI_n$, and sends this to the MS encrypted under the cipher key K_c. Upon receipt of the message, the MS deciphers and replaces $TMSI_o$ by $TMSI_n$.

2.3.3 The User PIN – Real Subscriber Authentication

Subscriber authentication within current mobile network architectures is limited to the authentication of the SIM (also see Section 2.3.5) which may or may not be in the possession of the SIMs legitimate subscriber; handset authentication via the IMEI is not a subscriber issue. The only tangible security system existing between the SIM and the legitimate subscriber is the user's SIM access Personal Identification Number (PIN); see Figure 2-6. The user PIN is the first line of defence against both casual, opportunistic unauthorised use and more serious pre-meditated masquerade attack. The PIN provides

a personal authentication check at the mobile handset, restricting open access to the SIM card and therefore the network; the onus on PIN activation being in the hands of the subscriber. With the intrusive nature of this security technique (i.e. requires conscious subscriber interaction) it is not uncommon to find subscribers actually choosing to leave the option disabled; this issue is investigated in greater depth in Chapter 3.

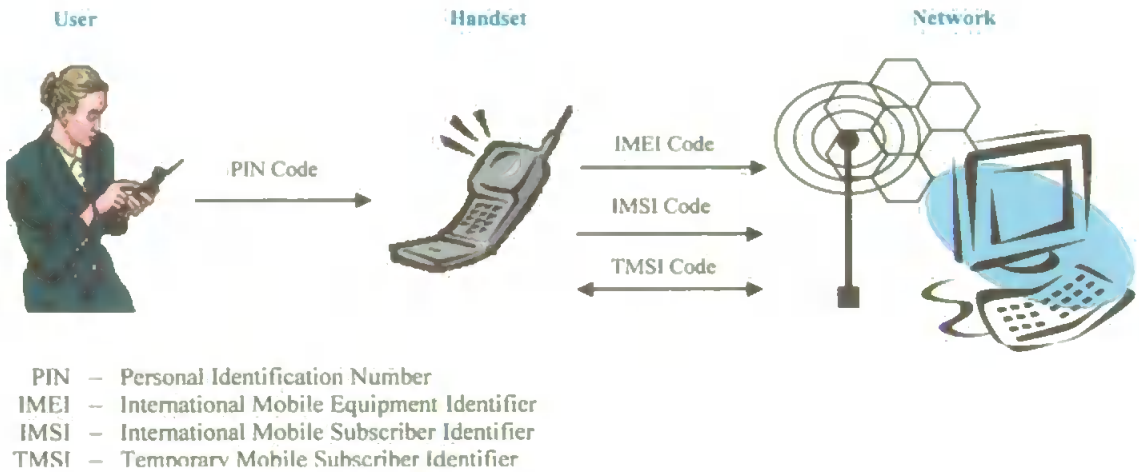


Figure 2-6 : The mobile telephony authentication chain

Although offering a relatively secure form of protection in terms of a brute force attack, offering normally 4 digits, with restricted attempts, the traditional subscriber PIN remains a Point-of-Entry (PoE) technique, triggered only when the handset is brought out of standby. If a handset is left in active mode, the PIN offers no handset protection whatsoever. Some handsets do offer an additional PIN facility to lockout the keypad after a specific time period, but generally this feature is limited to prevention of accidental activation rather than a security feature, with a simple two key access. In essence, the PIN authentication technique remains one of the primary security issues that needs to be addressed and improved upon in order to protect the enhanced services data of next generation wideband and broadband networks. Current mobile authentication therefore depends on two things:

- the PIN facility being activate;
- the user not inadvertently compromising the PIN protection themselves.

In a similar manner to traditional passwords in desktop IT systems, the PIN is based on a secret knowledge approach and is therefore inherently vulnerable to subscribers compromising their own security. This can be achieved by a user either selecting an inappropriate value, such as 1234, transferring or sharing the knowledge with others, or simply writing it down (Lemos 2003, Jobusch and Oldehoeft 1989). In addition, the secret knowledge approach is not strictly unique to any particular subscriber, leaving the technique openly vulnerable to masquerade attack.

2.3.3.1 Bypassing a handset's PIN code

In a similar approach to compromising a handsets IMEI, software to break mobile handsets PIN codes can be found relatively easily over the Internet in downloadable pirate versions. WinTelsa, for example, is a Nokia handset utility, designed to be used in authorized Nokia repair centres, for among other tasks, the recovery and maintenance of handset security data including the PIN. The very existence of such utilities represents a security risk: WinTelsa is already available illegally over the internet.

Examples have also been found where a mobile handset has been physically opened and hard-wired in order to bypass the PIN protection altogether. By inspecting the enlarged section of the mobile handset's main circuit board, illustrated in Figure 2-7, notice the multiple thin trailing wires around the ICs (Integrated Circuits) effectively 'hot-wiring' the board (Geissler 2001).

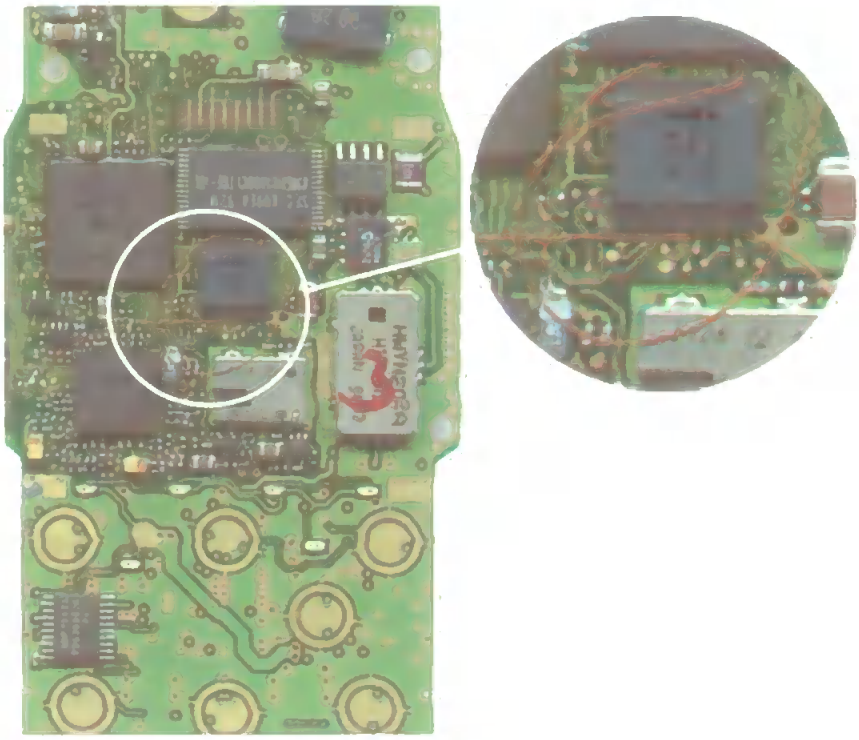


Figure 2-7 : A mobile handset modified to bypass the PIN

2.3.3.2 Enhancing Authentication Security

Recognising the security weaknesses of the PIN, highlighted in Section 2.3.3, some manufacturers have tried to address the issue by introducing some form of truly personal authentication; biometric authentication. In 2002, Sagem released the first mobile handset to incorporate a biometrics (see Chapter 4) authentication approach (Sagem 2000): the Sagem MC959ID (Figure 2-8) incorporated a built in fingerprint sensor. Although, the device seemed to mark a turning point in the market, acceptance has been slow and currently only NTT DoCoMo of Japan offer a similarly equipped device (NTT DoCoMo 2004): the Fujitsu F505i (Figure 2-9). Although fundamentally more secure than existing authentication approaches, the system still suffers the major drawback of requiring conscious subscriber interaction with the mobile device: it is therefore only suitable for PoE protection of mobile hardware or services.

Figure 2-8 : The Sagem MC 959 ID mobile handset (*ST/Upek* fingerprint sensor)

Figure 2-9 : The Fujitsu F505i mobile handset (*Authentec* fingerprint sensor)

2.3.4 3rd Party Security

An already established Internet trend is for service providers to enforce their own specific security safeguards, usually some form of knowledge-based (password) authentication system. In a mobile context, this security technique would reside after the standard security provided by the mobile handset and somewhere between the network and the specific service access point. This approach is especially relevant to separately billed services such as mobile e-commerce. With the convergence of mobile and land based services and the introduction of rich web browsing, provided by the wideband next generation systems, this trend is certain to predominate for the short term.

Looking to the future, in practice, a hybrid approach is likely to represent the most appropriate solution, where a security management system determines and maintains the most efficient security at the least expense on system transparency, from an available cache of security approaches, techniques or protocols.

2.3.5 Mobile Authentication Methodology

Anyone who uses a mobile handset is susceptible to masquerade attack and the subsequent compromise of personal and potentially sensitive data. Authentication is the corroboration that an entity is the one claimed and in mobile terms, this translates to the verification of the identity of the SIM registered to a subscriber. The design of the GSM authentication and encryption schemes is such that this sensitive information is *never* transmitted over the radio channel.

The main entities responsible for the authentication of a subscriber to a network are the subscribers SIM and the Authentication Centre (AuC) of the home network. Both

contain the operator specific one-way authentication algorithm (A3), and a secret authentication key K_i, unique to the users SIM subscription. The authentication process employs a challenge-response protocol/mechanism between the AuC, a part of the Home Location Register (HLR) and the SIM, using non-predictable numbers.

When the home network receives an authentication request, and established the *claimed* identity of the SIM, it transmits a non-predictable number RAND as a challenge to the MS. The ME passes this number to the SIM, which computes the *response* SRES to this *challenge* using the algorithm A3 using the arguments RAND and the key K_i stored in the SIM. The response SRES is then transmitted back to the network, where it is compared with the value pre-computed by the network using the same network algorithm A3 and the same arguments RAND and the key K_i associated with the claimed identity of the subscriber. The MS is granted network access only if the value generated by the SIM and transmitted by the ME is identical to the value generated by the home network; i.e. subscriber authentication is approved.

Accompanying the challenge-response pairs calculated in the HLR/AuC is a new 64 bit cipher key K_c. This is computed using the key K_i and the same non-predictable RAND number with a new operator specific algorithm A8. The purpose of enciphering is to ensure the privacy of the subscriber's information over the radio interface. A discussion of ciphering is beyond the scope of this thesis.

Functional descriptions of security aspects are contained within Technical Specification, GSM 02.09 (1998), with security related network functions within Technical Specification, GSM 03.20 (1999) (Link: ETSI).

2.3.6 3G (UMTS) Security Drivers

It is sensible that the sensitivity of information associated with the services of a given network should be commensurate with the levels of protection inherent in that network. The proposed services of wideband 2G and 3G networks (Cox 1997) require increased amounts of specific user data. This data will, at least, represent sensitive information, the user's current location for example and potentially highly confidential information, financial details or third party authentication codes. These services demand more secure authentication systems to protect the information in the event of a masquerade attack.

The security functions incorporated into 3G (UMTS) are fundamentally based on those established with 2G (GSM), even when considering the enhanced services of 3G. Inherited security functions have generally been improved upon, like a stronger air-interface encryption algorithm and where new security features exist, they are focused around stronger protection and storage of the data stream. There is no specific improved subscriber authentication aspect to the new security architecture.

The main security elements inherited from GSM are:

- Authentication of subscribers via secret knowledge
- Authentication of handsets via removable SIM
- Subscriber identity confidentially
- Radio interface encryption

Security elements new to UMTS are:

- Security against using false base stations with mutual authentication
- Encryption extended from air interface only to include Node-B to RNC
- A mechanism for upgrading security features

Security data in the network to be protected in data stores and while transmitting ciphering keys and authentication data in the system

The security needs of UMTS are covered by standards drawn up by its governing bodies (3GPP 1999), with work progressing within five feature groups (3GPP TS 33.102):

- Network access security

  Secure access to 3G services: protecting the wireless link

- Network domain security

  Secure exchange of signalling data: protecting the wired link

- User domain security

  Secure access to MSs

- Application domain security

  Secure exchange of application data

- Visibility and configurability of security

  Features to continuously monitor and report the security state of the device and also set the security dependence of the device

Considering the attention 3G enabled devices are currently receiving and the new revenue streams covered in the previous Section, 3G is attracting a great deal of interest from the criminal element, in a similar way to the public Internet. With services suggested including medical records data, e-commerce, and online banking, an improved level of subscriber authentication is not only recommended, but a necessity. The always-on Internet service further demonstrates the need for not only enhanced authentication, but a continuous monitoring scheme capable of detecting an intruder at the earliest possible stage.

On a typical 2nd Generation GSM handset, the consequences from theft or impostor access can be broadly grouped into two categories:

- **Financial loss**, as a result of the thief making calls at the legitimate subscriber's expense (depending upon the policy of the operator, these losses may not be passed on to the subscriber once the handset is reported as stolen).
- **Breach of personal privacy**, as a result of subscriber contacts' details being stored in the handset; although it is acknowledged that this is a limited amount of information, the disclosure of which would not normally be considered highly sensitive. Stored text messages may potentially have more significance, but would not generally represent a significant body of information.

When considering the nature of a 3G devices, however, the potential consequences become far more severe. The inevitable convergence of current mobile telephony devices with PDA style devices, in addition to the novel services, 3G itself will spawn, presents a completely different security picture. An always-on 3G mobile device can store, in addition to a phonebook:

- full contact details of friends, business colleagues and associates (Microsoft Outlook style contact lists can contain extensive personal contacts information, including spouse details, anniversaries etc.);
- personal financial details enabling mobile e-commerce (m-commerce);
- electronic certificates for digital signatures;
- email account details and history archives;
- miscellaneous information of a commercially sensitive or private nature (e.g. entered into a personal scheduler or simply-plain text notepad documents);
- Possible medical information enabling telemedicine.

2.3.7 Terminal vs. Network-centric Security

An important issue in the subscriber authentication debate is whether future security authentication and monitoring systems and/or their enabling data, should reside within the mobile handset or within the operator network; or perhaps a hybrid of the two based on, at least, a security weightings for the required service.

Although UMTS, similar to GSM, shares the concept of a home network, the 'universal' aspect suggested in the name is based upon roaming between operators to suit the service requirements. This raises a number of important issues, not least of which being that any future security system designed to protect the enhanced services of wideband mobile networks, needs to transcend the technological barriers of both the systems software and hardware, both nationally and internationally, raised by the different operator networks.

2.3.7.1 Terminal-centric Security

Considering first the terminal-based approach, where a subscriber's security profile or perhaps a *biometric template* are held within the mobile terminal (handset), or more likely within the mobile handsets SIM. This places responsibility for the security of any sensitive authentication data and consequently security of the network portal, in the hands of the subscriber. Although from an operator's perspective, this negates the need for specific government legislation on data-protection of potentially uniquely personal subscriber data or additional network server security to protect such data, ensuring sufficient protection from abuse in such a system may be difficult, if in not in practice, impossible.

A terminal-centric security based technique would perform and maintain the integrity of its chosen authentication approach completely within the mobile handset. One major advantage to this approach, relevant to the current predomination of 2nd generation networks, is that the technique would not be a burden on network bandwidth; this will be far less of an issue in post 2nd generation networks. Subscriber authentication can also be performed completely independent of link/bandwidth availability, a potentially important issue considering the convergence of mobile with PDA style devices.

There are a number of hardware issues relevant to the terminal-centric solution also worth introducing. Firstly, additional authentication cycles, will require additional processing within the mobile handset, requiring a more powerful handset CPU if the authentication process is not to impact on the normal operation of the handset. Of course, this would also have an associated toll on the handsets battery pack and subsequent recharge interval, in addition to operational temperature criteria.

2.3.7.2 Network-centric Security

There are some very strong arguments for introducing a network based security system, in fact some operators have shown reluctance to consider anything less; i.e. that placing security into the handset and effectively the control of the subscriber, is inherently insecure from the offset. The justification for this approach is not the flexibility offered by enhanced personal mobility or the costing of the mobile handset, although these are certainly important issues, but the inherent insecurity of any network access system security outside of their own jurisdiction and management. Although this attitude may add fuel to the civil liberties debate, Part 2 of the user authentication survey in Section 4.5 found a strong bias towards terminal-centric security (50%) compared to a network-centric approach (33%), in practice, the network-centric solution represents a far more

elegant and powerful solution. It enables network operators to better protect themselves *and* their subscribers, by centrally managing and securing subscriber security information, in a similar way to the IMEI (Section 2.3.2) and better distribute new security systems and updates, offering ultimately a more secure solution to both the subscriber and the network operator. The discussion in Section 4.5 goes on to argue that the survey results may in fact represent participants ignorance of the holistic view and the benefits a network-centric solution can offer.

Apart from the security management benefits offered by a centralised system, when compared to a distributed one, the network-centric technique offers the mobile consumer a significant convenience benefit, in the form of enhanced personal mobility.

2.3.7.3 Mobility

Potentially, one of the most attractive benefits of a network-centric security system is that of increased personal mobility (Furnell *et al.* 1996), where a subscriber may for example register with any terminal (fixed or mobile) in order to access their mobile operators services, under their own personal subscription. Although GSM was originally designed to offer personal mobility via the SIM, operator network incompatibilities (both hardware and software) have restricted this to a limited mobility only within the subscribers own operator network. In practice, the personal network mobility aspect offered by the mobile SIM is rarely utilised: how often is a network SIM card removed from a handset after being installed and the battery inserted? Even ignoring the obvious fact that the SIM usually resides behind the battery, within the closed body of the mobile handset, it is inherently too small and the SIM hardware interface too inconvenient to be of practical use as a token of true personal mobility. This argument is even more relevant with the introduction of the 3FF SIM standard, see Section 2.3.1.1. The sort of personal mobility

proposed for next generation wideband systems (Section 2.2.4.2) can only be enabled via a: non-token-based, non-knowledge-based, *subscriber* based, network-centric, non-intrusive continuously monitoring authentication system. Current doctrine dictates that this can only be achieved through biometrics.

Of course, this ideal mobility scenario does however suffer its own set of consequences. The primary points of issue being:

- Increased data (authentication) traffic over the wireless link;
- Subscriber authentication sample confidentiality;
- Subscriber location confidentiality;
- Biometric samples variability.

Taking each point in turn, the massively increased bandwidth of the next generation mobile networks should have little trouble handling the extra handshaking required by a subscriber based security system, even if authentication was performed continuously, especially when compared to the bandwidth of say a video conferencing signal. The second point of subscriber signature confidentiality reverses the trust issue mentioned earlier in Section 2.3.7.1. With the onus of data confidentiality in the hands of the network operator, subscribers must entrust sensitive, potentially biometric, data to a third party. Considering the current trend of seemingly mass distribution of personal contact information to the highest bidder and the albeit justified paranoia of national security agencies, after world events like the September 11th terrorist attack (911 2001), confidentiality of bank, medical or biometric information must be brought into the spotlight. Following on with this discussion, continuously monitoring mobile systems also have the potential, whether desired or not, of tracking users across heterogeneous networks (Herzberg 1994). When considering the dynamic nature of biometric samples,

this is less of an issue when considered within the context of a continuously monitoring security system. Such a system could incorporate a *middleware* architecture, designed specifically for the management of biometric templates, including:

- threshold management of non-Boolean authentication outcomes;
- continuous maintenance and augmentation of signature data over time;
- alternative access provision(s) in the event of authentication failure due to, for example, a change in a users' biometric markers as a resule of physical injury.

Subsidy Lock and Mobility

The subsidy lock is popularly used by network operators to lock mobile handsets to the service provider's own network, irrespective of the SIM card. Once a mobile handset is subsidy locked to a specific operator network, inserting a SIM card from an alternate operator network will cause the handset to lock. The relevance of subsidy lock to the issue of mobility is that by physically tying the terminal to the host network, mobility originally designed into the mobile hardware, is being restricted. The reason for this is the business model network operator's use, which depend on mobile handsets being sold at subsidised prices, in return for the consumer committing to a minimum term contract.

2.3.8 Continuous, Non-Intrusive Security

One of 3GPP's requirements for secure UMTS service provision is it should be possible for network service providers to "authenticate users at the start of, and during, service delivery" (3GPP 1999). Authentication *during* service delivery represents a departure from the established 2G approach and again implies the need for a non-intrusive approach to avoid disrupting a subscriber's legitimate network activity. Options for achieving this may be related to periodic or continuous supervision of subscriber activity, utilising behavioural profiling techniques or continuous biometric monitoring.

There is already a significant emphasis upon subscriber profiling in order to counter fraud, with operators applying data analysis techniques to network data in order to identify and flag potentially fraudulent transactions (Modisette 1999). The same principles could be extended to the user authentication environment for anomaly detection. Profiling could encompass factors such as the types of services typically accessed and the times/durations of access in order to construct a model of the subscriber's normal behaviour. Such techniques have been the focus of work in the general IT domain for some time and have already been incorporated into network-based intrusion detection systems (Porras and Neumann 1997).

Features of 3G handsets that will enable advanced subscriber services, also offer the potential to facilitate more advanced security options. For example, a number of biometric approaches (Cope 1990) could conceivably be integrated in a non-intrusive manner, depending upon the nature of the mobile device and the service being accessed.

2.4 Conclusion

Mobile security within the currently evolving generations of mobile communications technology are still predominantly based on the security systems set in place over a decade ago when 2nd generation mobile communications networks, and rudimentary services, were first introduced. As the technology rapidly progresses and new individual services are conceived, the supporting security systems need to evolve rapidly in order to maintain protection commensurate with the risks and consequences associated with the new developments. The next chapter is devoted exclusively to the opinions of the general public on the specific mobile security related issues raised within this chapter.

Chapter 3

Assessing Subscribers' Attitudes towards Mobile Services and Security

3 Assessing Subscribers' Attitudes towards Mobile Services and Security

As an integral part of the *assessment* stage of the PhD, in addition to the technological review covered in Chapter 2, a public opinions survey into mobile telephony based security and related issues was conducted. This chapter, along with a separate sub-section on biometrics and advanced security (see Section 4.5), presents an in depth discussion and interpretation of the survey results; a full copy of the survey questions is included in Appendix C.

3.1 Introduction

It has been established in the previous chapters that the current 2nd generation GSM and 3rd generation UMTS systems offer only one line of defence at the Human-Computer Interface (HCI), an impersonal knowledge-based system susceptible to masquerade attack: the traditional Point-of-Entry (PoE) PIN. In order to gauge public opinion on this and other mobile authentication issues, a survey was conducted. The survey was primarily distributed online over an extended period of two years, with additional hard copy local distribution within the University of Plymouth (Rodwell and Clarke 2002), accumulating just under 300 sets of respondents' results. The survey was also marketed through various online links and university-based public announcements.

The primary aim of the survey was to evaluate subscriber awareness and attitudes towards the various forms of security available within their mobile devices and their understanding and opinions regarding the various forms of *enhanced* security available in general. A hypothesis was formed which the survey aimed to investigate that states:

The majority of mobile subscribers either do not understand or are lacking well founded opinion on mobile security issues. They are also generally ignorant of the security implications of the advanced services being offered through the next generation of wideband networks known as 3G.

This attitude unfortunately reflects the success of the technology suppliers' marketing campaigns, where the latest ring-tones and third party connectivity are highlighted over security features, which are usually disabled by default and their activation buried within the user manual. Although to date, security has rarely been a marketing attractor, a fact highlighted by survey respondent's purchasing priorities, discussed later in this chapter, it could also be argued that product marketing is simply reflecting the fact that there have been no new or significant security developments to market or promote.

The survey consists of four main sections, each intended to assess a certain aspect of the participant's views and understanding of their mobile usage. These sections are:

- **Demography:** Fundamental data on participant's gender, age group and affiliation (if any) with the University of Plymouth.
- **Services:** Questions covering operator networks, hardware and services usage and which aspects the user considered important when selecting them. This helps gauge the level to which additional security can be considered necessary.
- **Security:** A selection of questions covering respondents' views and awareness of existing and future methods of mobile security. User's perception of security is considered to be fundamental to its acceptance and subsequent adoption.
- **Topic Awareness:** A selection of topical mobile related questions, in order to gauge the participant's basic depth of knowledge of the subject area.

3.2 Demography

The survey was available online for a period of two years, covering the years 2002 and 2003. The only formal requirement of participants was that they had experience of owning or using a mobile phone at some stage prior to completing the survey.

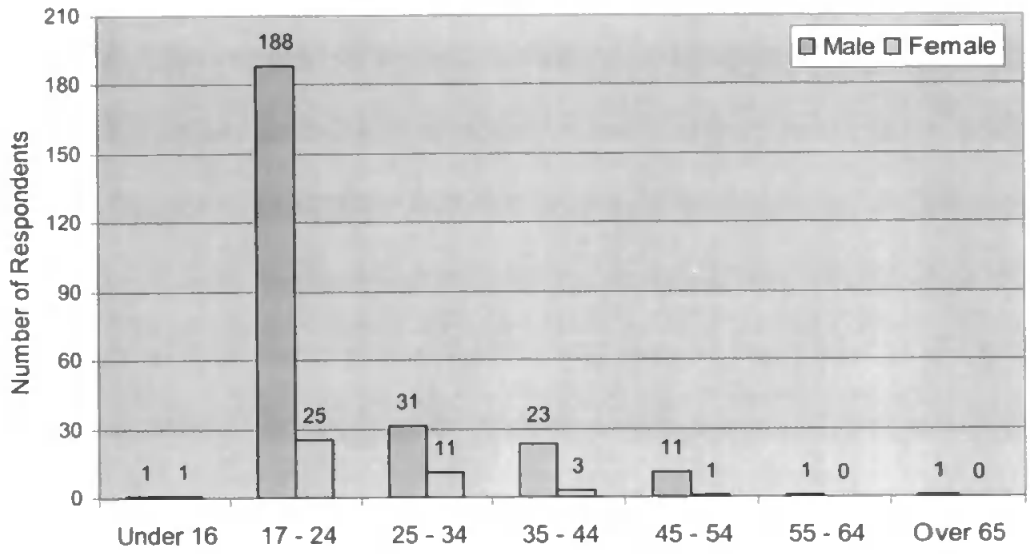


Figure 3-1 : Security survey demography

From the 297 respondents, the majority fell into the '17 – 24' category with a bias towards male respondents, as illustrated in Figure 3-1. There are a number of variables which should be considered when analysing these figures:

- **Survey marketing:** The marketing and distribution of the survey amongst a specific population; e.g. Links on Internet websites.
- **Survey distribution:** The popularity/penetration of the distribution medium(s) within certain sub-groups of a population; e.g. The Internet with Students.
- **Respondent interest:** The appeal of the survey topic to specific sub-groups of a population; e.g. Mobile technology to Teenagers.
- **Respondent character:** The willingness of specific sub-groups to actually participate in a voluntary survey; e.g. the unemployed.

The survey was hosted on a university campus server through a departmental website with a basis towards IT and electro technology; it was therefore expected to have an initial majority penetration amongst males of classical university age. It can, however, be demonstrated that amongst the general population, adoption of mobile technology is predominant amongst those within the age group 15-24 years (Miller 2001; Squires 2001; Competition Commission 2003), closely reflecting the surveys respondent population. It has also been found that the differing views of men and women on the adoption of mobile services are in fact minimal (CellularOnline 2004). The surveys results can therefore be accepted, with some confidence, to statistically represent a fair reflection of typical mobile user attitudes.

3.3 Access and Services

Services are the *raison d'être* of mobile communications; especially in the post 2G arena. This section covers respondent's selection criteria for both mobile hardware and services providers', in addition to their usage of the services available at the time of the survey and their perceived future services requirements.

3.3.1 Network Operator Survey Shares

In order to obtain an overall picture of service usage, it is necessary to know some basic details about subscribers' choices of both network operator and mobile hardware. Figure 3-2 shows the variation in respondents' choices of network operator (by market share) in comparison to the actual UK Figures (W2F 2004). It can be seen, that although the UK market share of mobile network operators is distributed relatively equally, there is a marked variation in the survey respondents' choices of operator.

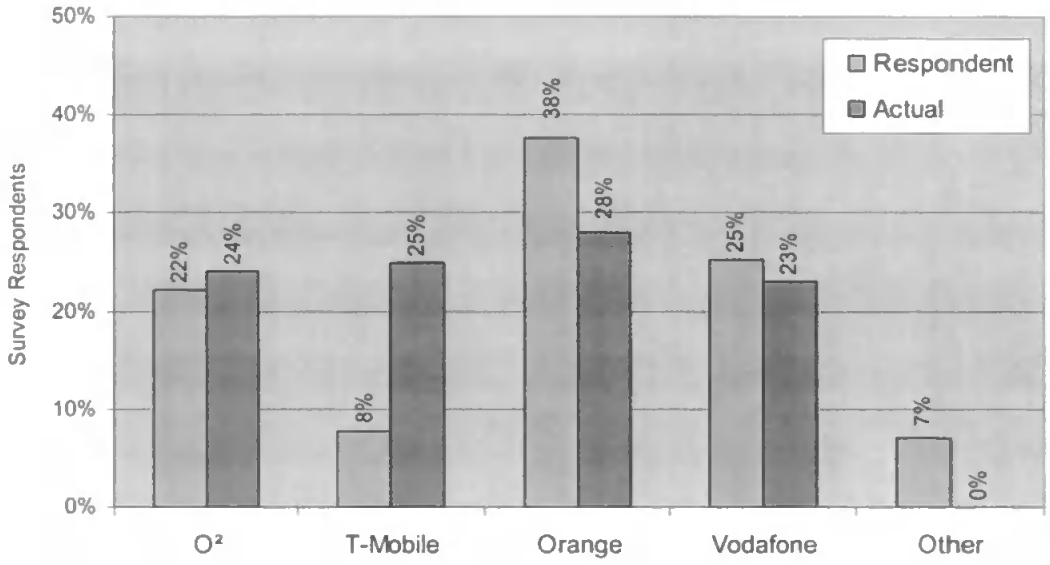


Figure 3-2 : Network operators' market-shares

There are a number of possible reasons for this variation, related primarily to the network operators presence in the primary survey location. These are:

- Operator's mobile coverage.
- Operators' commercial outlets.
- Operator specific promotional incentives: services, handsets, gifts.
- Independent 3rd party supplier promotional incentives: services, handsets, gifts.
- Survey population.

Although the main UK network operators share almost complete national *population* coverage, the T-Mobile brand had the weakest network coverage in the survey region at the time of the survey; reflected in T-Mobiles poor result compared to its actual UK share. It could be further hypothesized that a high profile presence of the Orange brand within the city where the survey was marketed could have also biased the local respondents to this brand. As all network operators offer similar services within a standardised security architecture, these results will not bias the overall security aspect of the survey.

3.3.2 Handset Supplier Survey Shares

There are currently more mobile handsets in the UK than people (W2F 2004), with around 8 out of 10 adults owning at least one of the 60 million active mobile handsets. Of those surveyed, 85% left their handset switched on for more than 10 hours a day, making it the first choice for instant communication. When considering this, it is worth reasserting the point that from the humblest 2G handset to the latest 3G devices, they all share the same basic subscriber PoE PIN and hardware SIM card authentication mechanisms.

Figure 3-3 shows the variation in respondents' choices of handset compared to national and global figures for the year of completion of the survey (CellularOnline 2003).

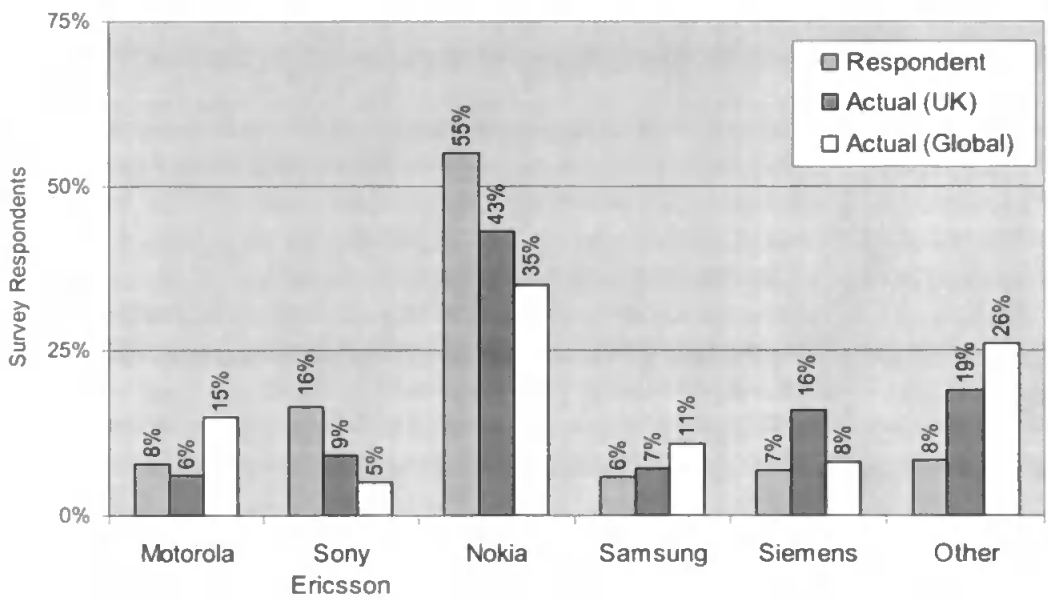


Figure 3-3 : Handset manufacturers' market-shares

Acknowledging slight variations in respondents' choices of handset, compared to UK national figures, Figure 3-4 shows the market share results as a line chart of linked values to visualise the survey results correlation with UK market shares: a good result in support of the validity of the survey. A global plot is also included showing clear correlation with international market shares for the named suppliers, with only the non-UK *other* suppliers appearing to significantly upset the trend.

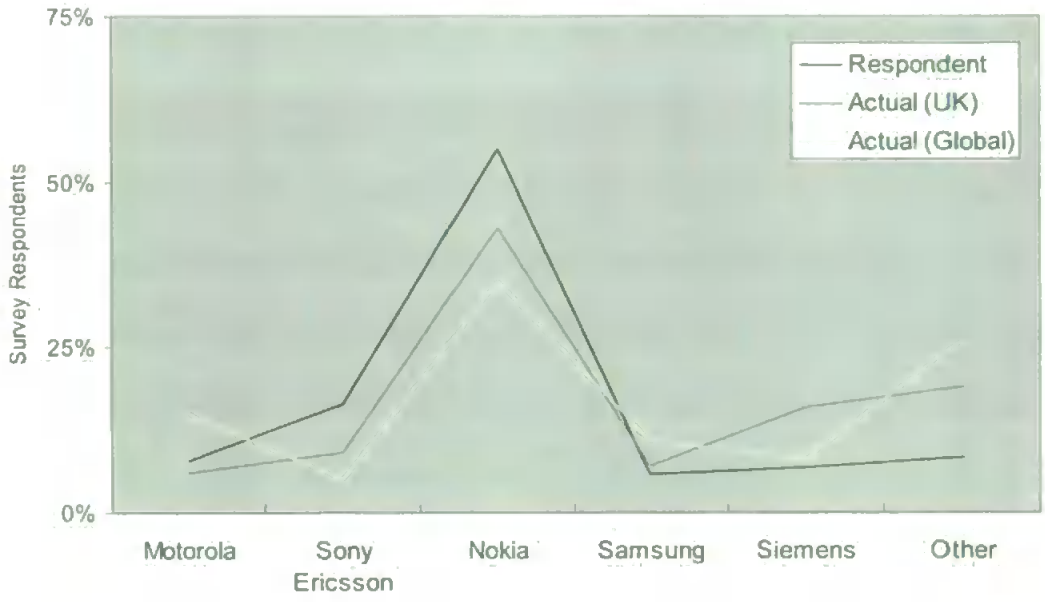


Figure 3-4 : Handset manufacturers' market-shares correlation plot

3.3.3 Network Operator Selection Criteria

When considering a mobile subscription, either contract or *Pay-As-You-Go*, there are essentially two decisions which the buyer has to make: choice of the network operator and choice of the handset supplier. Dealing with these issues in turn, the survey first investigates the buyers' views on a selection of network operator criteria. The results have been sorted in order of importance to the buyer, from left to right in Figure 3-5.

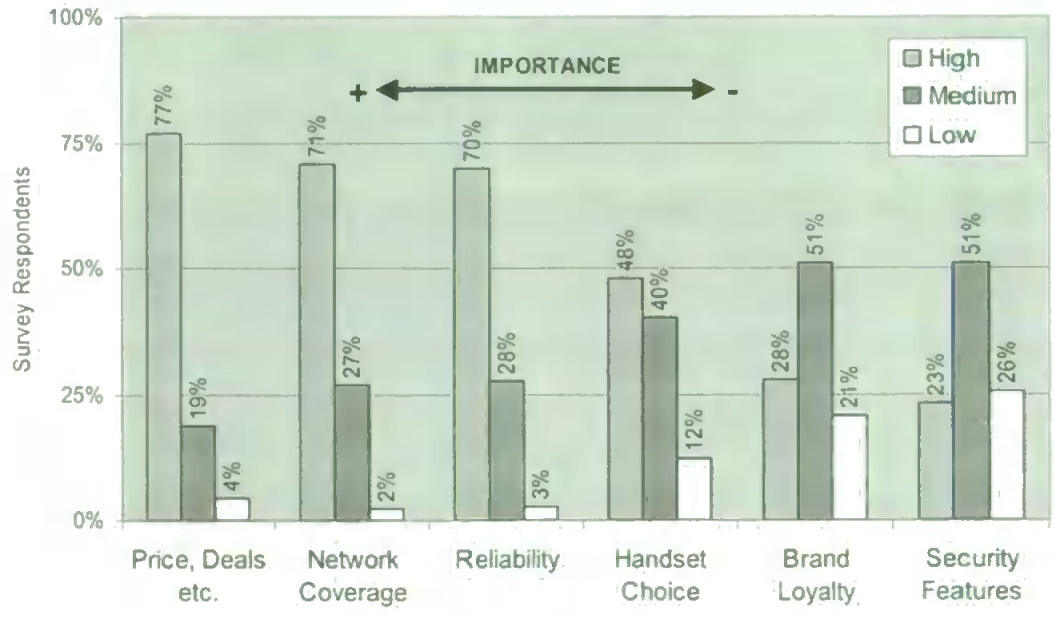


Figure 3-5 : Network operator user selection criteria

It was found that 77% of subscribers considered contract cost, or handset subsidy for pre-pay, to be of greatest importance, followed closely by network coverage and reliability. The results are not surprising as these are quality of service issues and any change or variation would noticeably affect the service. Choice of handset sits in the middle of the table, neither strongly persuading nor dissuading potential customers; reflecting the fact that not only do the majority of handsets offer similar specifications, but also that all network operators offer a choice of nearly all available handsets. With brand loyalty only commanding 28% of customers votes, it is not surprising the lengths network operators go to in order to keep existing customers, offering the latest handsets and preferential rates when a subscriber threatens to change supplier when a contract expires. Finally and in support of the hypothesis introduced in Section 3.1, security features reside at the bottom of the list of buyer's criteria of importance when considering a network operator.

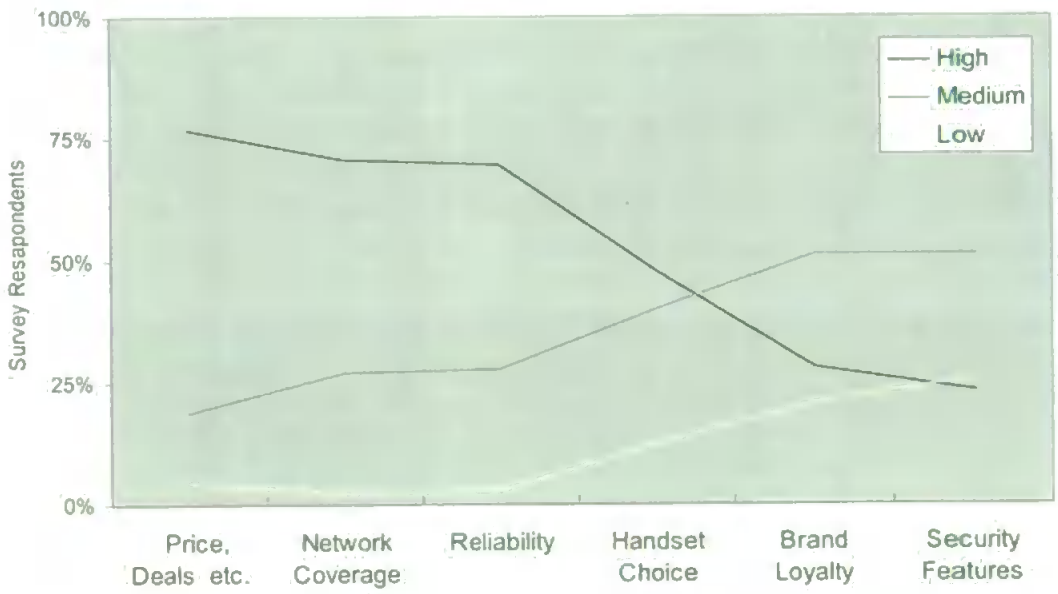


Figure 3-6 : Network operator user selection criteria (linked maximum values)

The line chart of linked maximum values in Figure 3-6, clearly visualises that security was considered the least importance operator selection criteria, with the highest (26%) *Low* importance vote and the lowest (23%) *High* importance vote. To further emphasise the point, security also received the highest (51%) moderate (no strong opinion) vote.

3.3.4 Handset Selection Criteria

When considering the choice of handset, 61% of respondents considered battery life to be of greatest importance from the selection of choices; more than double the second most popular issue of 3rd party connectivity (Bluetooth, IR Etc.) With a similar result to the network operator result in Section 3.3.3, brand loyalty was considered of higher importance than security, albeit by a narrower margin. Although security features command a stronger overall position than in the network operator results, they still received the highest proportion (49%) of the moderate vote and a significant quarter (27%) of the low importance vote, demonstrating either consumer misunderstanding or genuine lack of consideration for security issues. Once again, this is an important result in support of the hypothesis stated in Section 3.1. It is also interesting to consider that the only issues that respondents considered less important than security were essentially insubstantial: mobile accessories, handset games and swappable fascias.

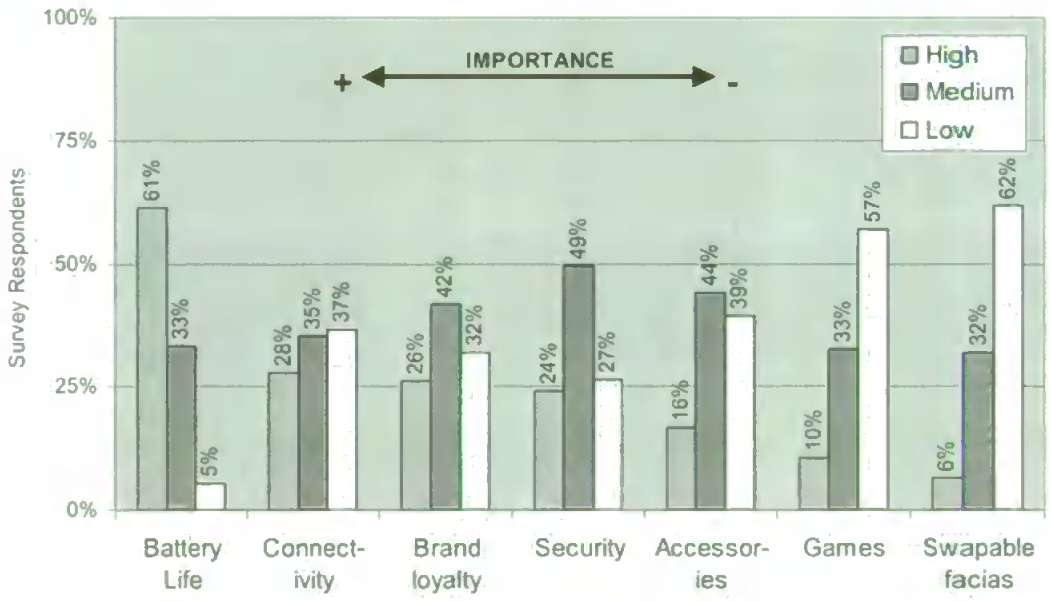


Figure 3-7 : Mobile handset user selection criteria

Figure 3-7 shows a complete breakdown of the results, sorted in order of considered high importance. It is accepted that the list of offered criteria is not exhaustive: it does however enable security to be ranked within a representative selection of options.

3.3.5 Services Usage

Having justified the need for enhanced subscriber authentication, based on the enhanced services of the new wideband mobile networks, the survey proceeded to explore existing service usage and investigate the trend towards acceptance and adoption of enhanced data services. It is not unexpected to find that the majority of respondents still use their mobile handset principally as a form of mobile communication, either through real-time telephony or the data based Short Message Service (SMS), currently in the order of 2.1 billion per month nationally (W2F 2004). What is of more interest is that 5% of respondents DO NOT consider telephony of high importance, preferring the data based services of their device; translated nationally this represents around 3 million users, or the entire population of Wales (UK) (Link: National Statistics).

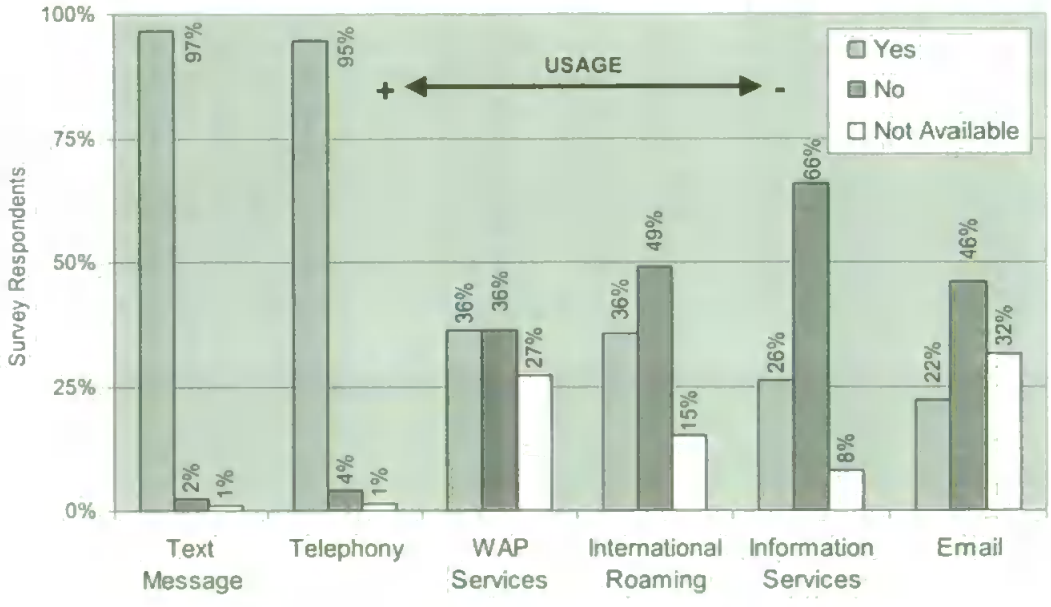


Figure 3-8 : Mobile services popularity (circa 2003)

The results shown in Figure 3-8 are representative of the primary existing services of 2nd generation networks at the time of the survey. Although the usage of WAP Internet based services only accounted for 36% of respondents' votes, nationally around 780 million WAP pages were being accessed per month (W2F 2004). To demonstrate the recent growth in this area, this figure had risen by 42% the following year to 1.11 billion

(W2F 2004), driven by factors such as the massive rise in popularity of ringtones and the Euro 2004 football competition, some matches of which were only available live online and not available in a mobile context through any other service.

3.3.6 Preferences for Future Services

The number of mobile handsets with GPRS-enabled Internet and Multimedia Message Service (MMS) capability doubled in the year 2003 to 2004 and is expected to account for 75% of all UK mobiles by the end of 2005 (W2F 2004). This will bring the total number of Internet capable handsets in the UK to around 53 million, potentially connecting up to 88% of the UK population to the World Wide Web via at least one access terminal.

Although many of the *future* services offered for opinion at the commencement of the survey are now current technology, such is the growth in the area, all were proposed as future services, with only MMS being rolled out nationally by the completion of the survey in 2002. The selected services were all based on the enhanced services' capabilities enabled by the network access technologies of wideband mobile networks.

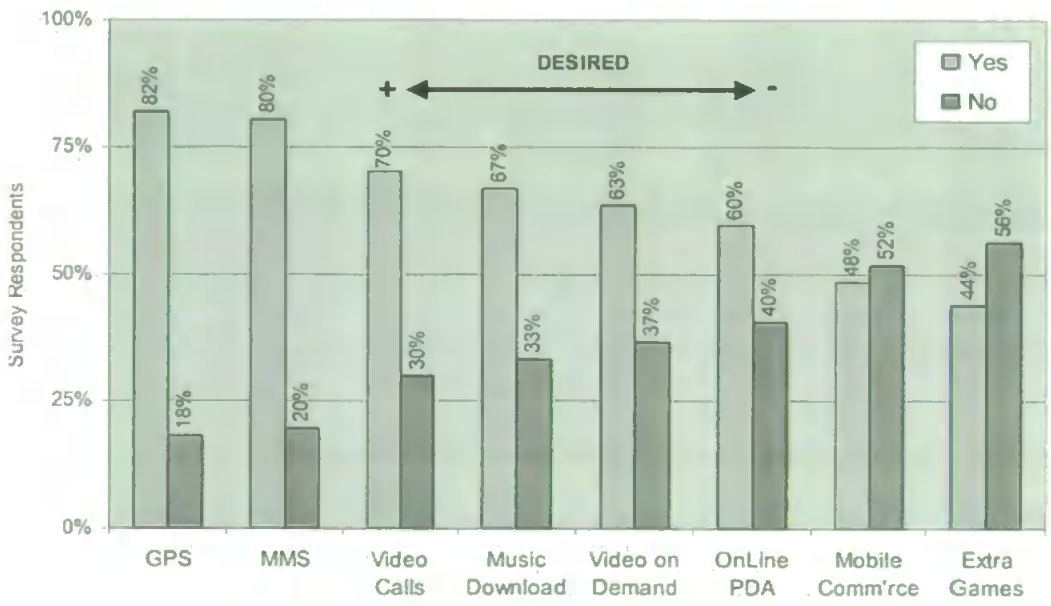


Figure 3-9 : Future mobile services' user preferences

Figure 3-9 shows the results of the respondents' preferences, placed in order of desire. Notice the general strength of opinion towards future services, supporting current mobile growth trends and consumer's insatiable appetite and desire for more services.

Coming out top with 82% were Global Positioning Services (GPS) based services, offering the facility to not only inform the user as to where they are at any particular time, but essentially enabling Location Based Services (LBS); for example, to supply real-time directions to a local facility (a bar or a petrol station). With the SMS service well established in the psyche of the mobile user, it should not be too surprising to find its multimedia equivalent, the MMS, very high in the chart, proving a popular choice with 80% of respondents. Two years on and the growth in camera phones has translated this desire into a MMS market estimated to be worth £5 billion by 2004 (Juniper Research, 2002). From the remaining video based services, video conferencing proved marginally more desirable than video on demand (VoD), although it could be argued as to the respondent's appreciation of scope of VoD, as its current existence in the world of television limits it to films. Scenarios of a VoD file arriving on your handset the instant: a favourite sports team scores a goal; an intruder alarm is triggered in your home; a local news story breaks from a location outside the UK (for foreign nationals) may not have been considered. Mobile commerce is still in its infancy in the UK compared to the now well established Internet-based ecommerce. This is likely to change rapidly with the growth of wideband networks and the improved rich Internet browsing experience they offer. The demise of WAP enabled light browsing and slow unreliable 2G data links should finally bring ecommerce to the mobile, with subscribers purchasing online goods in much the same way and frequency as seen on traditional Internet-enabled computers. It is interesting that although only 10% of respondents considered games of high importance when selecting a handset in Section 3.3.4, 44% expressed a desire for

more or better games in the future. Although games still reside at the bottom of the popularity chart, the growth in wideband enabled online gaming will surely change user's perception of a mobile game from being 'Tetris', in a similar way to early computer user's view of a computer game as being 'Pong'.

This section of the survey has shown that the trend in mobile usage is moving inexorably towards wideband data services, which the respondents have indicated they would be keen to use. The majority of these services will require the use of some form of personal data, whether it is stored purchasing profiles or banking details for mobile commerce, current subscriber position for LBS or private video messages recorded for MMS or video conferencing. These services demand a commensurate level of protection to guard against masquerade abuse, protection currently not offered and only realisable through a subscriber-based authentication system.

3.4 Mobile Security

This section covers a selection of questions investigating respondents' views and awareness of existing and future methods of mobile security. User's perception of security is considered to be fundamental to its acceptance and subsequent adoption.

3.4.1 Experiences of Mobile Handset Abuse

It has been established that the primary method of user authentication for mobile handsets is a PoE PIN code. Before ascertaining the survey respondent's awareness and attitude towards existing security techniques, they were questioned on their own experiences of mobile handset abuse. It was found that 28% of respondents reported cases of theft or abuse of their handset, as shown in Figure 3-10.

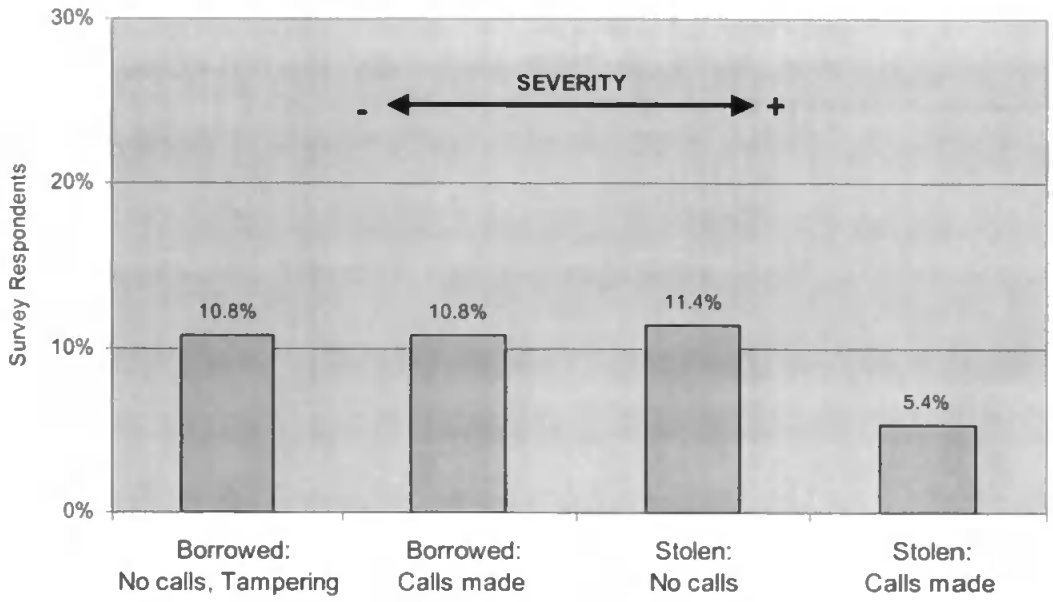


Figure 3-10 : Personal experiences of handset abuse

It can be seen from the results that handset theft is the most common form of criminal abuse, with half of those handsets stolen being subjected to further masquerade network abuse. It can be strongly argued that although abuse of a handset loaned to a friend or colleague can be inconvenient (e.g. changing the handset default language) and even unexpectedly cost the legitimate user money (for example: calling a premium rate number), in such cases a high degree of liability rests with the legitimate user and their own judgement. This is not to say that a suitable subscriber authentication mechanism would not be appropriate. On the contrary, imagine a scenario where a network had the appropriate security infrastructure to reliably authenticate subscribers in real-time and immediately react to services that fall outside of a pre-defined operational envelope or behavioural profile; without specific permission from the legitimate user. Chapter 5 introduces a novel authentication system conceived specifically to address this issue, when integrated into an appropriate mobile security framework.

3.4.2 User Issues Regarding Mobile Handset Authentication

Section 2.3 of the thesis introduced and discussed the IMEI, the primary mobile hardware authentication mechanism. The survey questioned respondents on their awareness of the IMEI and its relevance to security, with an alarming 41% of participating users claiming no knowledge even of its existence. This could have serious implications for the recent security drive to harmonise and regularly update network operators IMEI black lists (GSM Association 2002). If 41% of users are unaware of the existence and significance of the IMEI, 41% of users are unlikely to realise the importance of reporting a stolen handset, risking the handset's IMEI not being black listed within the CEIR.

When asked about the primary user authentication mechanism, the Personal Identification Number (PIN), it was not a surprise to find more than 99% of respondents familiar with the technique; this approach is universally used outside of mobile circles. Although 69% of those users questioned also engage the PIN to protect their handsets at switch on, this still leaves 31% of respondent's handsets completely unprotected by the only form of subscriber authentication currently available. If this result is scaled up to the UK population (2004), it represents some 18.6 million handsets, or approximately the population of greater London (Link: National Statistics 2003). Perhaps the reason for this is the fact that a remarkably similar 31% of survey respondents consider the PIN authentication mechanism to be inconvenient and intrusive. This highlights the point that no matter how effective a security system may or may not be, if it is a voluntary system and is not perceived as being convenient, it will not be widely accepted. Any proposed future authentication mechanism must therefore not even be a convenience issue, but completely transparent in operation.

Of those users questioned who regularly use the PIN, it was found that over a third (39%) have never changed it from the factory default (usually '0000'): this would be the first and most obvious attack for a potential abuser. As manufacturer hardware default PIN codes are easily found, usually printed in the hardware handbooks, by not changing the default PIN a user is effectively advertising their PIN code to every similar hardware user, in addition to openly on the internet via chat rooms and forums. These users essentially have no more protection than the 31% of users who do not use the PIN at all; they can therefore be aggregated to give an overall figure of unprotected handsets in the UK of 70%!

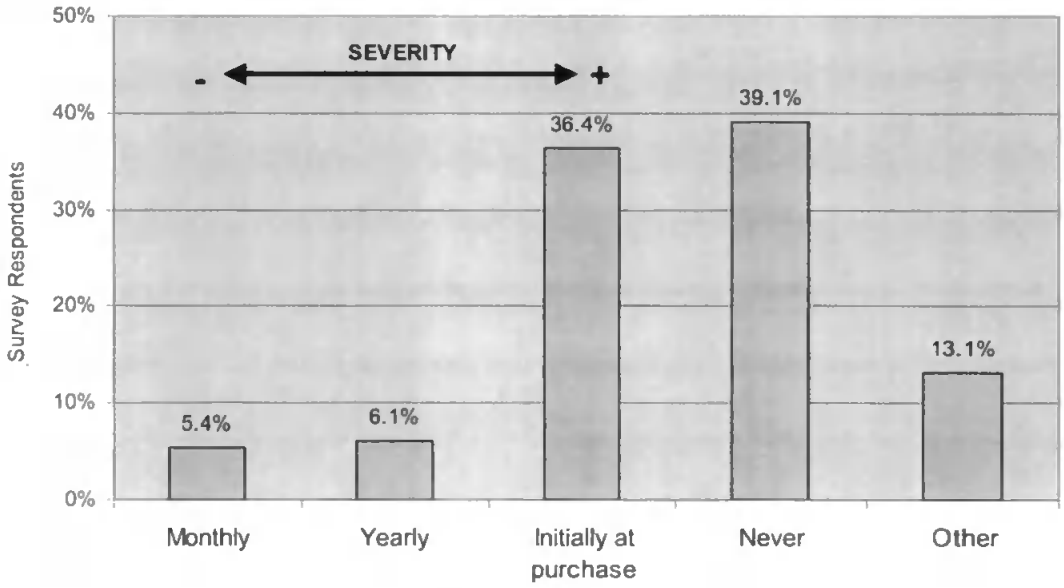


Figure 3-11 : Frequency of mobile handset PIN changes

For those users who do change their PIN, Figure 3-11 clearly shows that the vast majority perform the action only once at time of purchase and not again. Although this is a major improvement over using the default PIN, it does imply another recognised PIN-related security issue: PIN multi-casting. With 36% of respondents admitting to using the same PIN code for multiple services, the probability of an individual PIN being compromised is greatly increased, as are the consequences. A likely reason for extensive PIN reuse is the proliferation of knowledge-based authentication mechanisms, the average person now having to remember up to 10 password/PINs (Link: CompTIA).

With the majority of personal resources now password/PIN protected (bank cards, mobile communications, internet based services), users are now required to memorise many critical security access codes, with the almost inevitable consequence of reuse or multi-casting. When those surveyed were asked if they have ever used a PIN Unlock Code (PUK), due to either forgetting or miss-entering their PIN. It is debatable whether the 38% of 'yes' respondents were admitting just poor memory, or good security protocol by conscientiously assigning different PINs to different personal services.

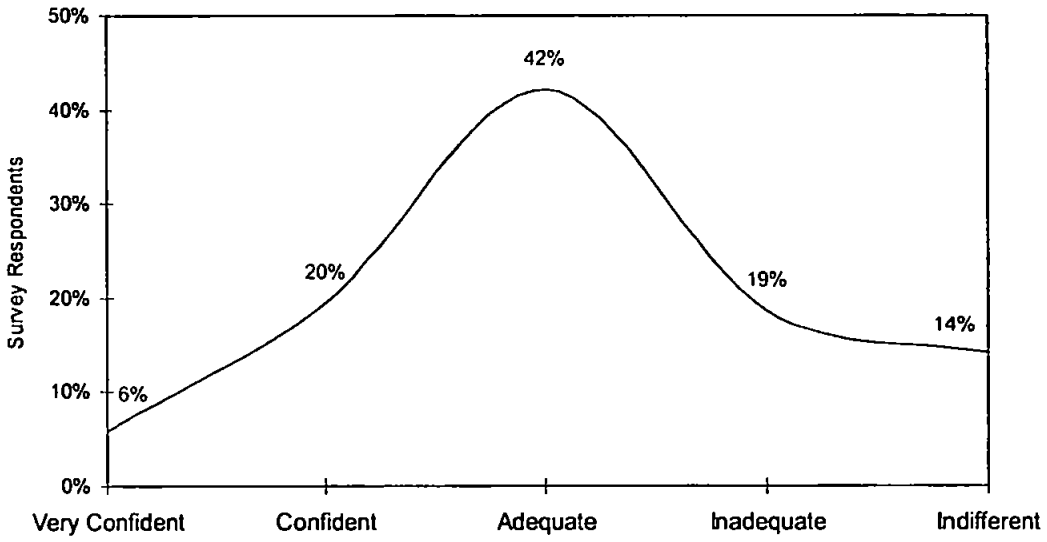


Figure 3-12 : Users perceived effectiveness of the PIN mechanism

Considering the PIN-related security issues discussed previously, 86% of those surveyed had a definite opinion on the effectiveness of the PIN technique. The curve in Figure 3-12 represents a distinct Gaussian distribution around a feeling of only adequate protection offered by the PIN approach. When considering this result, it needs to be reaffirmed that around the time of the survey, mobile services were still predominantly 2nd generation telephony-based services, with data-based services still in an embryonic state. A recent joint study by Cranfield University and the London School of Economics (LSE) and funded by the Department of Trade and Industry (DTI) broadly supports this mood, indicating that consumer confidence in mobile communications devices, including wireless devices is at it's lowest point for a decade (IEE IP 2005a).

Although the PIN has not moved on as the basis of HCI security for mobile handsets, it has been shown in Section 2.2.3.3 and subsequently discussed, that mobile devices, the networks which they serve and the advanced services they enable certainly have.

3.5 Topic Awareness

To gauge an awareness of the survey participant's level of understanding of mobile related issues, the demography performed in Section 3.2 was complimented with a selection of three, progressively more specialised, mobile communications questions.

The first question relates to the issue covered in Section 3.3.1, that of UK mobile network operators and it was expected that the majority of UK mobile users would be familiar with the major UK network providers and spot the rogue provider (Nokia). Question 2 presented a more difficult choice of IT based acronyms, one of which (ADSL) is not related to the field of mobile communications, but wire-based communications. The final technical question required the participant to identify the basic data-rate of GSM mobile communications. All the offered solutions are widely advertised valid communications data-rates from both mobile and wire-based disciplines and as such present a difficult choice to the respondent not familiar with the correct solution. The multiple-choice options were:

- 9.6 Kbps - The standard GSM data-rate.
- 14.4 Kbps - An example of a multiple time-slot (x2) HSCSD rate.
- 56.6 Kbps - The standard V.90/92 home dial-up internet data-rate.
- 64 Kbps - The standard (x2 channels) ISDN data-rate.

The set of results shown in Figure 3-13 tend to indicate that the survey population were relatively familiar with the issues and terminology of mobile communications, primarily indicated by the high success rate achieved on question 3. This was not entirely unexpected after the demographic results in Section 3.2 indicated that the predominant profile for a survey respondent was male, aged 17-24, with a bias towards technology.

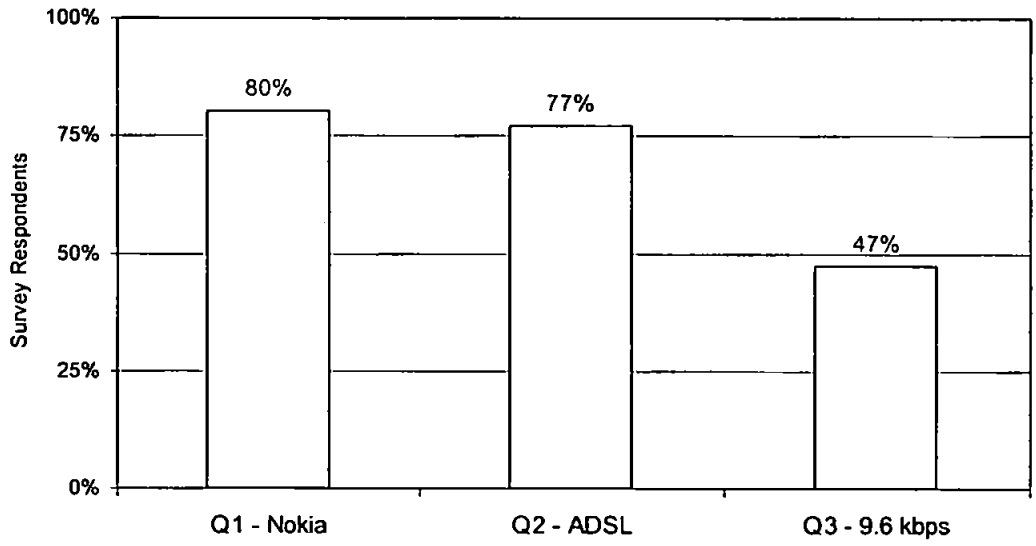


Figure 3-13 : General user awareness of mobile issues

In analysing the results, only 80% of respondents identified Nokia as one of the dominant mobile handset suppliers and not a mobile network operator. This could be due to the fact that both are essentially mobile service providers and distinguishing between the two may be inconsequential to the consumer. 77% of respondents recognised ADSL as a landline telephony delivery service and not a current mobile technology. This is a strong result for a technology question and is likely influenced by the heavily marketed broadband internet rollout over the last few years, enabled by ADSL technology and marketed as such. Almost half of respondents (47%) knew the basic data transmission rate of 2nd generation GSM to be 9.6 Kbps. This is another strong result, for this technical question and indicates a high degree of understanding of mobile issues, by a large proportion of the respondent audience; backing-up the survey results on technical questions.

3.6 Conclusion

The rapid growth in mobile data services has highlighted the weakness of the existing user authentication system. This survey identified that by the end of 2003, users were already using rudimentary data services and that they are willing to use future services as and when they became available. Recent research from the Gartner Group suggests that currently around 90% of mobile devices are lacking the security to prevent hackers from gaining access (Gold 2004).

The hypothesis introduced in Section 3.1 has been upheld. Although 85% of respondents appeared to recognise the need for additional security in future generations of mobile devices, this is in clear contradiction to the 70% of respondents who do not actively use the existing PIN system. This tends to indicate that it is the authentication mechanisms themselves, rather than the concept of security that users are rejecting.

To address this issue, what is needed is a non-intrusive subscriber authentication mechanism, not token-based or knowledge-based, but user-based. A mechanism that can be implemented transparently, reliably authenticating the active user continuously and conveniently; acting as a network gate-keeper in addition to protecting sensitive subscriber data from masquerade abuse. A system that will be:

- Accepted by network operators and service providers.
- Tolerated by mobile subscribers.
- Widely used.

The next chapter investigates truly personal authentication mechanisms, drawing from the discipline of biometrics as a foundation for a solution to the problem.

Chapter 4

Biometrics and Mobile Devices

4 Biometrics and Mobile Devices

Having established a need for enhanced mobile subscriber authentication in Chapter 2, this chapter proceeds with a review and discussion of biometrics and its applications. The field of biometrics has been chosen as the primary resource for tackling the authentication issues raised and forms the foundation of the novel authentication mechanism introduced in Chapter 5; which is the core of the PhD research.

4.1 Introduction

Biometrics describes the 'automated recognition of individuals based on their behavioural or biological characteristics' (ISO/IEC JTC1/SC37 2004). It is the method of identification we all use *everyday* to recognise *everyone* we meet, from the closest family member to the occasional chance meeting of an old friend in a corridor. In its purest form, biometrics is incredibly powerful and enables near perfect recognition in minimal time. They allow a person to recognise a familiar character from within a group of almost limitless size, almost instantly, then continuously reconfirming the identity with near zero error. Even when used with human senses in isolation, we have all recognised a familiar voice within the melee of a bar or on the end of a phone, or a familiar face in a crowd from a distance or on the television, without giving it a second thought. It is perhaps therefore not surprising that security firms are striving to harness this powerful technique, for if a system were even to approach the efficiency of the human biometric system, masquerade attacks could be reduced significantly, releasing funds currently lost to identity fraud and litigation, estimated at £1.3 billion in 2004 (Home Office 2006) and enabling a host of new identity-assured services to be brought to market.

In practice, the human biometric system has been perfected over thousands of years and an artificial implementation of techniques familiar to a young child are incredibly complex without the processing resources of the human brain. Nevertheless, ground-breaking biometric techniques like fingerprint recognition have been in use by New Scotland Yard, the headquarters of the Metropolitan Police, since 1901 (MET 1901) and as early as 1968, saw the introduction of 'Identimat', the first commercial electronic biometric system, costing US$20,000, for a Wall Street (USA) investment bank (Konstantinos 1997). Although in IT terms, progress within the field of biometrics has been relatively slow, in 2003 the Massachusetts Institute of Technology (MIT) predicted biometrics to be one of the top-ten emerging technologies expected to "change the world" (MIT Tech 2003). After the September 11th terrorist attacks on the United States (911 2001), the U.S. Government announced "Biometric Identifiers" as a top priority in their fight against terrorism (Bush 2002), forming the InCITS (International Committee for IT Standards) M1 Technical Committee for domestic biometrics standards.

Widespread adoption of biometric security systems is still however in its infancy. A recent sobering report by the London School of Economics (LSE), rather ironically not even addressing the predominant technical hurdles of biometrics, warned that the biometric techniques proposed for the UK governments *National Identity Card* program may fall foul of 'disability anti-discrimination legislation' (IEE IP 2005b). However, before negotiating societies politically correct minefield and individual disability issues, such as the difficulty a blind person could have positioning appropriately for an iris scan, certain biometric approaches consistently work better or produce lower error rates, with certain individuals. Even considering these issues, Figure 4-1 shows that biometrics is currently witnessing substantial commercial growth, with revenues increasing by around 60% year on year, from US$20million in 1996, to US$1.2billion in 2004 and predicted to exceed US$2.5billion by 2006 (Norton 2004; IBG 2004).

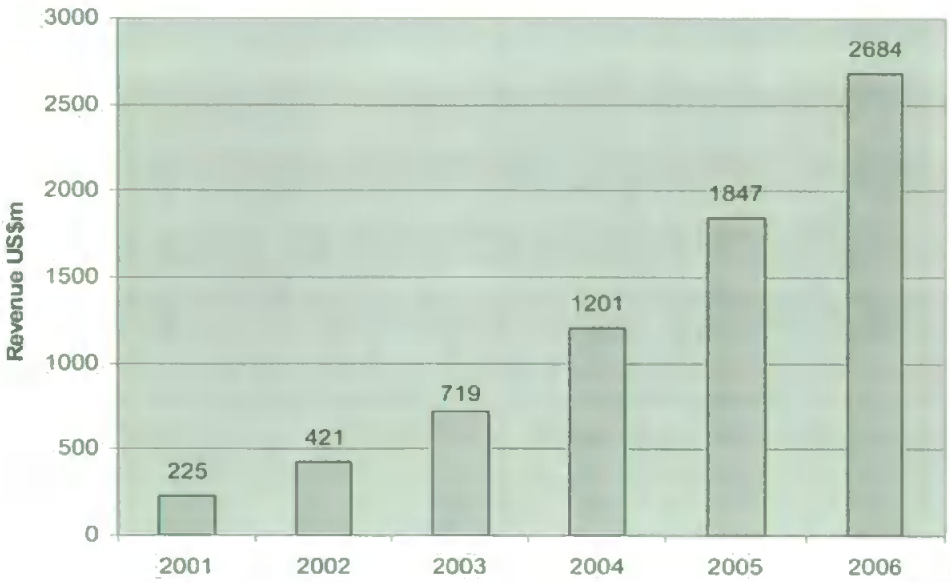


Figure 4-1 : Biometric revenue growth, 2001-2006

4.2 What You Are

The process of user authentication, which describes the comparison of an input sample against one or more reference samples, can traditionally been broken down into three distinct categories, those of: *What you know*, *What you have* and *What you are*. Arguable the simplest form of authentication is the password or ubiquitous PIN (Smith 2002, pp.163), representing *What you know*. As discussed in Section 2.3.3, the PIN is the established authentication mechanism for validating a user to their mobile handset. To validate the mobile subscription on the network, a SIM is inserted into the handset, carrying the appropriate authentication data (Section 2.3.1). This SIM represents the second authentication category, that of *What You Have* and together with the PIN, these two mechanisms constitute subscriber authentication within the current mobile security framework. Although biometrics are rarely applied to current mobile technology, the third authentication category of *What You Are* offers networks many advantages over existing mechanisms.

4.2.1 Authentication Security Focus

With traditional knowledge-based and token-based authentication systems, the effective security resides solely in the strength of the password and location of the hardware, respectively, which can exist independent of the authentication system; see Figure 4-2. Consequently, any user can use the registered user's authentication mechanism to gain access to the protected network, a masquerade; independent of security policy.

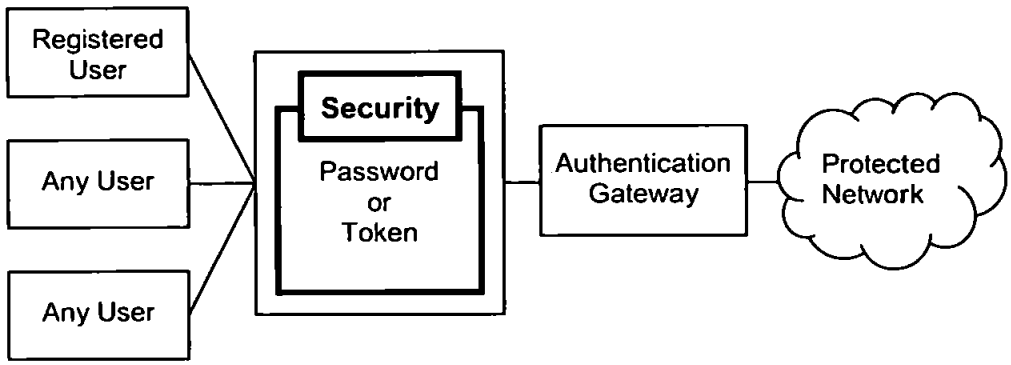


Figure 4-2 : Security focus in a knowledge/token based security system

In contrast, biometric-based security utilises an authentication mechanism or biometric-markers which are inseparable from their owner and authentication cannot be performed independently of the registered user. Authentication is truly personal and unique to each registered user, it cannot be shared and security is dependent on security policy.

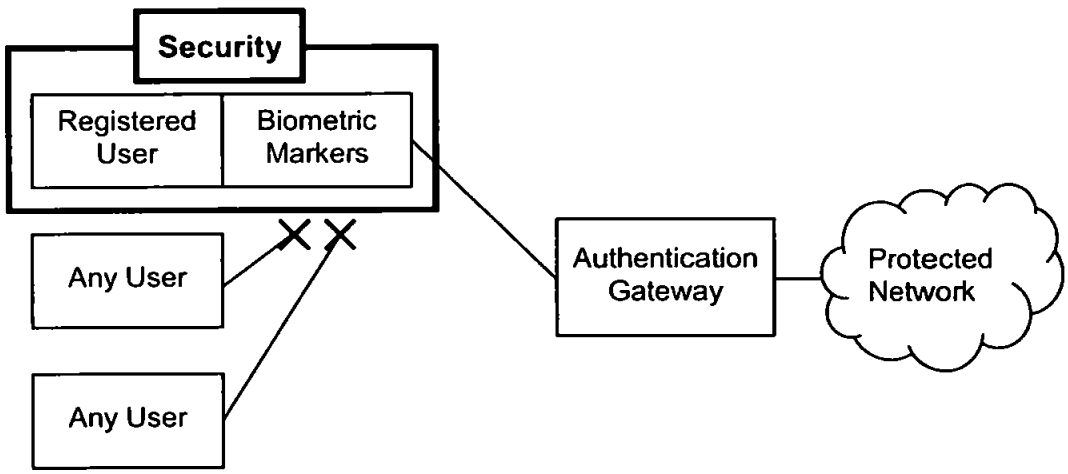


Figure 4-3 : Security focus in a biometric based security system

4.2.2 Factors Affecting Biometric Systems

Table 4-1 compares the three different authentication approaches discussed, with a selection of nine key authentication issues, ranking the three approaches of: *What You Know*, *What You Have* and *What You Are*, in order of their inherent ability to address each chosen issue: '1' being the most suitable and '3' being the least. Totals have also been included for mutual comparison of the issues raised. The table demonstrates that with these nine authentication issues, the inherent properties of biometrics' clearly lend themselves to advanced authentication and although not ideal, with the approaches currently available and acknowledging possible contextual variations, present the most comprehensive set of results and therefore the best generic security solution.

Issue #	1. Intrusiveness	2. Intimacy	2a. Distinctiveness	2b. Transferability	3. Vulnerability	4. Permanence	5. Accountability	6. Assignability	7. Selection Criteria		Totals *(Lower is better)*
What You Know *Password*	3	3	3	3	3	1	3	1	3		23[1]
What You Have *Token*	2	2	2	2	2	1	2	2	2		17[1]
What You Are *Biometrics*	1	1	1	1	1	3	1	3	1		13[1]

Table 4-1 : Comparison of the three authentication categories, with a selection of key authentication issues

Notable by its absence, performance is dealt with separately later in the thesis. A full discussion of the remaining authentication issues raised in Table 4-1 and their relevance to mobile authentication and security will now be discussed in greater depth.

[1] Cumulative results are subjective and for mutual comparison only. No allowance has been given for specific contextual applications.

1. **Intrusiveness**: *Can the technique be applied non-intrusively and continuously?*

   In addition to realising the security potential of biometrics, certain approaches have the added and very *marketable* benefit of being able to be performed transparently (see Section 4.3), increasing subscriber acceptability.

   Non-intrusive identity-assurance is a key driver in the move towards advanced authentication systems and has a number of distinct advantages over the intrusive PoE techniques which still predominate in current entry systems:

   - The ability to perform subscriber authentication continuously, reducing the security emphasis on any single authentication cycle failure; reducing false rejections, whilst maintaining identity-assurance.
   - The user convenience of not having to suspend current activity to perform an authentication cycle; the system can perform re-authentication as security protocols dictates, again, maintaining identity-assurance.

2. **Intimacy**: *Is the signature truly personal to the subscriber?*

   One of the fundamental properties of biometrics is the inherent intimacy of the physiological or behavioural markers, introduced in Section 4.2.1, which cannot be forgotten or mislaid any more than the registered users head! Even if a user's personal biometric sample data is illegally intercepted, it would be extremely difficult to suitably reconstruct the template and present it appropriately to the relevant authentication system collector. This is in contrast to a knowledge-based approach, where although authentication data can potentially be personal in nature (mother's maiden name), it is not tangibly linked to the user and can be changed transferred or re-assigned as conveniently as security protocols dictate.

2a. Distinctiveness: *The possibility of somebody else adopting the same signature?*

One of the recognised problems of password based authentication systems is the fact that many people can hold and share the same password. Company names and acronyms, computer names, family names and birthdays predominate in password lists everywhere; there are also some ubiquitous passwords which regularly crop up: 'God', 'password', 'sex' (Geodsoft 2005). It is accepted that all humans are different to some measurable degree, even superficially, all humans look and sound different, even twins. It is this inherent individual distinctiveness of humans and their biometric markers that biometric systems utilise in order to authenticate us. Although when taken as a whole, humans are highly distinctive, biometrics focus upon individual physiological or behavioural human traits which in isolation have varying levels of distinctiveness. This is discussed in Section 4.2.4.

2b. Transferability: *Is the sensitive authentication data/sample transferable?*

Extending the discussion on the personal nature of biometric markers (issue 2), biometric authentication data is non-transferable. As discussed in Section 4.2.1, with traditional knowledge-based and token-based authentication, the security lies solely in the password and hardware, respectively, which exists outside of the authentication system and can be applied by any user, regardless of security policy. In contrast, biometric markers cannot be separated from their host, except via surgical means, and hence biometric samples cannot be shared. Even if a legitimate subscriber wanted to allow a colleague access to their account on a biometrically protected system, they would still have to perform the authentication process themselves and ensure that the system security was not enforced continuously else even a masquerade without ill intent, would be quickly detected.

3. **Vulnerability**: *Is the technique vulnerable to masquerade or brute force attack?*

   All authentication systems are vulnerable to some form of circumvention or brute force attack; biometric systems being no exception (Ratha *et al.* 2001a). The traditional password can be attacked in a number of ways: either through a social engineering (Granger 2001) probability (calculated guess) attack; or via a brute force (systematic attempt of every possible combination) attack (Smith 2002, pp.258, 274). Even assuming an attacker could simulate a user's biometric markers, or devise a way of presenting pseudo-biometric samples in an appropriate format to a biometric collector, biometric sample data is generally far more complex than traditional passwords. Dependant on the approach, biometric systems utilise up to one thousand individual unrelated markers, significantly reducing the chance of any trial-and-error attack producing an acceptable sample within an acceptable time. Biometrics' vulnerabilities are explored in more depth in Section 4.2.5.

4. **Permanence**: *Does the authentication data vary in any way?*

   Biometrics differ from conventional authentication mechanisms in that each authentication cycle produces a slightly different set of biometric samples: all biometrics are dependent to some degree on prevailing environmental conditions; the majority of physiological biometrics vary with age; and behavioural biometrics can change with the subject's mood. This is contrary to password and token-based systems where, once defined, authentication data does not change, unless changed deliberately. This unique property of biometrics is handled by allowing for the variability within either the biometric collector or a *middleware* architecture, capable of managing authentication thresholds and confidence ratings, rather than simple Boolean responses. This variability is also why biometric samples cannot be protected with a 'hash' function, in a similar way to static passwords.

5. **Accountability**: *How accountable is the user for a signature breach?*

Another major benefit of the intimate nature of biometrics' samples is the accountability of the authentication system. If a user is actively logged into a system, system administration can be confident that it *is* in fact the actual account subscriber that performed the login. In addition, if the security system enforces continuous authentication, it can be confidently assumed that the user online is the legitimate account user and not somebody masquerading in the account. This issue has further reaching implications than simple account access: with a reliable, continuously authenticating system, it will be possible to confidently substantiate the location of a particular person at a particular time. The privacy implications of this system behaviour will surely set a precedent in the near future.

6. **Assignability**: *Can the signature be easily reassigned, if it is compromised?*

The benefits realised from the intimate nature of biometric samples, do not however present the full picture; biometric authentication does suffer a major complication. In the unlikely event of an attacker successfully compromising a user's authentication template, by whatever means, it is essentially impossible for the legitimate subscriber to change their own biometric markers; without surgery.

Whereas a password or token is as easily changed as a systems security policy allows, the possibilities for addressing a compromised biometric are more limited:

- Increase the resolution of the system by utilising additional markers.
- Tighten the authentication threshold(s); at the expense of increased false rejection of user(s) (see Section 4.2.3).
- Offer users alternative biometric approaches (see Section 4.3).

7. **Selection Criteria**: *Can a subscriber choose an easily compromised signature?*

   It has been well documented that users of password based authentication systems regularly compromise system security through the sharing, writing down and poor selection of passwords (Smith 2002, pp.155-192). Although a systems security policy can enforce good password selection, this is generally at the expense of user's ability to memorise a difficult authentication sequence and the subsequent impact on system administration and account recovery services. A biometric template is loosely synonymous with a traditional password of between ten and one thousand heterogeneous alphanumeric *vectors*, dependent on the approach chosen, which must be presented simultaneously to the authentication system. User registration on a biometrically protected system does not introduce the potential for human compromise. The user does not need to memorise anything, as the system determines the markers for the authentication template based solely on security.

4.2.3 False Match and False Non-Match Errors

The inherent variability of biometric markers (Section 4.2, Issue 4) and the subsequent variability of the samples generated by the biometric collector, gives rise to two characteristic percentage error rates (or likelihood of an error occurring), within a *biometric* system. These are:

- **False Match Rate (FMR)**: Equivalent to the *False Acceptance Rate (FAR)* of a system. FMR is the probability that an impostor's biometric sample will falsely match the stored enrolment template of a random user (of a system).
- **False Non-Match Rate (FNMR)**: Equivalent to the *False Rejection Rate (FRR)* of a system. FNMR is the probability that a biometric sample will falsely not-match the stored enrolment template from the same user (of a system).

Synonymous with FAR and FRR, FMR and FNMR are mutually exclusive, in that as one error rate decreases the other tends to increase proportionally, giving rise to the EER (Equal Error rate) where the two rates become equal. Figure 4-4 shows a theoretical *ideal* performance plot for FMR vs. FNMR, with both curves converging at zero percentage error; 't^1', representing the ideal threshold setting. There would be no point in setting a different threshold in the ideal case, as the EER is already at zero error and any variation of 't^1' would only increase FMR or FMNR system errors. In reality, a typical biometrics system will produce a plot similar to that shown in Figure 4-5, where the EER is above zero percent (Cope 1990). In this case, the system has to trade off FMR against FNMR, depending on the security requirements of the current operation. Starting with a threshold setting equal to the EER of the system, 't^2' can be dynamically biased, towards either *tighter* security (at the expense of increased user inconvenience) or greater user convenience (at the expense of *slacker* security), dependent on the current operational scenario. For the system designer, FMR and FNMR curves are fundamental in managing the quality-of-service for the system end-users.

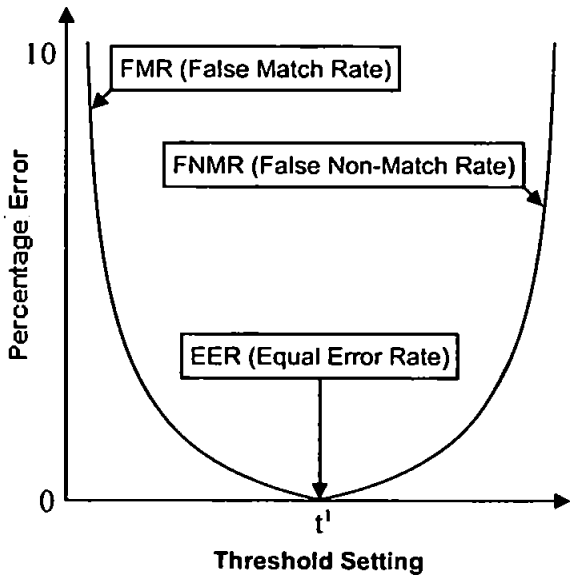


Figure 4-4 : The ideal FNMR vs. FMR performance curve(s)

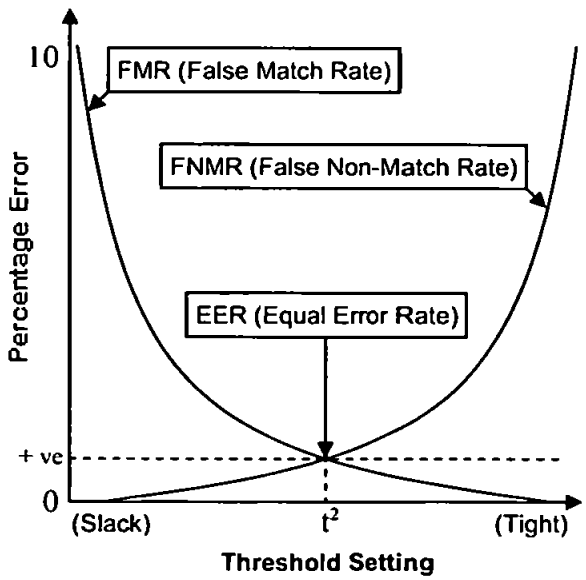


Figure 4-5 : Typical FNMR vs. FMR performance curve(s)

Table 4-2 below shows some typical EERs and commercial hardware solutions for the selection of biometric techniques, identified in Section 4.3, with currently the highest market shares (2004).

Biometric Technique	Market Share[1]	Typical EER	Example Hardware Supplier (Product) Internet Link: Supplier Homepage
Fingerprint	48%	1.5%	IDTeck Co. Ltd. (Finger007/x) Web: http://www.idteck.com
Speaker-recognition	6%	2.5%	Voice Security Systems (VoiceProtect®) Web: http://www.voice-security.com
Iris-scan	9%	3.5%	Argus Solutions (TrueIdentity®) Web: http://www.argus-solutions.com
Hand-geometry	11%	4.5%	Recognition Systems Inc. (HandPunch®) Web: http://www.recogsys.com
Signature-recognition	2%	n/a	Softpro (SignPlus®) Web: http://www.signplus.com
Facial-recognition (2D)	12%	7%	Identix Inc. (FaceIt®) Web: http://www.identix.com

Table 4-2: Equal error rates of popular biometrics, by technology

4.2.4 Identification versus Verification

In further considering biometrics as a method of advanced authentication, there are essentially two distinct modes of operation:

- **Biometric Verification (Authentication):** "The automated process of assessing a claim that [submitted biometric sample(s)] and [stored biometric sample(s)] are from the same source." (ISO/IEC JTC1/SC37 2004)
- **Biometric Identification:** "The automated process of comparing [submitted biometric sample(s)] to return an identifier(s) of the source(s) of the matched [enrolment record(s)]." (ISO/IEC JTC1/SC37 2004)

[1] Extracted from Figure 4-7, the Pie-chart: Biometrics market-share, by technology (IBG 2004).

Both of these approaches utilise the same essential capture and comparison mechanism, a fundamental difference lies in the different strengths of the two approaches in the real world. In an ideal biometric authentication system, it would not matter which approach was adopted, as once the system had determined the identity of a user, it would be academic as to whom they claimed to be. In reality, biometric systems are not perfect and if presented with the choice, the ability of a system to verify the user is whom they claim to be, is preferable from a security perspective, to an approach based on the probability of a *best fit* user, not knowing in advance if the user under investigation is even enrolled on the system.

The issue is also raised as to the performance and subsequent cost of the authentication mode. Identification requires the system to essentially check the captured biometric sample(s) against every single user enrolment record (biometric template) stored in its database (one-to-many) in order to confidently formulate the strongest probable identity; also checking that this probability is above a pre-defined threshold for unknown users. This would require significantly more processing (powerful hardware) than verification which, on the other hand, can be performed in a single operation: does the captured biometric sample(s) exceed the authentication threshold for the enrolment record of the claimed identity (one-to-one). Within a mobile environment, all processing imparts a cost on the battery life and inevitable performance (time between charge cycles) of the mobile device, therefore it is crucial to justify whether an authentication process is PoE or continuous, terminal or network-centric (Section 2.3.7).

4.2.5 Threats to Biometric Systems

It can be shown that biometric approaches present less risk in the areas of authentication attack when compared to traditional *What You Know, What You Have* based systems. The classic risk to an authentication system is the masquerade attack, or convincing the system security that the *actual* user is in fact the *legitimate* user. Biometrics are not knowledge-based, consequently there is no transferable knowledge to hijack. Biometrics is not token-based (the user is not considered a token), therefore there is nothing tangible to steal; although it could be argued that certain dismembered body-parts could fit this category! Therefore, to masquerade undetected on a biometrics protected system, an attacker must essentially present themselves as a clone of the legitimate user, or at least produce biometric samples which beat any system confidence threshold; dependent on which biometric approach the system has in place (see Section 4.3). Biometrics authentication markers cannot be inadvertently lost or deliberately shared in the same way that passwords or physical tokens can (Section 4.2.1), each user template is unique to its owner and as such offers increased accountability.

The second significant risk to authentication systems is that of *Trial-and-Error* attack, sometime referred to as *Brute-Force* attack. Again, biometrics present a significant obstacle to an attacker, as biometric templates are generally based on dozens of simultaneously captured, highly variable, loosely related samples, which cannot be guessed; compared to a password which is drawn from a set of alpha-numeric characters and although recommended against, usually arranged in a logical sequence (as words, names, sequential codes etc.). In addition, a well designed biometric system will employ a process known as *seeding* to ensure biometric sample(s) are in fact original and not replays of previous sample(s) (Ratha *et al.* 2001b). Certainly to the casual attacker, there is no easy or obvious way of defeating a biometric sentinel system.

The more determined attacker may attempt to literally steal a legitimate subscriber's identity and register *themselves* with a system, assuming the stolen identity; this is known as identity theft (Home Office 2006). Although identity theft essentially circumvents the authentication system completely, once system registration has been achieved, biometrics may present a solution in the form of behavioural profiling. If the security system had access to a behavioural profile for the claimed identity, a possibility in a network-centric security architecture (Section 2.3.7.2) of a large distributed network, such as a national mobile network operator, the system has a window of opportunity to flag the intrusion before any potentially defrauding profile refining takes place. If however, an attacker is determined enough and carefully chooses the identity of their victim, utilises social engineering techniques and chooses the identity of an authentication system/network with absolutely no knowledge of the person whose identity is being stolen, then only a traditional and thorough *human-to-human* interrogation has any real chance of identifying the fraud.

4.3 Biometric Techniques

Biometrics presents a selection of possibilities when it comes to the collection of biometric markers for an advanced authentication system. The possible approaches can generally be split into two categories:

- **Physiological:** Anatomical metrics or *What you are.*
- **Behavioural:** Behavioural metrics or *How you are.*

Physiological approaches such as fingerprint, face-recognition and hand-geometry still command the majority share of current commercial biometric systems, representing the more mature technologies. They are also more invariant and discriminative in comparison to the more transient behavioural approaches (Woodward *et al.* 2003, pp.45-100).

Although *behavioural* biometrics are not a new concept, the inherent need for an automated authentication system based on behavioural techniques can be linked with the growth of personal computing. A behavioural biometric that has witnessed massive growth in recent years is 'behavioural-profiling', although not specifically within the area of authentication, but within the area of targeted advertising; advertising based on individual users purchasing profile (Bisgaard-Bohr 2002). Another approach which has seen recent developments within the field of authentication, is keystroke-dynamics (Joyce and Gupta 1990, Legget and Williams 1988), or one's typing style, along with the release of commercial applications like: BioPassword (Link: BioPassword). BioPassword is interesting in that it adopts a hybrid *multi-modal* approach to authentication, adding biometrics to an established and familiar password authentication mechanism, realising a *What you type* and *How you type* approach. This is an excellent application of biometric technology; it not only strengthens an authentication mechanism that the security industry has experience and confidence in, but also enables a *soft* deployment of biometric technology to consumers in a way less brutal than a novel, purely biometric approach.

The question can be asked, 'Is there a *best* biometric?'. This depends on the application environment and the task the user is currently engaged in, as each biometrics' inherent qualities will lend themselves more to one particular circumstance than another. For example, although speaker-recognition may not be suited to application on either a loud factory floor or within a quiet library, it could be appropriate for telephony based authentication; whereas hand geometry (owing to the size of the collector) would not; behavioural profiling could be suitable for continuously monitoring an online banking site, whereas a user having to hold their eye against an iris-scanner would not.

The diverse nature of biometrics is well illustrated in the Zephyr diagram on biometric techniques, performed by the International Biometrics Group (Link: IBG) in 2004, and shown in Figure 4-6. The diagram illustrates the strengths and weaknesses of the various current biometric techniques and the subsequent importance of understanding and defining a system's environmental and application criteria in order to select the optimum technique. The IBG analysis was based on four criteria, selected by the group, to be of key importance to both the service provider and the user. These were:

- **Intrusiveness**: The level of intrusive interaction required (by the user).
- **Distinctiveness**: The level of uniqueness (of the biometric markers).
- **Cost**: The cost of deployment (primarily of the biometrics collector).
- **Effort**: The level of work required on the part of the user (for authentication).

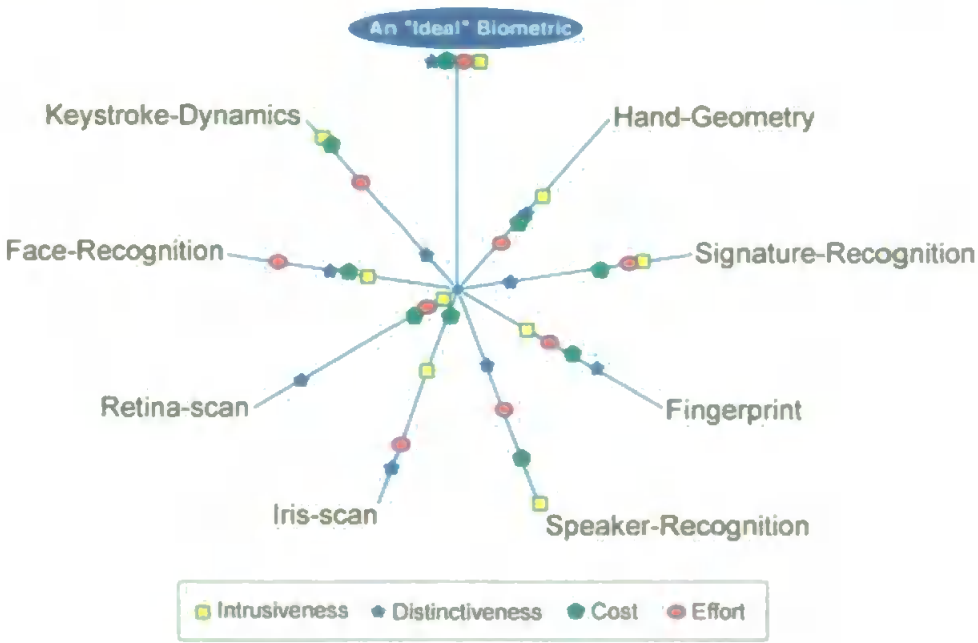


Figure 4-6 : Zephyr diagram of key biometric criteria (IBG 2004)

As a reference, the Zephyr diagram includes the *ideal* biometric result, with all other techniques radiating from a central (worst result) point source. By inspection, it can be seen that no single current biometric technique approaches the ideal case scenario:

although retina-scan exhibits highly distinctive samples, it is very intrusive and suffers the greatest cost to both the provider and the user; by contrast, although speaker-recognition is non-intrusive (convenient for the user), its biometric markers are indistinct and therefore vulnerable to increased false acceptance. The best generic result, with no significant weaknesses and moderate to good distinctiveness, remains the fingerprint; a result closely reflected in the techniques commercial success, shown in Figure 4-7.

Considering the uniqueness of the human subject, only a handful of biometrics' techniques have realised commercial success. Figure 4-7 gives a breakdown of the most commercially successful biometric approaches by technology for the year 2004, with their respective market shares (Link: IBG). By inspection, the more mature and well understood biometric markers, command the greater market shares, with fingerprint(s) commanding nearly half the commercial market.

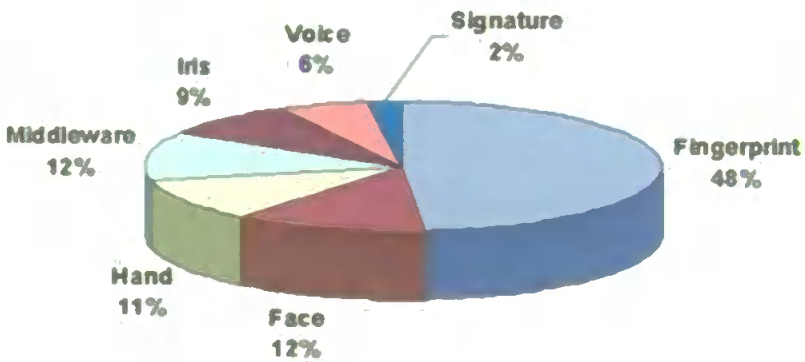


Figure 4-7 : Biometrics market-share, by technology (IBG 2004)

The next section of the thesis discusses current biometrics' techniques in more detail. The selected list is not considered exhaustive, as research within the field of biometrics is constantly realising novel biometric markers and sample collection techniques: an example of which is the **Head Authentication Technique** introduced in Chapter 5, along with some recent commercial approaches introduced in Sections 4.3.2 and 4.3.4.

4.3.1 Physiological Biometric Techniques

A literary summary of established anatomical or physiological metrics: *What you are.*

4.3.1.1 Fingerprint

The technique of fingerprint authentication is based on the fact that everybody's fingerprints exhibit different shapes of ridges and valleys, swirls and loops; even for identical twins. The discontinuities and irregularities, known as *minutiae,* form the basis of the oldest and most widely recognised biometric markers (Maltoni *et al.* 2003), dating back to 1858 (Herschel 1858). Fingerprint technology is by far the most commonly deployed biometric authentication system and offers a set of distinct advantages over other physiological biometrics:

- Mature and proven core technology.
- Time invariant discriminative features.
- Excellent economies of scale have driven down prices.
- Small ergonomic, easy to deploy devices.
- Scalable security, with the ability to utilise combinations of fingers.

Fingerprint based authentication systems are traditionally PoE only, requiring deliberate and intrusive interaction by the user with the system. Considering the strength and maturity of fingerprint recognition, its limitations have not hindered market dominance, see Figure 4-7, in fact the technique has experienced 14% market growth over the last five years (IBG 2004) and will likely remain the dominant biometric for some time.

Although fingerprint recognitions PoE security limitation does not lend itself to transparent or continuous authentication, the technique still lends itself to certain

advanced mobile services, such as m-commerce, where transactions may only require a single authentication. This has prompted mobile suppliers like Sagem to pioneer the incorporation of a fingerprint scanner into a mobile handset (Sagem 2000), although to date only one network, NTT DoCoMo (Japan), has introduced a similarly equipped handset commercially; the F505i (NTT DoCoMo 2004).

4.3.1.2 Hand-Geometry

Utilising the same physiological source as fingerprints, i.e. the hands (and fingers), hand-geometry employs much coarser and less distinct biometric markers; as a consequence it is does scale well in isolation for identification or secure authentication. In application, the technique uses an image scanner (Link: Recognition Systems Inc.) to capture a featureless silhouette of the users hand; biometric markers include measurements of the surface area of the user's hand and fingers, along with finger length(s) and width(s). Anything which can change the shape of the hand, such as large rings, injury or medical aids, can effect system efficiency and increase false rejection. Although the technique has halved its market share over the last five years (IBG 2004), the technique still proves commercially popular (see Figure 4-7), partly owing to its convenient HCI.

The continual drive within the mobile community for smaller lighter handheld devices sets up a conflict of interests with hand geometry technology. Owing to the markers employed (hand area), the required size of hand geometry scanners is restricted by the size of the human hand, making them inappropriate for application within the mobile arena. They are more commonly found in access control or Time & Attendance systems. Early examples include the system employed at the 1992 Olympic Village in Barcelona, and more extensively 4 years later in Atlanta (Washington Technology 1996): more recently, Disney (Link: Disney) have employed a system for multi-day park passes.

4.3.1.3 Facial-Recognition (2-Dimensional)

Two dimensional facial-recognition systems are currently the second most popular commercial biometric with 12% of the market, a share which has remained relatively unchanged over the last five years (IBG 2004). The technique utilises the geometric placement of distinctive features within the human face as markers and offers a number of unique advantages over other biometric systems, it can:

- utilise existing acquisition devices;
- be applied non-intrusively;
- be applied without specific interaction with the biometric sensor;
- remotely search photographic records.

The biometric markers employed are those which exhibit the least variance over time: the size and position of the eye sockets relative to the nose and sides of the mouth (Nanavati *et al.* 2002, pp.63-75). Areas which can suffer significant variance are normally avoided such as hair lines around the forehead and for men, around the chin. Although in principle, all two dimensional facial-recognition systems utilise the same biometric source, their exist at least five competing systems:

- **Eigenface** utilises a set of around 115 common facial templates.
- **Feature Analysis** utilises sets of common facial features' locations.
- **Neural-Network** utilises a neural-network to classify prominent features in the full face. The PhD research technique proposed and subsequently discussed in Chapter 6, utilises a similar approach to sample analysis.
- **Automatic Face Processing** utilises geometric mapping of the face.
- **Thermogram** utilises a thermal image of the face produced by an infrared camera.

Two examples of commercial facial-recognition products are: Imagis Technologies ID-2000 (2004) and Identix Face IT (2004).

One of the drivers for 3rd generation mobile networks is video conferencing (Sections 2.2.3.3 and 2.3.6). A mobile hardware requirement is therefore image capture capability which has the potential of enabling non-intrusive and potentially continuous face recognition technology to be employed when utilising a service which requires the user to interact with the screen and a suitably positioned camera, such as video conferencing or web browsing. Unfortunately this approach would be ineffective, when the handset is used in the traditional telephony mode, still the predominant mobile application. This limitation is addressed by the HAT approach introduced in Chapter 5.

4.3.1.4 Iris-Scan

Iris-recognition technology utilises one of the most invariant biometric markers, the distinctive features of the iris or richly textured ring of pigmented membrane surrounding the pupil of the eye. The techniques requires mapping of the *trabecular mesh* or complex pattern of unique furrows and ridges of the iris via use of, ophthalmologists approved, infrared imaging technology beyond the range of human vision (Daugman 1998). The techniques primary strength is the amount of distinctive data within the iris, offering tremendous potential for reliable identification and secure authentication, far exceeding the error rates of the most commercially successful biometric approach; the fingerprint. However, perhaps owing to the complex authentication process, iris-recognition technologies market share has remained stable at a moderate 10% for the last five years (IBG 2004).

From a mobile perspective, the excellent security potential of the iris is offset by a number of factors, preventing it from realising market application to date. These are:

- The need for small, dedicated authentication hardware.
- The limited authentication range of the biometric sensor, usually only a few inches; although there have been research projects into advanced systems capable of identifying *passers by* up to a distance of 10 metres (Zakaria 2003).
- The authentication process is intrusive and requires training.
- Some user apprehension towards eye-based technology.

Table 4-3 summarises the four principal *physiological* biometrics techniques identified in Figure 4-7 and discussed in this section, with a bias towards their inherent suitability for application within a small handheld mobile device; like a mobile handset.

	Market Share[1]	Non-Intrusive	Security Strength[2]	Template Size[3] (in Bytes)	Mobile Application
1. Fingerprint	48%	×	✓✓✓	250	Discrete[4]
2. Hand-Geometry	11%	×	✓✓	10	Unsuitable[5]
3. Face-Recognition	12%	✓	✓✓✓	1300	Continuous
4. Iris-Scan	9%	×	✓✓✓✓	500	Unsuitable[5]

Table 4-3 : Summary of physiological biometric techniques for mobile application

For a further in depth discussion of the application of biometrics in the mobile arena and the suitability of the available techniques to the medium, refer to Section 4.4.

[1] Extracted from Figure 4-7, the Pie chart: Biometrics Market Share by Technology.
[2] Extracted from Figure 4-6, the Zephyr diagram: Key Biometrics Criteria.
[3] Template sizes are not fixed, but represent typical sizes in current commercial systems.
[4] Authentication performed deliberately at a specific point within an operation.
[5] Owing to the size and inconvenience of the biometric collector.

4.3.2 Other Physiological Techniques

In addition to the market dominant physiological techniques discussed in Section 4.3.1, a number of less commercially significant techniques exist, with a cumulative market share of less than 1%; in addition to some novel techniques which are still in the conceptual stages of development.

Although an in-depth discussion of these techniques is beyond the scope of the thesis, they have been included here to demonstrate the diversity and breadth of the physiological biometrics field.

4.3.2.1 Retina-Scan

Retina-scan is the most well known and mature of the *lesser* biometrics, dating back to the 1930s, and the only technique to realise a successful (albeit limited) commercial application (Das 2005). It utilises an approach to authentication not dissimilar to the iris-scan discussed previously (Section 4.3.1.4), extrapolating a 2-dimensional map of *minutiae* points from an infra-red image of the blood vessels at the back of the eye; the membrane known as the retina. This produces a biometric template, similar to that of a user's fingerprint, though more secure owing to the internal nature of the biometric markers being less susceptible to deliberate modification or damage. Also, in the event of the subject's death, unlike fingerprint, the retina will deteriorate very quickly negating any need for *life* testing. Although producing invariable and highly distinctive markers, the technique is expensive to deploy and suffers from high user inconvenience (see Figure 4-6) and as a result, has only realised application in highly secure physical access areas, where security outweighs convenience; such as government buildings, military installations, power-stations and correction institutions.

4.3.2.2 Vein-recognition

Vein-recognition relies on the mapping of the vascular pattern of blood vessels in either the palm or the back of a subject's hand; not-dissimilar, in principle, to the mapping of minutiae points of fingerprints. The technique utilises an infra-red camera to produce an image based on the absorption characteristics of the deoxidized haemoglobin (in the blood). The technique offers some advantages over other biometric techniques, as it:

- can be implemented without contact with the biometric collector (hygienic);
- is relatively resilient to minor surface abrasions;
- is relatively easy to capture biometric sample(s). The subject simply holds or passes their hand above or below the biometric collector;
- can be implemented non-intrusively, allowing for continuous monitoring, within a suitably designed system.

These tangible benefits make the technique particularly suitable for high-traffic *access control* areas (such as airports) or *time & attendance* systems (found particularly in industry), presenting a real alternative to less robust hand-geometry systems. Vein recognition technology is currently witnessing steady growth in the marketplace, realising a number of new commercial applications (Fulton 2005) (Link: Veid Ltd).

4.3.2.3 Facial-Recognition 3D

3D facial-recognition is an extension of the 2D system discussed in Section 4.3.1.3, utilising an additional depth plane. The technique constructs a 3-dimensional topological map of a subject's face, triangulating each point within a 3-dimensional plane, via audio reflections from two sonar style transceivers placed a short-distance apart and in front of the subject (Link: DuPont Authentication; A4Vision)

4.3.2.4 Ear-Geometry

Ear-geometry utilises distinctive characteristics of a print of the pinna, or visible part of the outer-ear, not dissimilar in principle to a fingerprint; an ear-print. The unique shape of the human ear is currently the subject of ongoing investigation (Hoogstrate *et al.* 2001), with various legal bodies investigating its admissibility within criminal courts (Morgan 1999). In the UK in 1998 a murderer was convicted based on ear-print evidence (BBC News 1998), leading to further investigation by the National Training Centre for Scientific Support to Crime in the UK (BBC News 1999). In 2001, Alphonse Bertillon, a respected pioneer of the science of human identification, pronounced the ears uniqueness, stating," It is, in fact, almost impossible to meet with two ears which are identical in all their parts." (Moenssens 1971, p.17). It has even been suggested that the ear has more distinctive characteristics than the human face (Carreira-Perpiñán and Sánchez-Calle 1995), although in balance, it has also been argued that there is no empirical evidence to support the claim that ear-shape is *never* duplicated (Morgan 1999).

4.3.2.5 Facial Thermography

Facial thermography refers to the pattern of facial heat produced from the distinctive flow of blood under the skin. The technique utilises an infra-red camera to capture a heat image of the subject's face, from which a biometric template is formed. Although the technique has the advantages of being suitable for non-intrusive, not-contact application, it suffers from highly variant metrics owing to the abundance of blood vessels in the human face. Factors which can affect the signature are:

- ambient conditions (such as temperature affecting sweat production);
- subjects mood or emotional state of arousal (such as anger);
- subjects medical state (such as sickness, medication or menopause).

4.3.3 Behavioural Biometric Techniques

A literary summary of established behavioural metrics: *How you are.*

4.3.3.1 Speaker-Recognition

Often confused with speech-recognition, *speaker* recognition (aka voice-verification) utilises the physiological individuality of a user's vocal tract, including: vocal chords, palate, teeth and the shape and density of tissue along with the inherently behavioural characteristics of speech annunciation including: pitch, tone, volume and dynamic range (Woodward. *et al.* 2003, pp.101-136). Additional environmental factors, including: colloquial dialect, atmospheric conditions and elocution can also have an affect. Speaker-recognition is a true biometric, focusing on characteristics of *whom* is speaking (from a security perspective): conversely speech-recognition, concentrates on the generic *content* of the speech, where diversity of biometric markers actually hinders system performance.

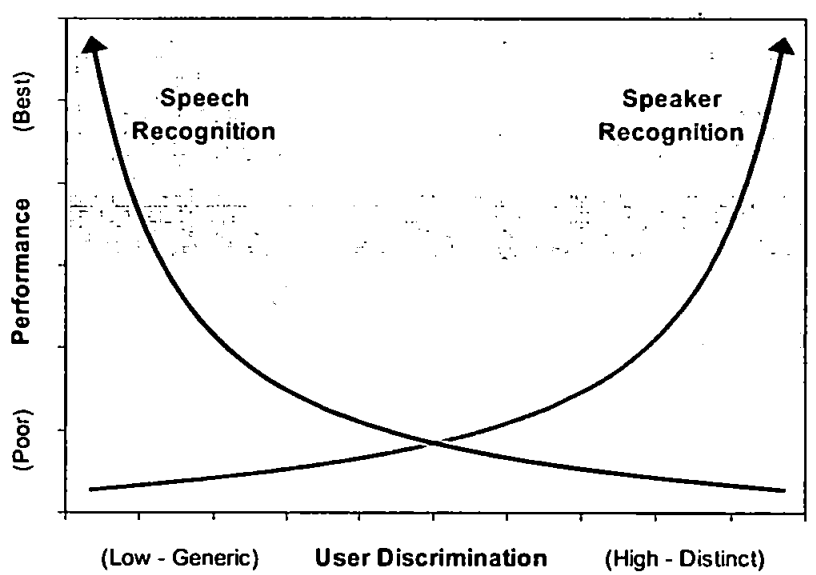


Figure 4-8 : The mutually opposed goals of *speaker* and *speech*-recognition

The diagram in Figure 4-8 demonstrates the diametrically opposed goals of the two systems: Speaker Recognition performance is dependent on highly distinct samples; conversely, Speech Recognition performance is dependent on highly generic samples.

Speaker-recognition can be performed in two distinct modes of operation:

- **Constrained**: Text-dependent, via pre-determined words or phrases.
- **Unconstrained**: Text-independent, via free-speech.

Although unconstrained speaker-recognition offers a less intrusive user interface and the potential for continuous authentication, in use, the restricted text of a constrained system has proven to offer reduced FMR and FNMR errors (Section 4.2.3) and to date, proven the more popular approach within the 6% market share of commercial speaker-recognition systems (Link: Persay Inc.; VeriVoice Inc.; Nuance Communications Inc.).

Within the mobile arena, speaker-recognition is inherently suited to telephony based application[1], not only offering the enhanced non-intrusive security approach required by post 2nd generation wideband networks, but also offering the opportunity to leverage existing acquisition hardware and existing mobile subscriber behaviour.

4.3.3.2 Signature-Recognition

Signature-recognition is an automatic authentication technique, derived from the established Graphologists art of hand-writing recognition, where it is possible to verify the identity of a person purely from their characteristic writing style. Although graphologists can *claim* to further determine a persons character traits solely from their hand-writing, signature-recognition focuses only on the verifiable characteristics of the user's writing style and separates the biometric markers into two groups:

- **Static Markers**: Writing geometry, curvature, shape and histogram.
- **Dynamic markers**: Writing direction, speed, pen-up/down and pressure.

[1] Generic suitability in principle. In practice, mobile speaker-recognition is limited by factors including: handset microphone quality, security system centricity, voice codec, bandwidth of the medium.

Signature-recognition systems currently only command 2% of the biometrics market share (see Figure 4-7), reflecting the current market trend away from signature based authentication, and towards the market dominant and convenient password/PIN based authentication in pre-enrolled systems. Some issues affecting signature-recognition are:

- relatively indistinct biometric markers (see Figure 4-6);
- debit card(s) widespread replacement of signature-authenticated cheques;
- Chip'n'PINs replacement of signature-authenticated debit/credit card receipts.

However, with the move towards, PDA style mobile devices (Section 1.1), more handhelds are appearing with palmtop style touch-screens and stylus, enabling some leveraging of existing hardware and software, in the form of handwriting-recognition, for authentication purposes. A key issue is how far this particular HCI technology can penetrate the mass market of mobile handsets. Touch-screen technology is an expensive commodity and is highly unlikely to appear on a device for purely security purposes.

4.3.3.3 Keystroke-Dynamics

Keystroke-dynamics takes advantage of behavioural differences in typing style on any keyed input device, usually a computer style keyboard or numerical keypad; the input device forming the access point to the protected environment. The behavioural markers are primarily user's inter-key latency and hold-down latency, which has been shown to demonstrate unique personal properties (Joyce and Gupta 1990). In a similar way to voice-recognition, keystroke dynamics can leverage existing hardware and be applied in two distinct modes of operation:

- **Constrained**: Text-dependent, via pre-determined words or phrases.
- **Unconstrained**: Text-independent, via free-typing.

A natural and commercially successful application of keystroke-dynamics is *hardening* existing password based authentication systems; a hybrid multi-modal approach, adding biometrics to a mature authentication mechanism (Link: BioPassword). Although offering relatively indistinct biometric samples, keystroke-dynamics non-intrusive nature enables it to continuously and cumulatively monitor a users typing behaviour and over time, statistically offset this vulnerability and reduce system authentication errors.

With traditional 2nd generation mobile handsets, the use of mobile phonebooks all but eliminated the use of the keypad in day-to-day use. However, the introduction of wideband networks and their enabled online services, has seen the evolution of the mobile handset into a device with similar capabilities to a PDA or palmtop computer (Section 1.1), with the associated human computer interface; this shift in technology re-enabling the possible application of keystroke-dynamics (Clarke *et al.* 2003).

Table 4-4 summarises the three principal *behavioural* biometrics techniques, identified in Figure 4-7 and discussed in this section, with a bias towards their inherent suitability for application within a small handheld mobile device, like a mobile handset.

	Market Share[1]	Non-Intrusive	Security Strength[2]	Template Size[3] (in Bytes)	Mobile Application
1. Speaker-Recognition	6%	✓	✓✓	2000+	Continuous
2. Signature-Recognition	2%	×	✓	~1500	Discrete[4]
3. Keystroke-Dynamics	<1% [5]	✓	✓	*Unknown*	Continuous

Table 4-4: Summary of behavioural biometric techniques for mobile application

[1] Extracted from Figure 4-7, the Pie chart: Biometrics Market Share by Technology.
[2] Extracted from Figure 4-6, the Zephyr diagram: Key Biometrics Criteria.
[3] Template sizes are not fixed, but represent typical sizes in current commercial systems.
[4] Authentication performed deliberately at a specific point within an operation.
[5] Inferred from Figure 4-7, the Pie chart: Biometrics Market Share by Technology.

4.3.4 Other Behavioural Techniques

In addition to the market dominant behavioural techniques discussed in Section 4.3.3, a number of alternate techniques are under investigation. An in-depth discussion of these techniques is beyond the scope of the thesis and they have been included here to demonstrate, once again, the diversity and breadth of biometrics.

4.3.4.1 Service Profiling

Behavioural profiling is the process of determining the identity of a person via their characteristic interaction with a system. It can describe a path of activity taken by a user to achieve a specific goal, or the order in which a list of tasks is usually performed on a regular basis; forming a profile. An example may be: Check email, use cursor keys to scroll; read the news on BBC News website, use mouse to select topics; exit system, use shortcut keys. Although the process is not unique enough to perform user identification, in a multi-modal system its strength lies in the fight against fraud, with its ability to non-intrusively and constantly monitoring a systems' users and flag behaviour which is *out of character* (Rogers 2001), for further investigation.

4.3.4.2 Gait-Recognition

Gait-recognition is a spatio-temporal biometric which leverages existing CCTV camera deployment to classify subjects' walking patterns (gait and stride), for either Simple Harmonic Motion (SHM) or statistical Principal Component Analysis (PCA). Although unsuitable as an access technology, its potential resides within automatic surveillance systems which can be used to trigger additional security responses, such as CCTV recording or a silent alarm, if a flagged template is detected within a controlled area. There are a number of DARPA research projects ongoing within this area (Link: ISIS(a)).

4.4 Biometrics and Mobile Handsets

The evolution of the mobile handset (Section 1.1) from a rudimentary telephony device into, a multi-functional personal mobile computer has had repercussions within the field of mobile biometrics. Although physically smaller than traditional palmtop and laptop computers, mobile handsets now incorporate many of their advanced human computer interfaces, which biometric systems designers can *lever* in order to realise *biometric* security approaches previously impossible owing to the size and cost of the enabling hardware. Figure 4-9, illustrates the biometric approaches discussed in the previous sections that are relevant to application within a mobile handset.

Figure 4-9 : Biometrics applicable to mobile handsets

With the addition of a high resolution camera[1], initially for photographic use and later, with the introduction of wideband networks, for video conferencing, 2-dimensional face-recognition and potentially even iris-scanning, is now a possibility.

[1] Pixel resolution of the CCD in the latest generation of mobile handsets is now realising 3 megapixels, with some specialist units reaching up to 6 megapixels (Grundig Mobile X5000).

Touch-screen technology from the PDA market, along with hand-writing recognition software, is enabling techniques such as signature-recognition. The improved dynamics of high-quality audio microphones, part of the 3rd generation rich-voice service (Section 2.2.3.3), is enabling speaker recognition. Although the reduction in size of the handset has dictated the size of the keypad, this has not eliminated the potential for keystroke-dynamics, research in this area has shown that even using just *thumbs*, there is still enough of a residual signature to perform authentication (Clarke *et al.* 2003).

	Biometric Technique[1]	Market Share[2]	Non-Intrusive	Security Strength[3]	Lever Existing Hardware	Mobile Application
Physiological	**Fingerprint**	48%	×	✓✓✓	Limited[4]	Discrete[5]
	Hand-Geometry	11%	×	✓✓	×	Unsuitable[6]
	Face-Recognition (2D)	12%	✓	✓✓✓	✓	Continuous[7]
	Iris-Scan	9%	✓	✓✓✓✓	Limited[4]	Continuous[7]
	Retina-Scan	<1%	×	✓✓✓✓	×	Unsuitable[8]
	Vein-Recognition	n/a	Possibly	✓✓✓	×	Unsuitable[8]
	Face-Recognition (3D)	n/a	✓	n/a	×	Continuous[7]
	Ear-Geometry	n/a	×	n/a	×	Continuous[7]
	Facial-Thermogram	n/a	✓	n/a	×	Unsuitable[8]
Behavioural	**Speaker-Recognition**	6%	✓	✓✓	✓	Continuous[7]
	Signature-Recognition	2%	×	✓	Limited[4]	Discrete[5]
	Keystroke-Dynamics	n/a	✓	✓	Limited[4]	Continuous[7]
	Service-Profiling	n/a	✓	✓✓	✓	Continuous
	Gait-Recognition	n/a	✓	n/a	✓	Unsuitable

n/a = information not available at time of writing

Table 4-5: Suitability of various biometric techniques to application within a mobile handset

[1] Techniques in bold are currently predominant within their particular discipline (see Figure 4-7).
[2] For the year 2004. Extracted from Figure 4-7, Pie chart: Biometrics Market Share by Technology.
[3] Extracted from Figure 4-6, Zephyr diagram: Key Biometrics Criteria.
[4] Leverage dependent on availability of advanced hardware.
[5] Authentication performed deliberately at a specific point within an operation.
[6] Owing to the size and inconvenience of the biometric collector.
[7] Whilst within a suitable mode of operation, e.g. video-conferencing for face-recognition.
[8] Requires the use of a suitable infra-red camera.

4.5 Assessing Subscribers' Attitudes towards Biometrics and Advanced Mobile Security

As part of the survey into public opinion of mobile telephony based security and related issues, covered in Chapter 3, four questions were composed to probe survey participants understanding and views on a selection of advanced authentication issues, including the topic of biometrics. The following section is a discussion and interpretation of the results to these questions. A full copy of the survey is included in Appendix C; with biometrics and advanced security being covered in sub-Section 3.

4.5.1 Users' attitudes towards biometric authentication

Participants were initially asked how they basically felt about biometrics and more specifically their own biometric markers, being used for the purpose of mobile authentication. The available responses were: Good, Bad or Indifferent.

Figure 4-10 shows a majority of 83% of respondents expressing the view that it is a good idea in principle. If this total is combined with the 13% of respondents who expressed no definite bias either way, the total without obvious objection to biometric authentication being incorporated into mobile handsets is 96%; a significant positive result.

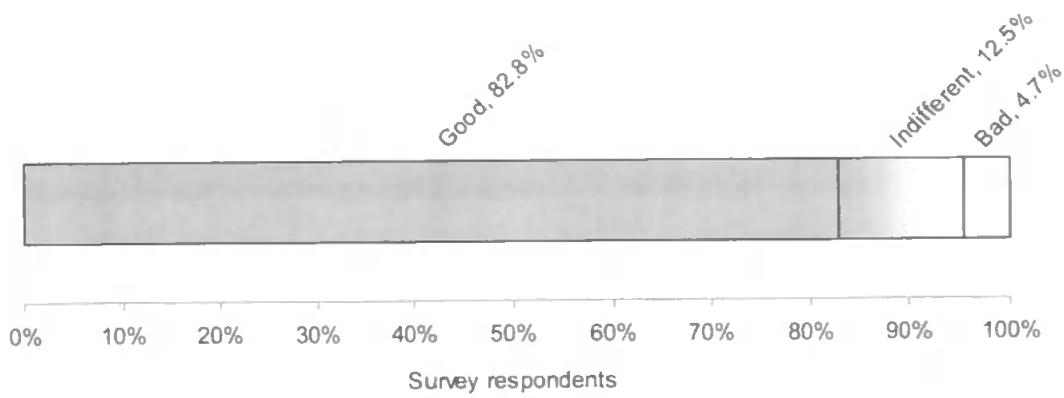


Figure 4-10 : Survey respondent's acceptance of biometric authentication

4.5.2 User's awareness and understanding of biometric techniques

Having established that the majority of respondents were accepting of additional authentication measures, the survey proceeded to assess their preferences towards the forms that the authentication could take. Having determined that PIN-based protection is problematic at best, it is considered that other authentication methods based upon something the user *knows* (e.g. password) would be equally under-utilised, inconvenient or vulnerable to similar masquerade attack. The implication of this is that the most sensible route for improving authentication is to base the approach upon some form of physiological or behavioural characteristic. Focusing on proven biometrics, participants were questioned on two levels: firstly, their awareness of a range of proven biometrics (Polemi 1997), both physiological and behavioural, and secondly their willingness to use the respective techniques within a mobile handset. Figure 4-11 summarises the results.

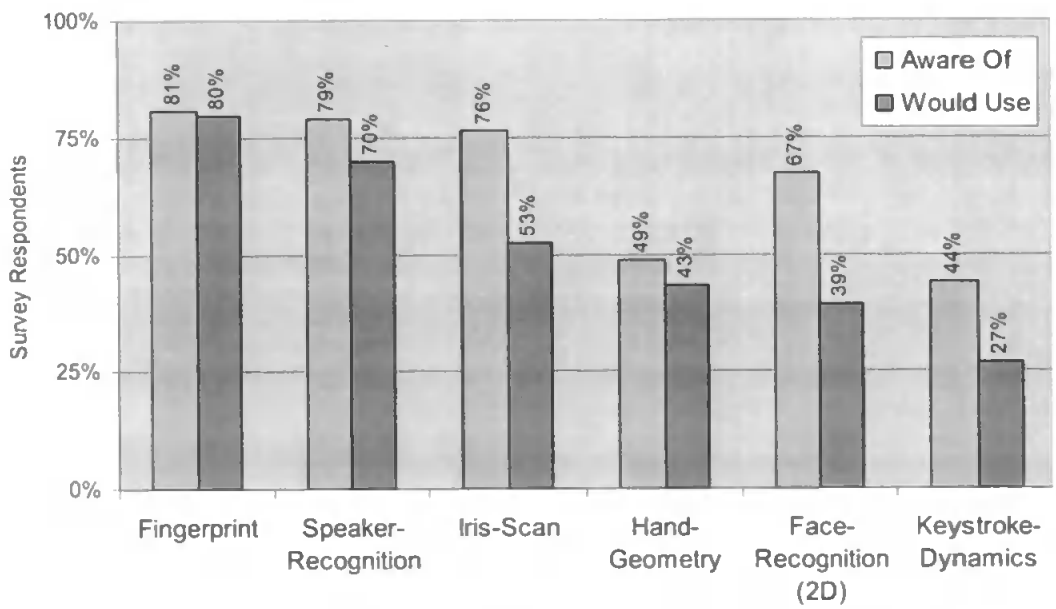


Figure 4-11 : Survey respondent's awareness and acceptance of biometric techniques

Having been known about for approaching 150 years (Herschel 1858) and forming the basis of police forensics for almost as long, the fingerprint received the greatest positive response in both the level of awareness and participants' willingness to use the

technique. Although the technique suffers the disadvantage of not being able to lever existing mobile handset hardware, but requires the incorporation of a dedicated biometric collector, as discussed in Section 4.3.1.1, confidence in this technique has already been demonstrated with some limited commercial success, through NTT DoCoMos fingerprint enabled handset; the F505i (NTT DoCoMo 2004). However, the fingerprint does not naturally lend itself to non-intrusive implementation (Table 2-1), as the user traditionally needs to pass his/her finger over a scanner at discrete times within a process, such as at the checkout within an ecommerce operation.

Speaker-recognition was also rated highly by respondents in both awareness and acceptance. Performing almost as well as the fingerprint, speaker-recognition has attracted much attention through the media and computer software, in addition to the mobile telephone industry, albeit predominantly as a means of voice activation of services, rather than as a means of authentication. As speaker-recognition depends upon the distinctiveness of the human voice, the development of hardware to support the increased frequency and dynamic-range of 3G's rich-voice service (Section 2.2.3.3) will lend itself naturally to the employment of this technique. However, owing to the vulnerability of this technique to pre-recorded authentication data, this technique can only realise its potential within a continuously monitoring environment.

Out of the biometric techniques provided, it is iris-scan which received one of the best results. Generally being considered an esoteric biometric approach, it was recognised by 76% of respondents and acknowledged by over half of all survey participants as being an acceptable biometric approach to authentication. This was somewhat unexpected, as biometrics relating to the eye, have traditionally been regarded with apprehension (IBG 2004). More unexpected, was the result that iris-scan was not only more familiar than face-recognition, but also preferred by a significant 14% of respondents.

Of the remaining techniques, which received less than half of respondent's confidence vote, hand-geometry received the healthiest vote, with 49%. However, it would have been interesting to question the 43% of respondents, who agreed to having used it, about how they expected the technique to be realised in practice within physically diminishing handsets! With only a third of the votes, face-recognition was an unexpected fifth in popularity; it is worth remembering at the time of the survey (during 2003), 3G was still undergoing testing and commercial video-conferencing was generally confined to desktop-computing. Although keystroke-dynamics naturally lends itself to non-intrusive authentication, facilitating a continuously monitored environment during appropriate keypad-oriented activity, the techniques' indistinct biometric markers (Figure 4-6), generally consign the approach to a support role within a multi-modal security system.

Caution should be exercised when drawing any conclusions from these results, as it is likely respondents may have responded more positively to those techniques with which they were already familiar, or which are proven in the eyes of the general population. For example, fingerprints have long been known to provide a means of successful and reliable identification, long before any forms of electronic scanning. The point, therefore, is not to regard the results as a conclusive attitude towards one technique over another. The key observation that can be made is that, in support of the previous question, all techniques were considered favourably, by at least 25% of respondents and if a particular technique were to be implemented that was less well known, a degree of re-education and awareness raising would be necessary before wide scale acceptance.

4.5.3 User's impression of continuous authentication

One advantage certain biometrics offer when compared to the PIN technique, is that they offer the potential for authentication to be performed on a continuous basis rather than as a one-off, usually PoE, judgement. Respondents were, therefore, asked whether they considered continuous authentication during mobile service usage to be acceptable; with the possible responses again being: Good, Bad or Indifferent.

The results, shown in Figure 4-12, reveal that 61% of respondents considered continuous authentication to be a good idea, which if accumulated with the indifferent respondents in a similar way to Section 4.5.1, gives a healthy 83%. Accepting that these 83% of users would likely be unwilling to regularly break their normal mobile activity to perform manual authentication, as discussed previously (Table 4-5) certain non-intrusive authentication techniques clearly lend themselves to this task more than others, such as:

- **Speaker-recognition:** *talking* is still the top activity on mobile handsets.
- **Face-recognition (2D):** with the introduction of mobile video-conferencing.
- **Keystroke-dynamics:** with the popularity of mobile texting (SMS).
- **Service Profiling:** for security, rather than targeted advertising

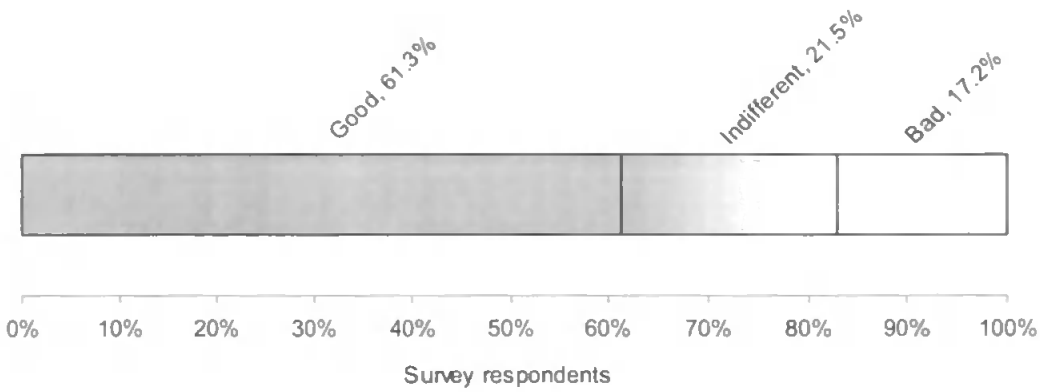


Figure 4-12 : Survey respondent's acceptance of continuous authentication

4.5.4 Storing biometrics' templates

For all authentication techniques, including the PIN, a template needs to be stored as a reference, so as to enable the comparison with new authentication input data. The final objective of the survey was to establish users' opinions on where they would prefer their biometric template(s) to be stored; either in the handset and the responsibility of the subscriber, or in the network and the responsibility of the network operator. In Section 2.3.7, the advantages and disadvantages of terminal vs. network-centric security profiles were discussed in detail, with the conclusion that a network-centric solution ultimately offered the more elegant and powerful solution.

Where a preference was expressed, survey respondents clearly favoured the profile being stored in the handset, with 50% of respondents selecting this option. By contrast, 33% favoured the network and 17% had no preference. The discussion in Section 2.3.7 highlights that this issue is in fact far more complex than simply a matter of privacy, but systematically affects issues such as, personal mobility and corporate liability. It would be wise, therefore, to acknowledge that as respondents were not explicitly made aware of all the issues, that perhaps a part of this result is biased by respondent's ignorance of the holistic view and the benefits a network-centric solution can in fact offer.

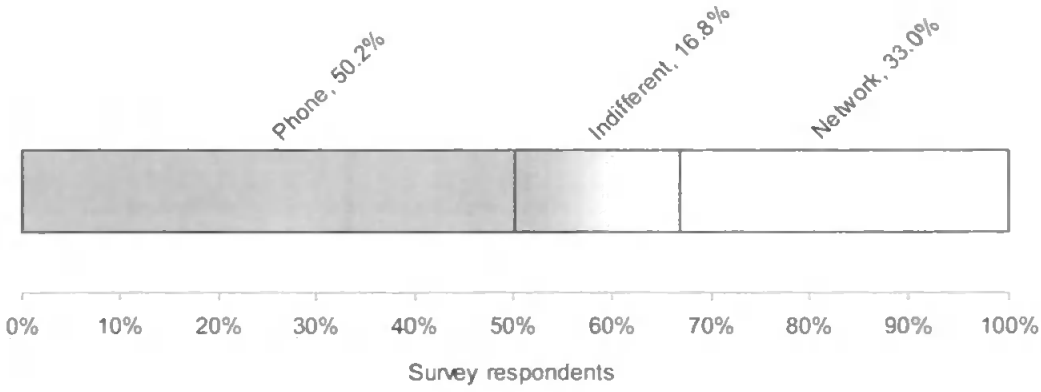


Figure 4-13 : Survey respondent's preference for biometric-template storage

4.5.5 Conclusion

This chapter presented an introduction to the area of biometrics and biometric security, with a bias towards the authentication system within current 2nd generation (GSM) mobile telephony handsets.

Much research has already gone into developing biometric techniques into practical systems, and many are already employed as alternative authentication methods within the desktop PC environment. For example, 9% of respondents to the 2001 CSI/FBI Computer Crime and Security Survey claimed to use biometric security technologies (CSI 2001). In the year 2000, Sagem were one of the first commercial companies to incorporate biometric authentication into a mobile handset; a fingerprint scanner within the back panel of the Sagem MC959 (SAGEM 2000), this technique being more recently incorporated into NTT DoCoMos, F505i (NTT DoCoMo 2004) handset in Japan. Although many biometric approaches would have traditionally required the incorporation of dedicated capture hardware, the move towards wideband 3rd generation handsets and services is enabling operators to compliment the existing PIN-based system, with a more powerful continuously monitored authentication system, through leverage of the new advanced services enabling hardware. For mass-market devices component cost is a major consideration, handset prices are already heavily subsidised by network operators in the current business model in order to keep the start-up cost down for the consumer, at the expense of buying into a contract.

It is the consumers in todays market that dictate the success or failure of a product, so some accommodation for their attitudes and opinions is not only wise, but fundamental.

The user survey continued from Chapter 3 addressed consumer views on the topic of advanced authentication and biometrics, with strong support for the more popular and familiar biometric techniques, and good overall support for biometrics in general. Since none of the biometric techniques discussed can provide non-intrusive authentication under all possible scenarios, it would seem logical that a hybrid multi-modal authentication system presents ultimately the best solution, drawing on a number of non-intrusive techniques as the first line of security, with perhaps the PIN (or some other knowledge-based methods) providing traditional PoE security and a fallback line of defence, if required.

In the next chapter, an innovative authentication technique appropriate to mobile application is introduced, which in addition to leveraging existing mobile hardware, presents a completely novel hybrid approach to biometric authentication, utilising both the physiological composition of a user's head along with the behavioural characteristics of the speakers voice to realise a unique biometric sample. The technique is known as the Head Authentication Technique.

Chapter 5

Conception of the Head Authentication Technique

5 Conception of the Head Authentication Technique

Security deficiencies within the current mobile authentication methodology highlighted in previous Chapters, are not themselves a product of the growth in mobile communications; they have always been present. It is the growth in data services enabled by developments in mobile communications infrastructure, which has resulted in the imbalance in security commensurate with the services they are now expected to protect.

This chapter introduces a novel biometric technique conceived to redress this imbalance. Building on the biometric approach proposed in Chapter 4, and the advanced authentication findings (Section 4.5), of the security survey covered in Chapter 3, the proposed technique levers existing mobile HCI behaviour to enable a unique multi-modal approach where selected physiological and behavioural characteristics work in symbiosis. The technique is known as the **Head Authentication Technique**.

5.1 Introduction

The Head Authentication Technique (HAT) was conceived out of the established need (Section 2.3) for an effective and reliable authentication system, capable of continuously verifying the claimed identity of a user accessing the advanced voice activated services of a wideband mobile network[1], usually through use of a compact mobile handset. The main requirements, from both an academic and commercial perspective (Orange PCS), were for a novel authentication approach that could deliver the following four key security advancements:

[1] The PhD requirement, as defined by the researches industrial sponsor, specifically targeted the data services enabled by 3rd generation wideband mobile networks: Orange PCS (Link Orange).

- **Improved user-identity verification**, through use of more unique and personal authentication templates.
- **Non-intrusive authentication**; authentication transparent in use to the network user, enabling an authentication cycle to be initiated at will by either an application, a security sub-system or the network operator.
- **Continuous authentication**; overcoming, for example, circumvention of the traditional PoE authentication request by simply not turning the device off.
- **Capable of leveraging existing mobile hardware**, and recasting it into additional security roles, such as facial recognition through use of mobile video conferencing hardware.

To further elaborate on these requirements: improved user-identity verification can only realistically be achieved through use of more personal user authentication data. The discipline of biometrics naturally lends itself to this task, providing various proven techniques (Section 4.3) designed and refined to distil unique personal physiological and/or behavioural characteristics from a human subject. Biometrics also offers the added benefit of a selection of current techniques capable of *passive* implementation, not requiring the conscious interaction of the subject, conveniently providing a path to the second research requirement of a non-intrusive authentication system. Non-intrusive authentication is itself a pre-requisite of a *usable* continuous authentication system, thus mutually addressing the third research requirement. The fourth requirement for a solution suitable for application specifically within a mobile device, preferably utilizing the established tools of that context, was fundamental in defining the scope of the research, and although tempering many otherwise promising authentication solutions, did ultimately realise the original and novel approach of HAT.

Once it was established that biometrics theoretically offered the best research area from which to draw a solution, as an intellectual exercise preceding any development work on a novel biometric approach, all known biometric techniques[1] were reviewed in depth (Section 4.4), with a view to potentially leveraging attractive and/or relevant features into a mobile context. During a number of brain-storming sessions many new and original ideas were considered outside of their original design context, such as keystroke dynamics on a mobile handset keypad using only ones thumbs (acknowledging the phenomenal growth in SMS), or the more controversial (though not entirely novel) idea of human Radio Frequency IDentification (RFID) 'SIM' chip implants (BBC News 2004); similar in principle to the established procedure of electronic animal tagging (Link: Biomark). By taking the idea of applying established biometric approaches out of context to the extreme, selected biometric techniques were considered completely outside of their traditional operational envelopes. If applied in unconventional ways, certain biometrics theoretically offered a novel lease of life, such as voice-recognition where biometric samples are captured at a user's ear, rather than traditionally at the mouth. It was from these sessions that a set of head authentication approaches based on sound (covered in Section 5.3.2.2), was conceived and submitted for patent approval (see Appendix I): one of these approaches was developed through proof-of-concept into HAT.

5.2 The Human Ear and Auditory Analysis Techniques

The Head Authentication Technique utilises the ear as part of a multi-modal biometric approach. Although the HAT process itself is original, identifying a person by some unique characteristic of their ears alone is not, and an example of this is discussed after a description of the human ear and its natural acoustic partner, the voicebox.

[1] Including: established commercial (eg. Fingerprint, Hand geometry), developmental (eg. 3D facial recognition, Gait recognition), and experimental (eg. Ear geometry) techniques.

5.2.1 Hearing and Anatomy of the Human Ear

The human ear is a bi-functional organ, containing structure for both the primary sense of hearing, and the bodies balance organs. The structure of the human ear extends up to 60mm into the average adult head and is connected to the brain by the eighth cranial nerve (the vestibulocochlear nerve), carrying nerve impulses for both of the aforementioned functions. A young and healthy ear has an operational frequency range of approximately 20Hz to 20,000Hz[1] and a dynamic range of about 100 decibels (see Figure 5-7). With reference to Figure 5-1, the human vocal range is restricted to the frequencies 80Hz to 7000Hz, with the natural spoken voice covering the narrower band, 80Hz to 300Hz (Baken & Orlikoff 1999): trained operatic (singing) voices cover the extended frequency range 80Hz to 1400Hz (Link: Vocalist).

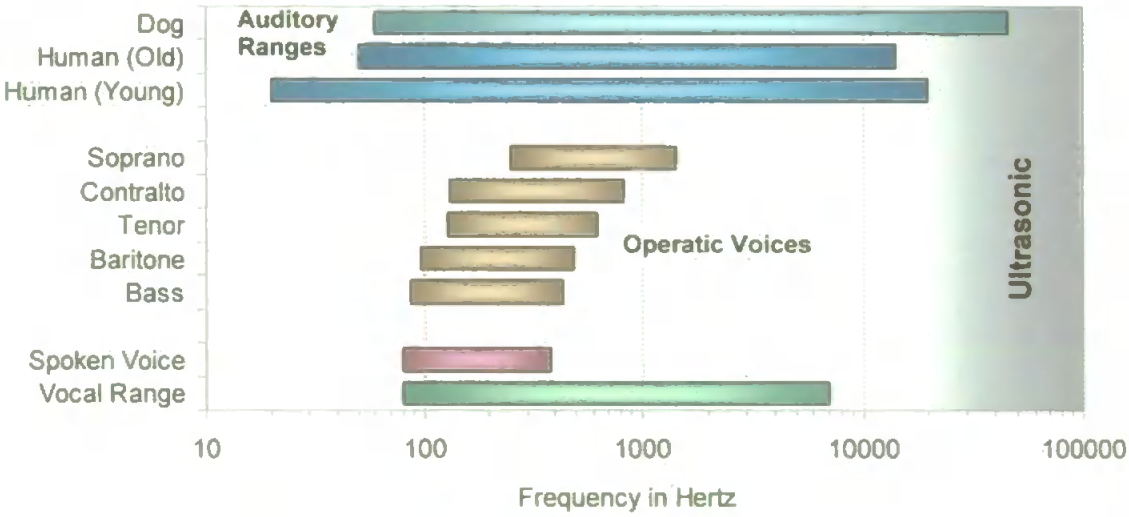


Figure 5-1 : Frequency ranges of the human vocal and auditory systems

Physiologically, the ear can be divided into three basic parts, defined by their function:

- **Outer-ear:** Collection and channelling of sounds into protected middle-ear.
- **Middle-ear:** Translation and amplification of sound waves into vibrations.
- **Inner-Ear:** Filtering and transmission of individual frequency data to the brain.

[1] Over time the ear's upper frequency limit naturally degrades, reaching around 15KHz by age 60 years.

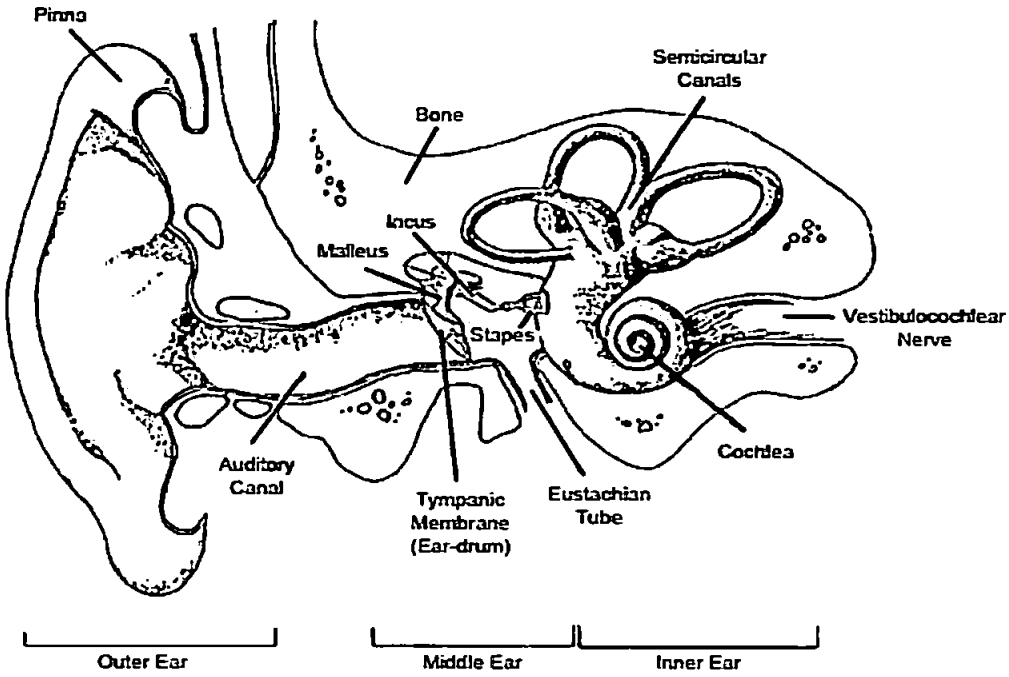


Figure 5-2 : The anatomy of the Human Ear[1]

The actual function of hearing is caused by sound pressure waves striking the pinna, or external structure of the **outer-ear** (see also Section 5.2.2), where they are channelled into the auditory canal and down to the tympanic membrane, commonly referred to as the ear-drum. The ear-drum forms an air interface between the outer-ear and the semi-sealed air-filled cavity of the **middle-ear**. The middle-ear contains a triplet of small bones (unique to mammals) called the ossicles, referred to in Latin as the Malleus, the Incus, and the Stapes; sometimes called the hammer, the Anvil and the Stirrup, owing to their shapes. The Malleus is attached directly to the ear-drum, and the triplet forms a mechanical linkage evolved to amplify the pressure wave at the ear-drum by a factor of around 22 times (in a healthy ear), converting it from a mechanical wave into vibrations for transmission into the cochlea. The cochlea is part of the **inner-ear** and comprises a fluid filled spiral canal separated by a membrane called the basilar membrane which contains tens of thousands of small hairs divided

[1] Adapted from an original image located on the 'New York State Disabilities Awareness' website.

into four rows of inner and outer hairs. The outer hair cells (OHC) receive *input* from the brain influencing their motility and the sensitivity of the cochlea to differing amplitudes of sound. The OHCs are also the source of the auditory response anomalies known as otoacoustic emissions (see Section 5.2.3.1). The inner hair cells (IHC) provide the primary neural *output* of the cochlea. The hairs are all of slightly different lengths and individually have natural sensitivity to specific frequencies. When the frequency of the compression wave in the cochleal fluid matches that of an IHC, the cell induces a unique electrical impulse in the auditory nerve; collectively, these impulses are interpreted by the brain as sound.

5.2.1.1 The Eustachian tube

The Eustachian tube performs the vital role of maintaining the compliance of the ear-drum, by balancing the pressure in the air-cavity of the middle-ear with the outside air pressure: it also forms the most direct link between basic HATs two sample capture points.: the mouth and the ear. The tube directly connects the middle-ear to the upper nasal cavity, and contains a selective valve which opens and closes to balance the internal and external air-pressure; this can sometimes be felt as the familiar 'popping' sensation when large changes in air-pressure are experienced in a short period of time. Leading up to the effect, the subject will also usually notice a reduction in hearing efficiency caused by the pressure imbalance reducing the compliance of the ear-drum and the efficiency of the middle-ear apparatus. A similar effect can be experienced when the Eustachian tube becomes blocked due to infection, such as a cold, and is unable to equalise the pressure: the unnatural (unbalanced) middle-ear pressure at these times can also, in extreme cases, lead to dizziness and headaches.

5.2.2 Ear-prints and 'earology'

Almost a century before fingerprints were first used as a mode of identification, Johann Caspar Lavater (1741-1801)(Link: Lavater), Theologian and physiognomist, had been working on the 'individualization in the design of the human ear', a practice which came to be known as 'earology'. In the 1960's Alfred Iannarelli, a deputy sheriff in the United States, tried to turn the concept of ear-identification into a recognised science, devising an ear-print classification system and writing the first book dedicated solely to the subject, "Ear Identification" (Iannarelli 1964). Although Iannarellis's work and ear-prints in general have never been widely accepted by the scientific community, recent cases within the criminal justice system have brought the subject of ear-prints and ear-print classification to the fore.

In October 1991, in the first case of its type in the United States, ear-print evidence was used to convict David Kunze of aggravated murder, burglary and robbery (Morgan 1999). At the Court of Appeals, the conviction was later overturned after essential ear-print evidence, previously deemed admissible by the judge, was subsequently ruled "unsafe". The change was primarily due to forensics expert witness testimony describing the ear-print technique as "not generally accepted" as a form of forensics due to the discipline being in its infancy (CoA 1999). The case did however highlight the first appearance of ear-print evidence in a court of law.

In a similar burglary and murder case in the UK in 1998, Mark Dallagher was convicted of unlawfully killing an elderly lady after the prosecution showed that ear-prints on a newly washed window could only have been left by the accused as he listened for movement inside the house (BBC News 1998). The case set a precedent and following the conviction, the British police force, through association with the National Training

Centre for Scientific Support to Crime Investigation (NTC-SSI)(Link: NTC), pioneered a national database of ear-prints to provide evidential support linking suspects to crime scenes, in a similar procedure to fingerprints (BBC News 1999). Since the database was started, police have investigated over 100 cases of ear-prints at crime scenes.

The importance of these developments in relation to the research is the formal recognition of the unique nature of the outer-ear, or pinna (Figure 5-2), which forms part of the physiological authentication chain effecting the biometric template produced by the Head Authentication Technique.

5.2.3 Auditory Evoked Responses & Otoacoustic Emissions

In the Introduction, HAT was presented as an authentication system borne out of the novel application of selected established biometric disciplines in unconventional ways. Possibly the closest recognised field to the proposed research approach, is the clinical auditory diagnosis technique of Otoacoustic Emissions (OAE), part of the broader discipline of Auditory Evoked Responses (AER).

An Auditory Evoked Response can be described as activity within the auditory system, (consisting of the ear, the auditory nerve and the brain), that is produced or excited by acoustic stimuli. Major AER techniques like Auditory Brainstem Response (ABR) and Electro-cochleography (ECochG) rely on a 'brain response' to a specific stimulating sound to produce their output. Although they do not require explicit subject interaction, from an overall research perspective the dependence of these techniques upon medical procedures unsuitable for translation into a distributed mobile environment, ruled out further research into the procedures: specifically their dependence on multiple skin-contact electrodes strategically positioned on the subjects forehead.

OAEs depend upon similar non-interactive stimuli to generic the AERs but differ in one major area, their stimuli delivery and data collection procedure depends on a single transducer device positioned in the subject's outer-ear. As this is the natural position of a mobile handset when being used for a traditional voice call, the procedure warranted further investigation within the context of the research.

The investigation into OAEs was conducted with the dual research objectives of investigating the techniques potential for re-engineering and deployment within a security orientated role or as a potential enabling technology for a novel biometric authentication approach. To achieve these objectives, the investigation was performed on three levels:

- A familiarisation with OAEs operational medium, the human ear (Section 5.2.1).
- An investigation into OAEs in their various forms, and the enabling technology.
- A practical evaluation of OAEs, through tests at a suitably equipped local hospital in order to experience and assess OAEs real-world potential from a user's perspective. This was performed at the Ear, Nose and Throat (ENT) department of Derriford Hospital, Plymouth, UK.

5.2.3.1 Introduction to OAEs

Discovered in 1978, by Dr. David Kemp (Hall 2000, pp.9-14), Otoacoustic Emissions are a relatively new field of audiology. The emissions are a spontaneous and naturally occurring bio-mechanical process caused by the compression and rarefactions of air in the ear canal (of a person with normal hearing ability), by inner-ear stimulation of the ear-drum (Figure 5-2). The difference between OAEs and the normal reactions of the ear-drum to the functions of breathing, speaking and the beating of a heart, are that

OAEs originate from the rows of outer hair cells (OHC) in the cochlea of the inner-ear (Section 5.2.1). Travelling sound waves entering the cochlea which are not entirely absorbed by the inner and outer hair cells build up and eventually can no longer be completely contained within the cochlea. This process causes the OHCs in the cochlea to scatter energy back to act upon the middle-ear apparatus, where it is relayed to the ear-drum producing the reactive sounds within the ear canal known as OAEs.

The medical discipline of OAEs is the retrieval and analysis of these natural responses to artificially shaped acoustic stimuli, and are used to compliment the traditional and well-established audiogram in the diagnosis of auditory problems. Although OAEs are produced solely by the outer hair cells of the cochlea, the technique can also reveal the condition of the ear-drum and middle-ear apparatus, by producing recognisable responses for specific auditory problems, including:

- congenital hearing loss;
- abnormal middle-ear function;
- dysfunction of the nerve cells in the cochlea.

In common with biometric techniques for authentication (Section 4.2.2), normal OAEs vary over time. The primary factors influencing OAE variance and performance are:

- Age.
- Gender.
- Body temperature.
- State of arousal.
- General condition of the ear apparatus.
- Additional medical conditions and/or medication.

5.2.3.2 Capturing OAEs

In order to record the OAEs, a probe containing an earphone and microphone, is fitted into the ear canal of the outer-ear. As the emissions would otherwise dissipate in the freely moving air of the ear-canal, the probe must make an air-tight seal with the outer-ear, isolating the small trapped volume of the ear canal and producing internal pressures up to an audible 30dBs. The probe, which is connected to an OAE analyser (currently of similar size to a laptop computer), delivers the auditory stimulus and the response to the stimulus is measured by a microphone in the probe tip. As the OAEs derive from the originating stimulus, they are synchronised and contain the same frequencies, only delayed by a few milliseconds, due to the slower travelling wave in the cochleal fluid: in addition, subjects' left and right ears exhibit a high degree of correlation.

5.2.3.3 OAE Stimuli

Although the inner-ear will apply the same effective transfer function to all acoustic stimuli, otoacoustic emissions can be divided into two broad categories; spontaneous emissions and artificially evoked emissions, where:

- **Spontaneous Otoacoustic Emissions (SOAE)** are the naturally occurring emissions from the normal everyday uncontrolled stimulation of the acoustic world. These emissions, caused perhaps by a car driving past, are rarely used for analysis purposes, and thus are not pursued further within the research.
- **Evoked Otoacoustic Emissions (EOAE)** are the emissions occurring as a direct result of a tightly controlled artificial stimulus. Evoked emissions are grouped according to their type of acoustic stimulus, which can be varied in frequency, intensity, spectral shape and duration according to the requirements of the analysis and the condition (response) of the subject's ear.

There are generally three accepted forms of evoked OAEs, divided by stimuli:

- **Transient Evoked Otoacoustic Emissions (TEOAE)** are generated by a series of short duration tone-bursts, heard by the subject as clicks. Each click is a combination of overlapping frequencies designed to stimulate those hair-cells in the cochlea sensitive to the respective frequency. Owing to the relatively poor signal-to-noise ratio of TEOAEs, accuracy is highly dependent on the averaging of a suitably large set of test data, and the upper test frequency is limited to 4000Hz. The average time needed to perform the otoacoustic analysis using this technique is 1-2 minutes (Grason-Stadler ca.2000).
- **Chirp Evoked Otoacoustic Emissions (CHEOAE)** are an evolution of TEOAEs protocols, where the stimulus is engineered to provide an improved system signal-to-noise ratio. The 'chirp', which consists of a short frequency sweep, produces similar emissions to the 'click' (of TEOAEs), but contain a lot more energy for the same amplitude (Newmann 1997), reducing analysis times to less than 1 minute (Grason-Stadler 2000).
- **Distortion Product Otoacoustic Emissions (DPOAE)** are emissions generated by a series of close ratio primary tone pairs (where $F_R=F_2/F_1\approx1:1.2$), presented in an ascending or descending frequency pattern. When the pure tone pairs arrive at the cochlea, they stimulate their respective groups of hair cells, setting up vibrations in the hair cells located between the two groups. These additional vibrations generate a third tone, known as the distortion product or intermodulation product. DPOAEs exhibits a far better signal-to-noise ratio than TEOAEs, are therefore more efficient at producing reliable results and can test frequencies up to 8000Hz. The average time needed to perform an otoacoustic analysis using this technique is 30 seconds (Grason-Stadler 2000).

5.2.3.4 A Practical Evaluation of OAEs for an Authentication Role

In March 2002 arrangements were made for the author to experience a series of otoacoustic tests first hand; to be performed at the Ear, Nose and Throat (ENT) department of the local hospital: Derriford Hospital, Plymouth, UK. The aim of the tests were to access OAEs practical potential for reassignment from an auditory diagnostics role to a user authentication role, both from a technological viewpoint and from a public acceptance viewpoint. With the authentication objective firmly in mind, the test environment was also conducive with conceiving alternate research ideas, utilising OAE techniques as donor technology.

As stated in Section 5.2.3.1, otoacoustic emissions rely on a healthy auditory chain from the ear-drum to the hair cells in the cochlea of the inner-ear. It is therefore standard procedure to first ascertain the normal working function of both the middle-ear and inner-ear via alternate established test procedures, in this case the tympanogram and the audiogram respectively. All auditory tests took place in a closed sound proof room, with an ambient noise level less than 10dBs. Tests were conducted in the following order:

- **Tympanogram** for ear-drum and middle-ear function.
- **Audiogram** for IHC (hearing) and inner-ear function.
- **OAE** tests for OHC and full auditory chain function.

5.2.3.4a Tympanogram

The Tympanogram is used to detect disorders of the tympanic-membrane or ear-drum and the triplet of small bones comprising the middle-ear (Figure 5-2). The test involves inserting a tight fitting probe into each ear, then pressurising and rarefying the air within the ear-canal in order to test the mobility of the middle-ear apparatus, detecting disorders such as a perforated ear-drum, detached ear-drum or middle-ear fluid ingress.

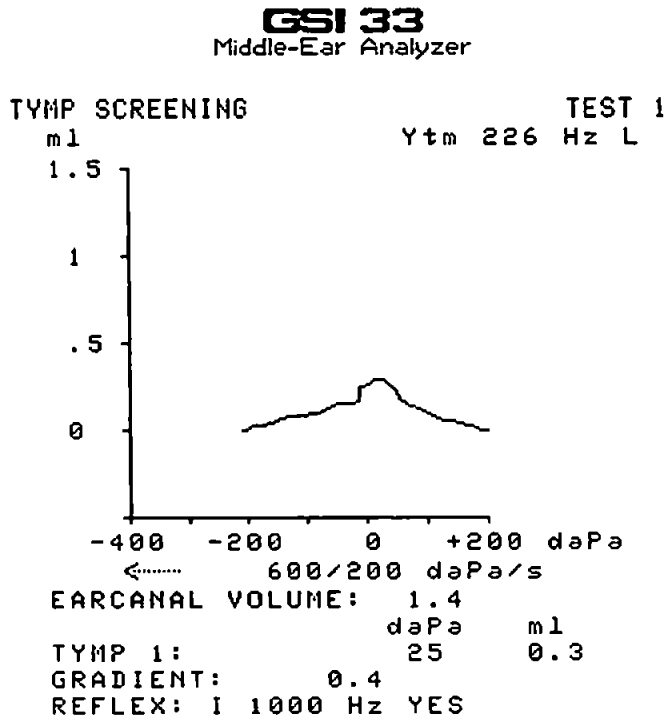


Figure 5-3 : Clinical Tests - Tympanogram

Figure 5-3 shows the tympanogram for the right-ear. The result shows a typical response for a normal ear, symmetrical around room pressure and indicating that the:

- eustachian tube is clear and the middle-ear is correctly at outside air-pressure;
- ear-drum is responding appropriately to pressure waves input in the ear-canal;
- ear-drum is correctly seated at the juncture between the outer and middle-ear, forming a compliant pressure seal with the outside air-pressure;
- small bones of the middle-ear are mutually connected and moving normally.

5.2.3.4b Audiogram

The audiogram is the traditional *hearing test* and is used to reveal the condition of the inner hair cells (IHC) of the cochlea (Section 5.2.1), after determining normal middle-ear behaviour. The test can be performed via either bone-conduction or air-conduction, the latter being the more prevalent where the subject wears a set of good quality 'full

cup' headphones. The test consists of a frequency sweep of discrete pre-selected pure tones into each ear at random time intervals in the frequency range 250Hz to 8000Hz; the approximate frequency range of the voice human box. The subject either acknowledges receipt of each tone via pressing a button on a handheld unit, or not if the tone went unheard. The random nature of the inter-tone time interval excludes guesses.

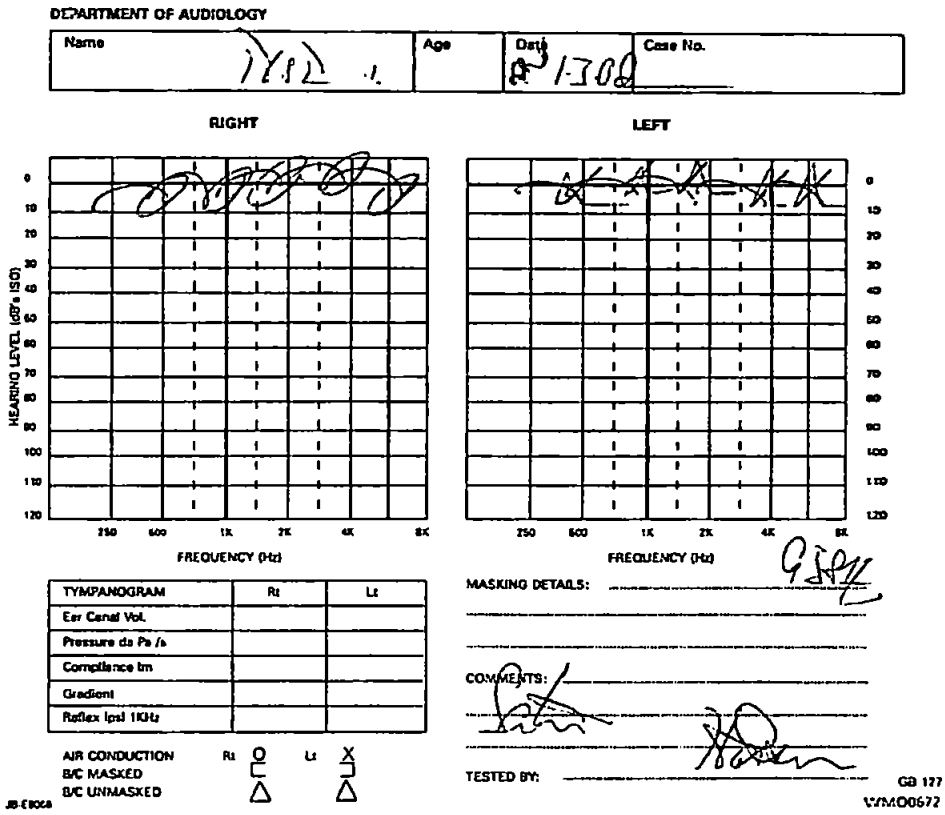


Figure 5-4 : Clinical Tests - Audiogram

The audiogram result is shown in Figure 5-4, and indicates all frequencies between 250Hz and 8000Hz were detected successfully at less than a test amplitude of 10dBs, with only a slight reduction in sensitivity in the right ear at around 500Hz. Results up to 20dBs are considered normal, making this an excellent result, indicating healthy cochlea function: the IHCs are functioning across the full test frequencies spectrum showing no signs of auditory abuse or premature aging, transmitting the appropriate impulses into the auditory nerve which are being received and correctly interpreted by the brain.

5.2.3.4c Otoacoustic Emissions

Having establishing normal function of the middle-ear and IHCs of the inner-ear via the tympanogram and audiogram respectively, the OAEs test can be performed on the outer hair cells (OHC) of the cochlea. The testing required the insertion into the ear canal of a suitably selected *bung* in order to form an air-tight seal with the outer-ear enabling pressurisation of the ear canal. The test equipment available to the ENT department at the time was an IL088 OAE analyser (one of the first and most popular OAE analysers) utilising two simple air tubes passing through openings in the bung and into the OAE analyser, retaining the transmission and reception circuits within the analyser. Being an early device, the analyser utilised the original technique of TEOAEs detailed previously, averaging over time a discrete frequency sweep from 500Hz to just over 4000Hz, with transient *click* stimuli of 1ms duration at a pressure of 3 Pascals.

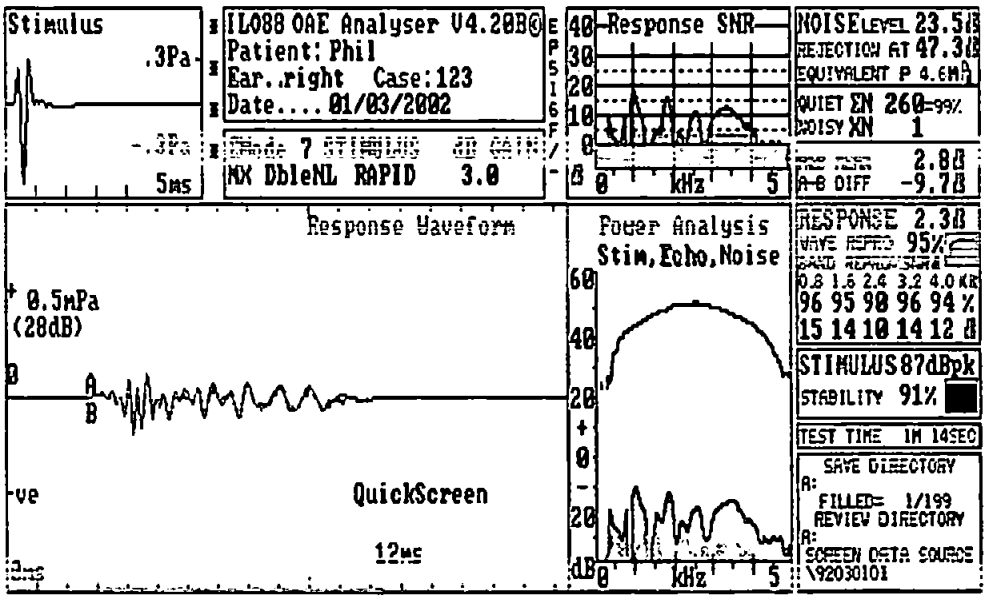


Figure 5-5 : Clinical Tests - Otoacoustic Emissions

Figure 5-5 shows the result of the OAE test. By inspection, the 'Response Waveform' indicates the clear presence of OAEs in response to the *click* 'Stimulus', indicating healthy cochlea OHCs and middle-ear function. Test duration was 1 minute 14 seconds.

5.2.3.4d Clinical Tests Conclusion

In association with the resident audiologist, the clinical tests proved a highly valuable exercise with regard to the research. The OAEs tests highlighted a number of important points which, in their current form, precluded TEOAEs from meeting the research requirements outlined in Section 5.1. In order of severity the precluding points were:

- All OAE techniques rely upon the insertion of a hermetically sealed probe into the subject's ear canal.
- The resultant unnatural and uncomfortable pressurisation of the subject's ear.
- A normal test duration cycle in excess of one minute.
- The need for a quiet environment for the collection of usable OAE data in an acceptable time; around 1 minute for a normal clinical diagnosis.

The outcome did however justify the exercise, as the tests spawned the concepts which shaped the future direction of the research. The Head Authentication Technique was developed from the following ideas borne out of the OAE clinical tests:

- Biometric templates derived from acoustic stimulation of bio-matter.
- The use of the voicebox as an internal stimulus; in the range 50Hz to 8000Hz.
- The *capture* of biometric sample data at a subject ear.
- The bio-matter between a subject's voicebox, their mouth and their ear(s) providing the source of variance in the stimulus.

The next section of the thesis explores these concepts in more detail, and introduces the fundamental principles for the head authentication technique, including the intellectual property which came to be included in the patent protecting the research.

5.3 The Human Head and Acoustic Head-Recognition

The head is the most visually individual and distinctive aspect of the human body, providing the primary form of post-natal[1] person-to-person identification. Collectively, it contains many unique biometric markers, which humans are capable of assimilating instantly and continuously, comparing the visual data (from persons in 'line of sight') with a memory of templates stored in the brain. Many of the current biometric approaches also harness the authentication potential of the human head:

- **Behavioural techniques,** by definition, are dependant on the brain, with any respective physiological traits having only a minor influence[2].
- **Physiological techniques** based on some property of the head include: face recognition, face-thermography, iris-scan, retina-scan, ear-print (Section 4.3.1).

The Head Authentication Technique takes a completely original and novel approach to the subject of authentication. With the exception of face-thermography, current head sourced biometric approaches are based on individual *visual* aspects of the head, a natural progression of the primary form of human identification. HAT however, uses *sound* rather than *light* to authenticate a user; producing a biometric template based on the spectral variance introduced by the human head on an acoustic stimulus, not an artificially generated stimulus such as OAEs use, but the richly complex stimulus of the human voice. HAT simultaneously captures and compares two separate samples of the sounds produced by the larynx (henceforth referred to by its common name, the 'voicebox') situated in the throat, recorded at two separate locations on the subjects head: the mouth (when talking) and the outer ear. It then compares the average amplitudes at multiple frequency points to produce a biometric 'absorption' template. The principles supporting this approach are detailed in the following subsections.

[1] Up to the age of 2 months, infants identify their parents primarily using the senses of smell and sound.
[2] The physiological effects on a behavioural biometric will be increased if physiological defects exist.

5.3.1 Anatomy of the human head

The biometric authentication principle utilised by HAT are dependent upon the way sound propagates *through* the human head. HAT's biometric template is essentially a record of spectral variance on a band-limited acoustic stimulus introduced at the base of the head, and measured at the head's two natural sound interfaces with the outside world: the mouth and the (outer) ear. To understand what is happening to the sound waves as they propagate through the head, it is necessary to understand the biological composition of the head.

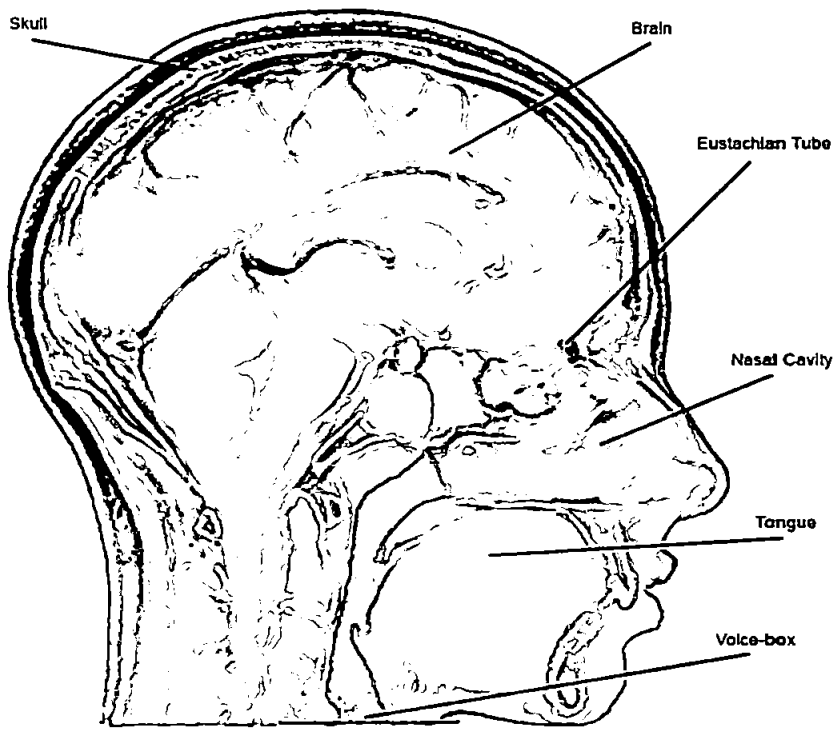


Figure 5-6 : MRI vertical bisection of a human head

One of the best ways to dynamically *look inside* a healthy living head for research purposes is using Magnetic Resonance Imaging (MRI)[1]. MRI is a technique for creating cross-sectional images, or slices, of opaque organs inside of living organisms (Hornak 2006). Figure 5-6, shows an MRI vertical bisection of a human head.

[1] MRIs correct title is, Nuclear Magnetic Resonance Imaging (NMRI). It was found however that, within medical practice, the term 'nuclear' encouraged a negative client image and is therefore usually dropped.

The head forms the upper part of the human body. The front (ventrum) contains the face, with organs enabling four of the five senses and associated physiological biometrics (Section 4.3.1): the head is also the repository of the brain enabling all behavioural biometrics (Section 4.3.3). The bones which encase the majority of the human head, of which there are in excess of 20 plates, are collectively called the skull, and separately the mandible or jawbone; in addition to enabling eating and chewing, the jawbone is fundamental to the formation of speech. The majority of the skull is filled with the brain, one of the largest and the most important organs in the human body. The brain is important to HAT, not directly for its mental capacity but, as with the other elements of the head, for its physical characteristics and the resultant effect on the propagation of the sound waves which describe the HAT template.

5.3.1.1 Propagation of sound waves in the head

Sound is the propagation of pressure waves through any compressible medium. Within the complex heterogeneous structures of the head, sound waves are accelerated, decelerated, reflected, refracted and attenuated; dependent upon the physical characteristics of the individual elements of transition. The principal properties affecting the behaviour of the waves in the head elements are:

- Volume.
- Mass.
- Density.
- Temperature.
- Stiffness/Viscosity.
- Humidity (in air).
- Frequency of the wave.

The first three of these elements, **volume, mass** and **density**, are closely related and are described by the following equation:

$$\rho = \frac{m}{V}$$

Where:

ρ is the density of the medium (in Kg/m³)

m is the total mass of the object (in Kg)

V is the total volume of the object (in m³)

The *speed of sound* propagation through media is dependent on the physical state of the matter (solid, liquid, gas), but is fundamentally a property of density: plus **stiffness** in a solid, **viscosity** in a fluid and **temperature** and **humidity** in air. For a dispersive medium like the head, the speed of sound is generally described by the equation:

$$c = \sqrt{\frac{C}{\rho}}$$

Where:

c is the speed of sound (in m/s)

C is a coefficient of: stiffness in a solid; viscosity in a fluid

ρ is the density of the medium (in Kg/m³)

By inspection, the speed of sound increases with the stiffness or viscosity of the material, and decreases with the density. Although an in depth discussion on the speed of sound in media is beyond this text, and comprehensibly covered elsewhere[1], an awareness of the principles governing the speed and propagation of sound in various states of matter helps the reader appreciate the underlying principles of HAT.

[1] E.g. Speed of sound: Wikipedia online encyclopaedia @ http://en.wikipedia.org/wiki/Speed_of_sound

Following on from the previous discussion, Table 5-1 (Cala *et al.* 1981) shows the relative densities and associated effect on the speed of sound for a selection of the biological media which compose the human head.

Component	Density (Hounsfield units[1])	Speed of sound (m/s @ 15°C)
Air	-1000	340
Fat	-50	1450
Water	0	1480 (fresh)
Brain	+34	1541
Soft tissue (muscle)	+40	1540
Blood	+25	1570
Bone (skull)	+1000	4080

Table 5-1 : Relative densities of the biological components of the human head

The research work that culminated in HAT also realised a number of notional derivatives which, although not pursued as part of HAT, are part of the intellectual property associated with the work, and as such are covered in the research patents (see Appendix I). The alternative techniques are based upon essentially the same principles of induced variances in acoustic stimuli, but using artificially created stimuli.

5.3.2 Acoustic biometrics of the human head for user authentication

Early investigations into acoustic head authentication realised a number of different conceptual approaches. The adopted technique, which came to be known as the *Head Authentication Technique*, was the result of preliminary evaluations of the various techniques, and represents a distillation of the best ideas into a single approach.

[1] The Hounsfield unit, named after Sir Godfrey Hounsfield, is a measure of density relative to water, and more commonly used in medical circles than Kg/m³. The human body is between 55% and 60% water.

5.3.2.1 Acoustic Stimuli

It was realised early on that for any acoustic technique to be truly transparent to an end user, any sounds introduced into the head had to be, at best, completely undetectable and at worst, effectively non-intrusive in order to maintain an acceptable Quality of Service (QoS). This premise resulted in three possible approaches.

5.3.2.1a Out-of-band stimuli

Out-of-band stimuli are sounds that exist outside of the natural audible frequency and/or dynamic range of the human ear. A healthy ear has a broad, essentially linear[1], dynamic range extending from below 20dbs (a whisper) up to 140dBs (a gunshot); illustrated in Figure 5-7. It is impractical to attempt to cite an acoustic stimulus outside of this range.

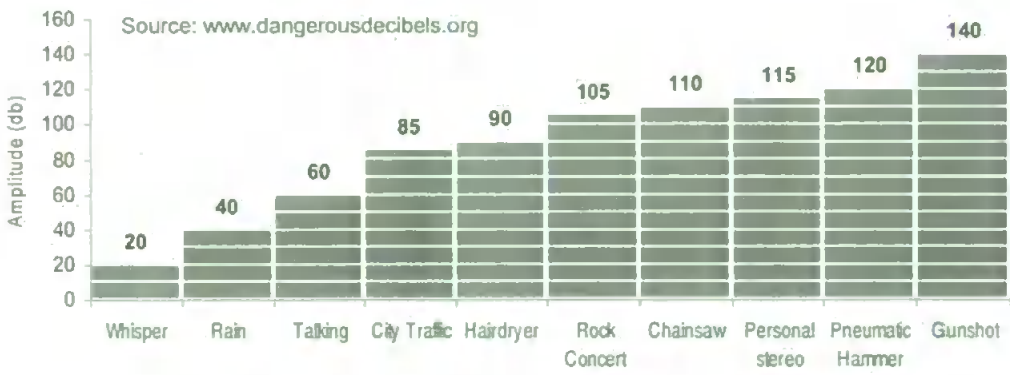


Figure 5-7 : Intensity of common sounds encountered by the human ear

In frequency terms, although it is possible to produce suitable infrasonic or ultrasonic frequencies; the question once again is whether it would be practical. There are a number of potentially contentious issues surrounding this approach for the hardware supplier, the network operator and the user. Respectively, these issues are:

- **Hardware Cost**: What would be the additional hardware cost (if any), for transducers and microphones capable of working at the extended frequencies at either end of the audible spectrum?

[1] The dynamic range of the human ear is non-linear outside of the range 40dbs to 110dbs.

- **User Acceptance**: What would be the commercial impact of an operator introducing a technique that could be *perceived* by the general public as a possible health risk? Even if it were scientifically proven, through trials, that introducing ultrasonic pulses into the head was safe, one only has to cite the on-going 'Can mobile phone radiation cause cancer?' debate (BBC News 2005) to realise that it is just as important for users' to perceive a technology as being safe as it is for the designers and operators to prove it is such.
- **Health Risks**: What would be the *actual* impact upon user's health (if any), of exposing them to extended periods of infrasonic or ultrasonic energy? How long would the clinical safety trials take before the approach could be certified as safe?

5.3.2.1b In-band Stimuli

In-band stimuli are sounds that can exist within the operational frequency and/or dynamic range of the human ear (Figure 5-1) yet remain effectively non-intrusive. This can be achieved in wither of two ways:

- **Low intensity**: Although it is possible to produce conceivable non-intrusive low intensity stimuli (<20dBs), the practical use of these sounds is minimal. Low intensity sound carries minimal energy and would need to be administered over long periods of time in relative silence to have a chance of propagating effectively through the head. This approach was therefore ruled out on a practical level.
- **Short duration**: In considering short duration high energy pulses, it is important to recall that amplitude and time are inversely proportional to energy: as pulse duration is *reduced,* in order to maintain the same energy level, the intensity of the pulse must *increase* proportionally or, once again, the pulse would not have sufficient energy to propagate effectively through the head. These pulses would sound similar to OAE style clicks and would be highly detectable by the user and therefore negatively impact on the systems QoS over a period of time.

5.3.2.1c Naturally Occurring Stimuli

Natural stimuli are those sounds produced naturally by the body itself, and in terms of the research refer to the sounds made by the voicebox. If the voicebox is used as the stimulus, it positively addresses many of the concerns cited for the other approaches:

- Talking is a natural process and cannot be considered intrusive to a user (of a voice-activated mobile service) when harnessed as an acoustic stimulus.
- Being non-intrusive (when used in normal conversation or for voice-activated mobile services) the voice carries a large amount of energy, in the order of 10,000 times more than low intensity sounds of less than 20dBs, containing sufficient energy to propagate throughout the head.
- Sounds from the voicebox are naturally harmless and are perceived as such.
- Current mobile acoustic hardware (microphones, transducers) are designed to efficiently handle the human voice, and as such can potentially be levered as part of the authentication process.

5.3.2.2 Authentication Approaches

Once the decision was made to use the body's two natural acoustic interfaces of the mouth and (outer) ear as the capture and/or stimulus input locations, it was necessary to further select one of four possible input/output permutations of the technique for the proposed research solution. All four approaches effectively harness the same acoustic variations of a stimulus, as a result of the composition of the human head. The final decision was therefore also subject to the suitability of each solution to the proposed application of mobile communications. Each of the different approaches is included within the intellectual property of the patents (see Appendix I), and further described in the subsections that follow.

5.3.2.2a Artificial stimulus: Ear-in, Ear-out

Not dissimilar in outward appearance to OAEs (Section 5.2.3.1), where a stimulus is introduced into the outer ear and then dynamically monitored at *either* ear, and compared to the original *reference* waveform to determine a consistent quantifiable variance. The concept is illustrated in Figure 5-8. Artificial stimuli have the advantage of *proactive* triggering, in contrast to *reactive* triggering of naturally occurring stimuli.

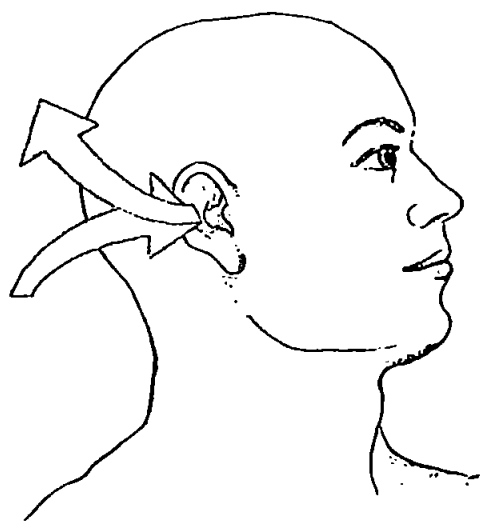


Figure 5-8 : Acoustic authentication using artificial stimulus: Ear-in, Ear-out

5.3.2.2b Artificial stimulus: Ear-in, Mouth-out

Although it may be possible to non-intrusively introduce stimuli into the outer-ear, this approach relies on the user opening their mouth in order to capture the propagating waves at a mouth-microphone. Figure 5-9 illustrates the principal. By definition, a non-intrusive technique cannot prompt a user to perform an action like opening their mouth, therefore this approach removes artificial stimuli's main advantage over natural stimuli, proactive triggering of the authentication process. This makes the approach inefficient and impractical for continuous monitoring: the alternative of the user opening their mouth on a signal from the authenticating system would make the system intrusive and inappropriate for the research.

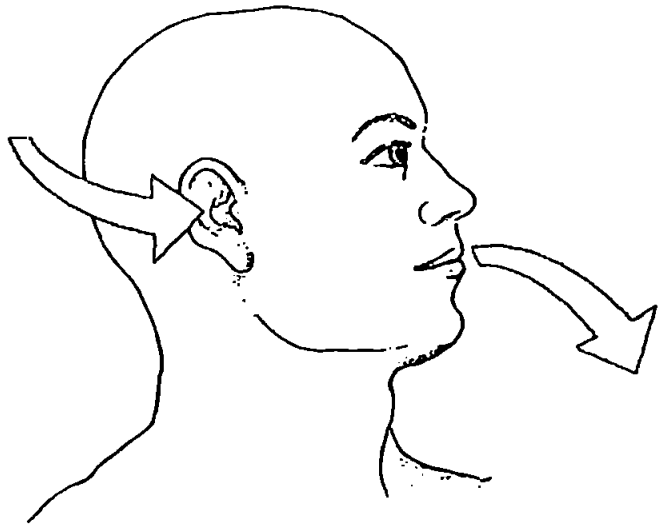


Figure 5-9 : Acoustic authentication using artificial stimulus: Ear-in, Mouth-out

5.3.2.2c Artificial stimulus: Mouth-in, Ear-out

This approach, illustrated in Figure 5-10, has the advantage of being more robust than the previous approach as the mouth (in isolation) has no means of detecting sound, the stimulus can therefore contain more energy without being intrusive. However, the approach still suffers the same arguments as the previous approach, where the user must consciously open their mouth in order for authentication to be performed. This approach therefore has to be considered intrusive and inappropriate for the research.

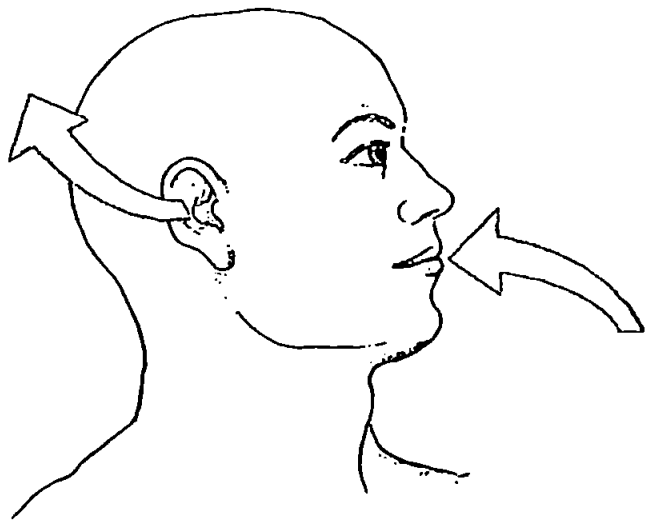


Figure 5-10 : Acoustic authentication using artificial stimulus: Mouth-in, Ear-out

5.3.2.2d Natural stimulus (Voicebox): Ear-out, Mouth-out (HAT)

Early experiments to prove the concept of acoustic head authentication used artificially created pure tones (sine waves). These were introduced at the mouth and collected at the (outer) ear, in order to verify the existence of any acoustic variance due to the head against a clean reference. It was with the knowledge of the various arguments discussed in Section 5.3.2.1 however, that the best long-term solution for the research was to pursue the approach of natural stimuli utilising the complex sounds produced by the human voicebox. The decision eliminated any choice of application permutations as the approach naturally defined its own operational parameters; the stimulus propagating up from the voicebox, with monitoring at the subjects mouth and ear, as shown in Figure 5-11.

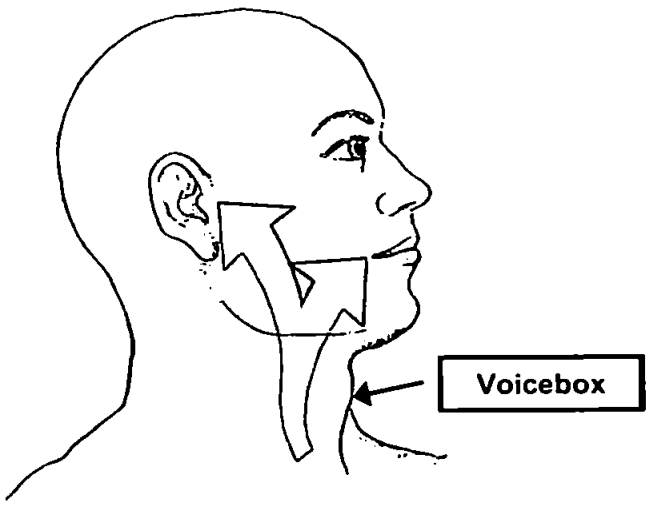


Figure 5-11 : Natural voicebox stimulus approach to acoustic head authentication

The human voicebox (larynx) is located in the front of the neck and contains the vocal cords, a pair of membranes stretched across the wind-pipe (trachea), which vibrate when air from the lungs is expelled over them modulating the air-flow and producing distinctive sounds (phonation) at the mouth. The vocal cords have a frequency range of 80Hz to 7000Hz, with the natural spoken male voice covering the range 80Hz to 200Hz, the female voice 160Hz to 300Hz (Baken & Orlikoff 1999); trained 'operatic' voices cover the range 80Hz to 1400Hz, illustrated in Figure 5-12.

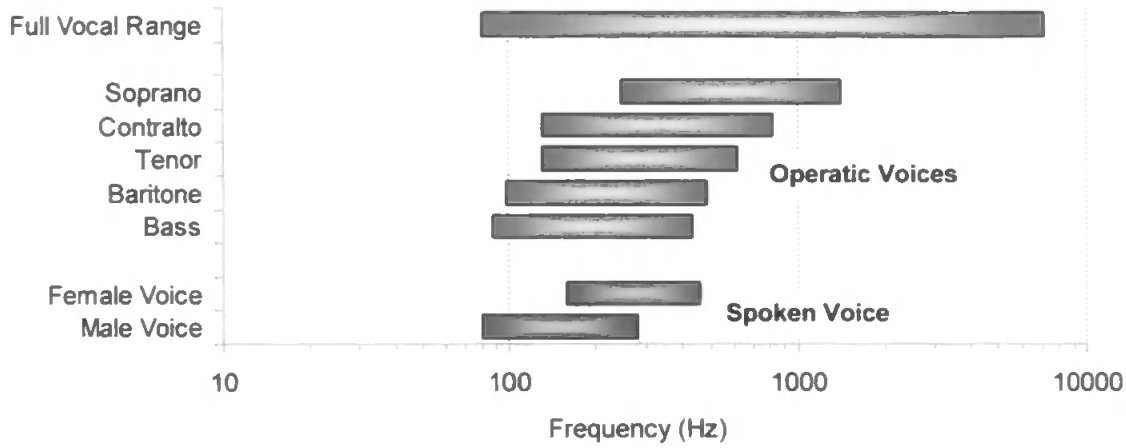


Figure 5-12 : The frequency ranges of the human voice (voicebox)

Utilising the voicebox as a natural stimulus for acoustic head authentication offers a number of significant advantages over deliberate and artificial stimulation; these are:

- The voicebox presents naturally occurring and harmless acoustic stimulation to the head. HAT is essentially utilising an untapped resource.
- Voicebox stimulation is not only safe, but cannot be perceived as anything other than safe by users; the propagating wave energy being present in the head every time we speak, whether harnessed or not.
- The acoustic spectrum of an individual's voicebox is different for every user, increasing system security. As the HAT process is a function of the head and NOT of the stimulus, this variable stimulus is an asset and not a complication.
- The voice easily contains sufficient energy to propagate throughout the head, without the need to mask the stimulus in any way.
- Mobile hardware is naturally configured for operation at vocal frequencies.

In balance, voicebox stimulation does however suffer one obvious limitation:

- The user must be vocalising for authentication to be performed. HAT does not therefore naturally lend itself to authentication during use of purely data services.

5.4 Conclusion

This chapter defined the research requirements for a novel authentication technique designed to redress the imbalance of mobile security commensurate with the data and services the security is designed to protect.

This chapter summarised the investigative and decision process that led to the identification of a novel biometric option based on a natural multi-modal approach, where selected physiological and behavioural characteristics work in symbiosis. Having considered all the arguments for and against the various permutations of acoustic head-authentication, the final option chosen for development utilises naturally occurring vocal stimuli in a unique *ear-out*, *mouth-out* monitoring arrangement. The technique came to be known as the **Head Authentication Technique (HAT)**.

In conceptual terms, HAT addresses all of the researches requirements, offering the following key security advancements:

- Improved user-identity verification.
- Non-intrusive authentication, transparent in use to the network user.
- Continuous authentication, not just PoE.
- Capable of leveraging existing mobile hardware into additional security roles.

The HAT technique was proven in preliminary tests to realise unique quantifiable authentication data. In the next Chapter, the HAT process is broken down into discrete stages, which are described in detail, along with some rationalisation of the key developmental decisions which led to the final HAT architecture.

Chapter 6

Realisation of the Head Authentication Technique

6 Realisation of the Head Authentication Technique

The Head Authentication Technique is a novel biometric technique developed specifically for application in mobile devices and conceived out of an investigation into numerous original advanced authentication ideas discussed in Chapter 5.

This chapter discusses the Head Authentication Technique in depth; introducing and explaining each discrete stage of the HAT authentication process. The chapter also discusses the developmental process which led to the final HAT architecture, along with an alternative architecture, and explains the reasoning behind some of the key research direction decisions.

6.1 Introduction

HAT is a multi-modal biometric technique capable of continuously and transparently verifying the claimed identity of a user accessing the advanced[1] data services of a wideband mobile network. This novel technique harnesses the natural symbiotic relationship of the 'behavioural characteristics' of the human voice stimulating the 'physiological anatomy' of the head. The resultant activity is monitored at separate locations on the head and a hybrid biometric template extrapolated from multiple spot-frequency spectra analyses between the data streams.

The key to the HAT authentication process is the unique way in which the human head is classified through natural audio stimulation. The research realised two distinct methods of processing the separate audio data streams:

[1] When compared to the data services of a traditional 2nd generation mobile network.

- The **Absorption** method utilises variations in spectral amplitude between discrete spectra of the audio data stream introduced by the propagation path.
- The **Correlation** method utilises temporal delays between discrete spectra of the audio data stream introduced by the propagation path.

Although each of these two methods is discussed in the following sections, it was the absorption method that ultimately proved to offer the better solution, and it was this method which was developed into HAT and refined within the HAT demonstration tool. A discussion of the correlation method nonetheless is justified, as it defends the decision to develop the absorption method, offers supporting evidence for some of the findings in the absorption discussion, and suggests a possible area for future work.

6.2 The Head Authentication Absorption Method

The absorption method of head authentication employed by HAT is a novel way of extracting a unique biometric template from a user's head, through use of a single source stimulus, and multiple audio data streams captured from discrete locations on a user's head. The process is broken down into five distinct stages of operation:

1. **Capture** multiple voice stimulated PCM audio data streams. Basic HAT[1] utilises two external capture points: the Mouth and the Ear.
2. **Filter** each data stream discretely at multiple pre-selected frequencies using a high roll-off, narrowband FIR filter. Basic HAT adopts twenty-five spot-frequencies.
3. **Absorption** calculation; the difference in RMS (Root-Mean-Square) energy between captured waveforms at each spot-frequency. Basic HAT compares discrete mouth and ear frequency pairs.

[1] 'Basic HAT' in this context defines the minimum operational requirements of the HAT tool. HAT does however have the potential of increasing both the number of sample capture points and the effective system resolution (number of spot frequencies); see future work in Section 8.3.

4. **Analysis** of the RMS absorption difference output, by feeding the resultant data array into a pre-trained (for authentication) neural-network. The training data for the HAT neural-network consisted of one of the data sets collected during the HAT field trials in Chapter 7.
5. **Classification** of the neural-network result by comparison with a preset authentication threshold. The HAT authentication threshold was determined using a second data set collected during the HAT field trials in Chapter 7.

These five stages of the absorption method are also shown schematically in Figure 6-1.

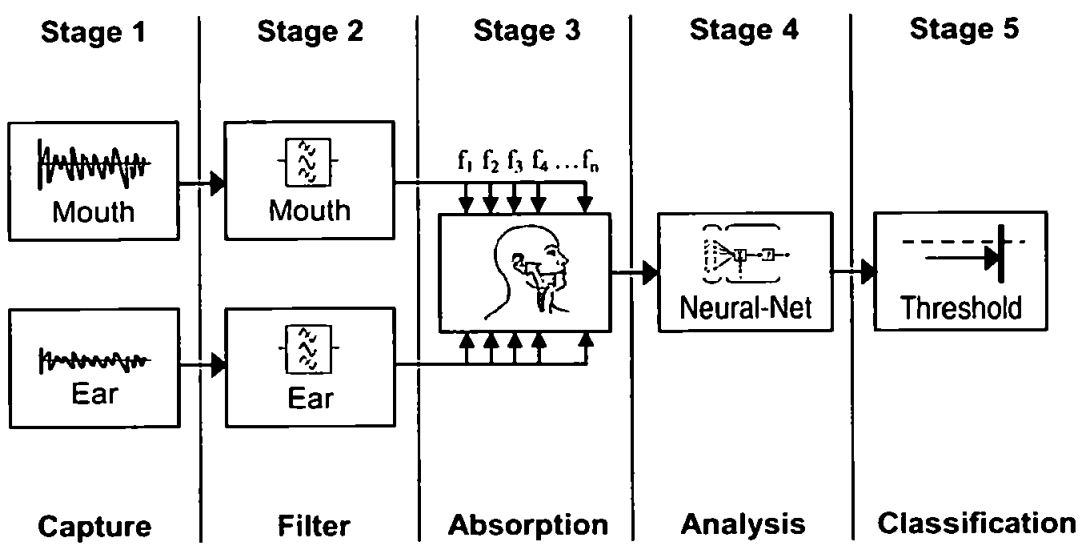


Figure 6-1 : The five discrete stages of the HAT (absorption) authentication process

The HAT software tool (see Section 7.2.2.2) additionally safeguards users against false rejections (Section 4.2.3) by applying a soft lock-out, where the user has to fail a pre-defined number of authentication cycles before being rejected by the system. This is only made possible by the continuous and non-intrusive nature of the head authentication process employed by HAT.

6.2.1 Stage-1 Capture HAT Sample Data

As introduced in Chapter 5, HAT takes advantage of different acoustic responses to natural vocal stimuli, produced by the voicebox, at different locations on the human head, due to the propagation effects of longitudinal waves in bio-matter (Section 5.3.1). The two most easily accessible acoustic locations to monitor the propagation effects inside the head, due to the voicebox stimulus located in the neck, are at the mouth and the outer-ear; HAT captures its samples from these two locations as illustrated in Figure 6-2.

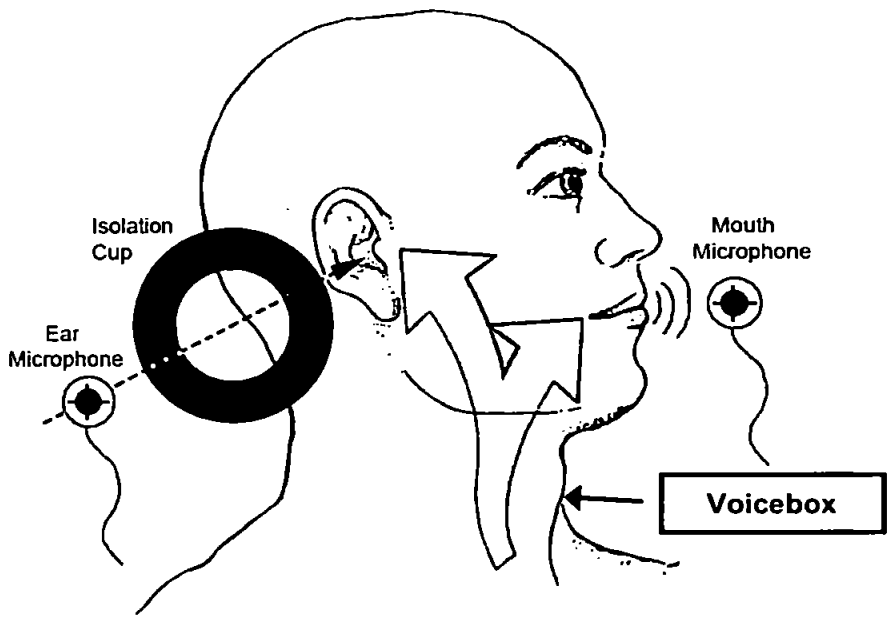


Figure 6-2 : The HAT Headset microphones configuration

Development of the first HAT headset placed the ear microphone inside of an isolation cup (Figure 6-2), minimising:

- side-tone[1] cross-contamination;
- microphone misalignment with the ear canal;
- extraneous noise;
- headset discomfort for the trial users.

[1] Side-tone is the sound heard at the ear due to sound uttered at the mouth. Although usually active in nature, in this case, side-tone refers to unwanted propagation between mouth and ear via the air-path.

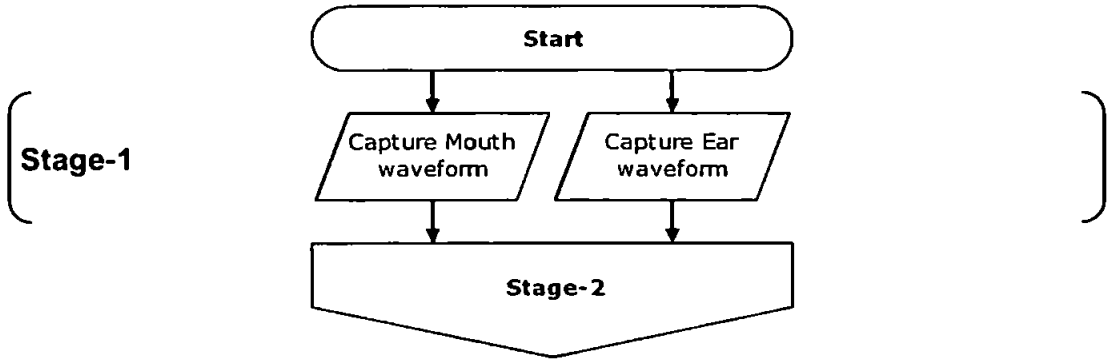


Figure 6-3 : HAT Stages flowchart - Stage-1 (Capture waveforms)

The flowchart in Figure 6-3 summaries the HAT Stage-1 capture process schematically. This flowchart is referred to as the **HAT Stages Flowchart** and will be expanded upon in subsequent HAT stage descriptions until it shows the complete HAT absorption methodology in Stage-5.

6.2.1.1 HAT Microphones

To maximise the chance of capturing quantifiable differences in the audio sample pairs, HAT utilises two identical high-quality voice microphones. It is fundamental to the HAT process to capture predominantly the head-based propagation waves, and as the microphones are positioned relatively close to each other, they are configured in such a way as to minimise cross contamination effects:

- **Ear Microphone Configuration**

  The ear microphone is identical to the mouth microphone. It is placed inside an isolation ear-cup in order to minimise air-path (mouth-to-ear) acoustic cross contamination and positioned on the pinna (Section 5.2.1) of the outer ear using a headset similar in design to a normal computer-based headset (see Section 7.2.1). The isolation cup has the added benefit of minimising extraneous sound contaminating the low-amplitude ear sample.

- **Mouth Microphone Configuration**

  The mouth microphone is positioned in front of the mouth in a similar configuration to a normal computer-based voice microphone (see the HAT headset in Section 7.2.1). The microphone captures a reference sample, being located nearest to the acoustic stimulus, which is later used to compare with the altered ear captured sample to determine the propagation variance.

6.2.1.2 Captured Soundfile Format

HAT captured soundfiles conform to a standard digital PCM[1] format, and are stored as uncompressed Microsoft Windows wave files[2], a subset of the broader independent Resource Interchange File Format (RIFF) (see Appendix D). This makes the files easy to manipulate on a PC within the following standard commercial development software:

- **Mathworks Matlab v6.1**

  Used for all HAT development work, before coding HAT stages into Visual Basic to form the HAT demonstration tool. Due to Matlabs excellent built-in neural-network toolbox, for convenience stage-4 analysis remained in Matlab.

- **Microsoft Visual Basic v6.0**

  Used for development of the HAT demonstration tool, including generic Microsoft Windows Graphical User Interface (GUI). After the HAT process was finalised, all stages except Stage-4 were ported across to Visual Basic®.

The size and quality of HAT captured waveforms are governed by the standard PCM specifications: Number of channels, Sample size (2^X where $X>1$) and Sampling rate (in Hertz). The values of these parameters were individually determined during the development stages of the research and are described here:

[1] Pulse Code Modulation is a sampling technique for digitising analogue signals, especially audio signals.
[2] Microsoft® Windows® wave files are identified by the extension '.wav'.

- **HAT Channels**

Function: Number of capture channels.

HAT Value: 2

Development: 2 channels are the minimum requirement the HAT comparison process to be performed. Basic HAT utilises the two channels: Mouth and Ear.

- **HAT Sample size**

Function: Number of bits-per-sample.

HAT Value: 16-bit

Development: bits-per-sample determines the number of quantisation levels-per-sample (sometimes called the resolution), and the dynamic range of the captured sound (Table 6-1).

Bits-per-sample (bps)	Quantisation Levels $2^{\text{bits-per-sample}}$	Dynamic Range $20 \times \log(2^{\text{bits-per-sample}})$
4[1]	16	24dBs
8	256	48dBs
16[2]	**65,536**	**96dBs**
24[3]	1,677,216	124dBs
32[1]	4,294,967,296	193dBs

Bold = HAT Selection

Table 6-1 : Quantisation levels and dynamic-range based on bits-per-sample

It can be seen from the typical capture shown in Section 6.2.1.3, that the low-amplitude ear waveform is particularly sensitive to signal resolution; therefore HAT maintains a sample size of 16-bit.

[1] Not in general use, included for comparison purposes only.
[2] Domestic CD audio standard.
[3] Domestic CD audio mastering and DVD-Audio Standard.

- **HAT Sampling rate**

Function: Number of samples-per-second.

HAT Value: 11025Hz (11025 stereo sample pairs-per-second)

Development: Initial tests of the HAT process adopted a frequency bandwidth of 50Hz to 16000Hz, approximately the bandwidth of a healthy human ear (Section 5.2.1). During subsequent development, this was refined to 100Hz to 8000Hz; and finally 100Hz to 4000Hz, when it was found that frequencies above 4000Hz contained minimal absorption information. This is illustrated in the example plot shown in Figure 6-4 (100Hz < bw < 8000Hz), where useful absorption information has tailed off above 4000Hz. The effect on sampling rate was a reduction from an initial 44100Hz to 11025Hz. This topic is covered in greater depth in Section 6.2.6.

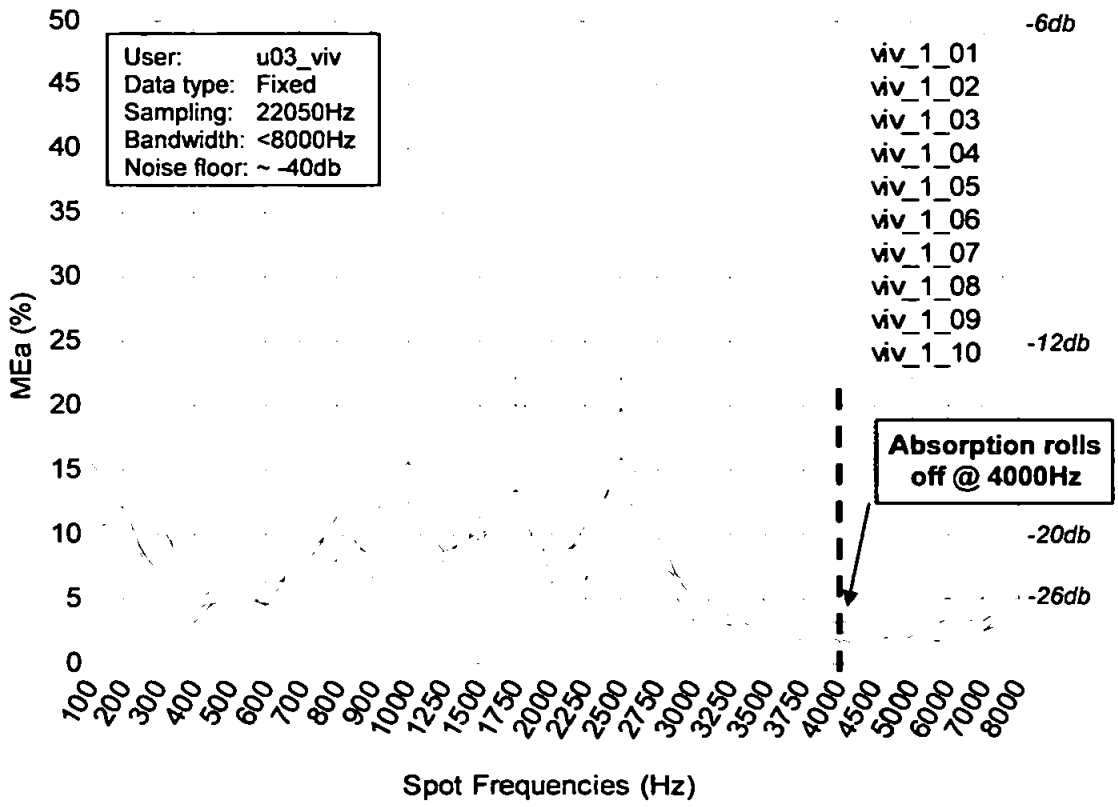


Figure 6-4 : Compound frequency absorption curves of the numbers '0' to '9' - HAT trial participant 'u03_viv' (100Hz < bw < 8000Hz)

6.2.1.3 The Captured Soundfile Waveform

An example of a typical HAT captured wavefile pair is shown in Figure 6-5: the upper trace represents the prominant *reference* Mouth waveform; the lower trace the *difference* Ear waveform. Notice particularly, HATs effect on Ear ampltiude.

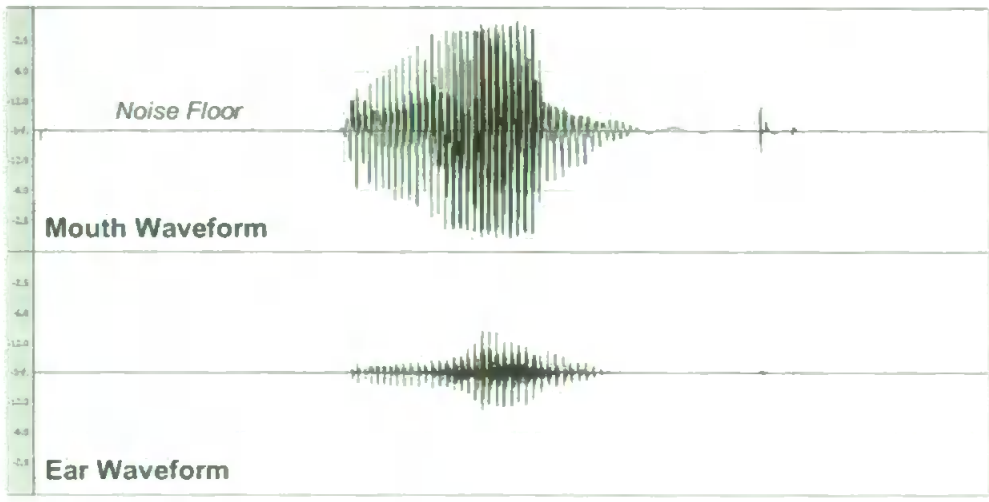


Figure 6-5 : A Typical HAT wavefile pair

In Figure 6-6, the noise floor in Figure 6-5 has been vertically zoomed to illustrate typical ambient noise levels experienced in the HAT trials discussed in Section 7.3. The values are around -40db for the Mouth, and around -48db for the Ear; the additional damping effect due to the isolation cup covering the ear, illustrated in Figure 6-2.

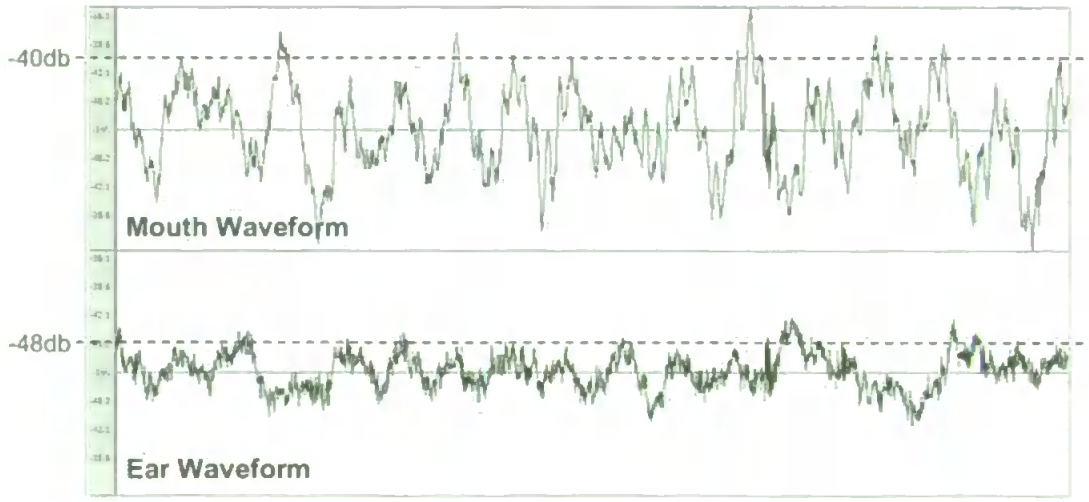


Figure 6-6 : Typical noise floor(s) of a HAT wavefile pair.

6.2.2 Stage-2 Filter HAT Sample Data

The basic authentication metric utilised by HAT is the mouth-to-ear pass-band RMS absorption figures of multiple narrowband frequency spectra, at pre-selected spot-frequencies, within the vocal range of the human voice (Section 5.2.1).

HAT Stage-2 filtering involves the cyclic application of a narrowband high roll-off digital bandpass filter to mouth-ear pairs of captured waveforms. Starting at a lowest frequency of 100Hz, a 100Hz bandwidth filter (see Section 6.2.2.1) is discretely applied twenty-five times, at pre-selected spot-frequencies, up to a highest frequency of 4000Hz (see Section 6.2.6.1) with additional Stage-3 Absorption processing being performed as an integral part of each filter cycle. The number and spectral locations of the spot-frequencies were determined empirically, and are shown in Figure 6-7.

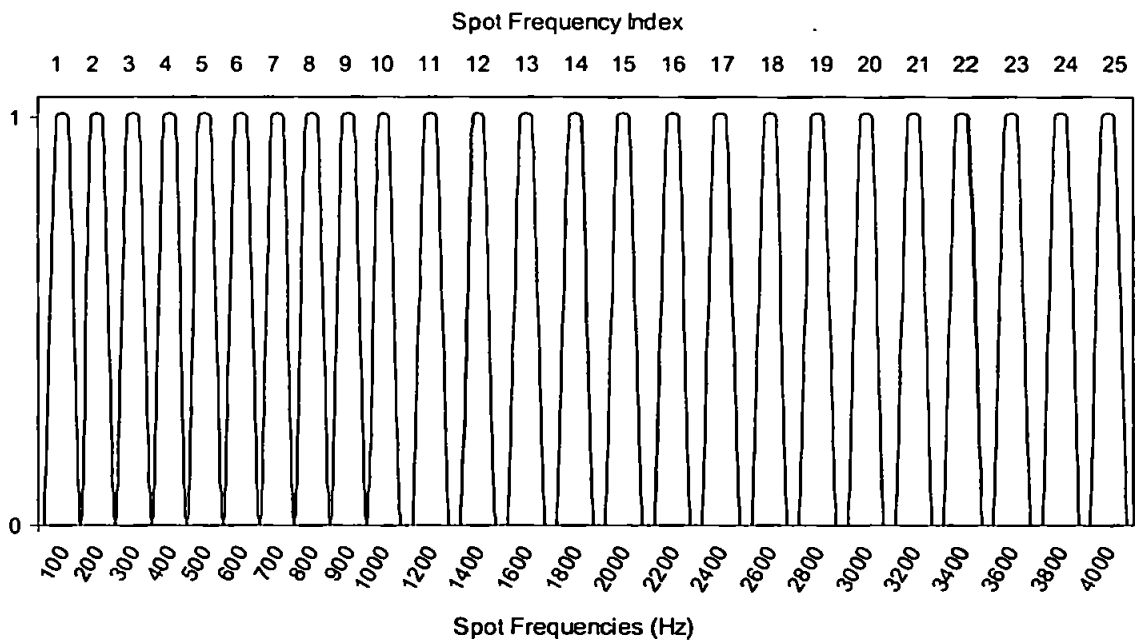


Figure 6-7 : HAT Stage-2 Filter spot-frequencies

By inspection of the filtered frequency spectrum, there are a number of important observations which can be made:

- Spot-frequencies are mirrored in the range 100Hz to 1000Hz, crossing over at a figure of -60db, maximising system resolution within the natural *spoken* frequency spectrum of the human voicebox (Figure 5-12).
- The actual number of spot-frequencies was partly governed by the hardware processing capabilities of the HAT system, as each spot-frequency feeds directly into a discrete input mode in the HAT Stage-4 Neural-network. The number of spot-frequencies also governs the number of (hidden) layer neurons in the neural-network (see Section 6.2.4.1). It was found empirically that a figure of twenty-five spot-frequencies (and neural-network neurons) maximised the available processing resources, realising good neural-network user classification, whilst maintaining acceptable authentication cycle times of a few seconds.
- The *stopgaps* between spot-frequencies above 1000Hz, when analysed, were found to offer minimal additional information to that already provided by the 100Hz filter passbands; filter bandwidth uniformity was therefore maintained across the full HAT spectrum.
- Although use of a Fast Fourier Transform (FFT) was considered for Stage-2 filtering, the HAT methodology currently in place (specifically the discrete stepping filter) draws parallels with the frequency component voice banding (of formant and carrier), found in Vocoder[1] voice synthesisers (Fellbaum 2005).

The flowchart in Figure 6-8 is the systematic continuation of the HAT Stages Flowchart introduced in HAT Stage-1 Capture (Figure 6-3), and places HAT Stage-2 Filtering in context with the previous stage.

[1] A vocoder is a voice synthesiser, often used to reproduce a human voice with a metallic and monotonous sound. An early example is the song 'We are the Robots' (1977), by the German band Kraftwerk.

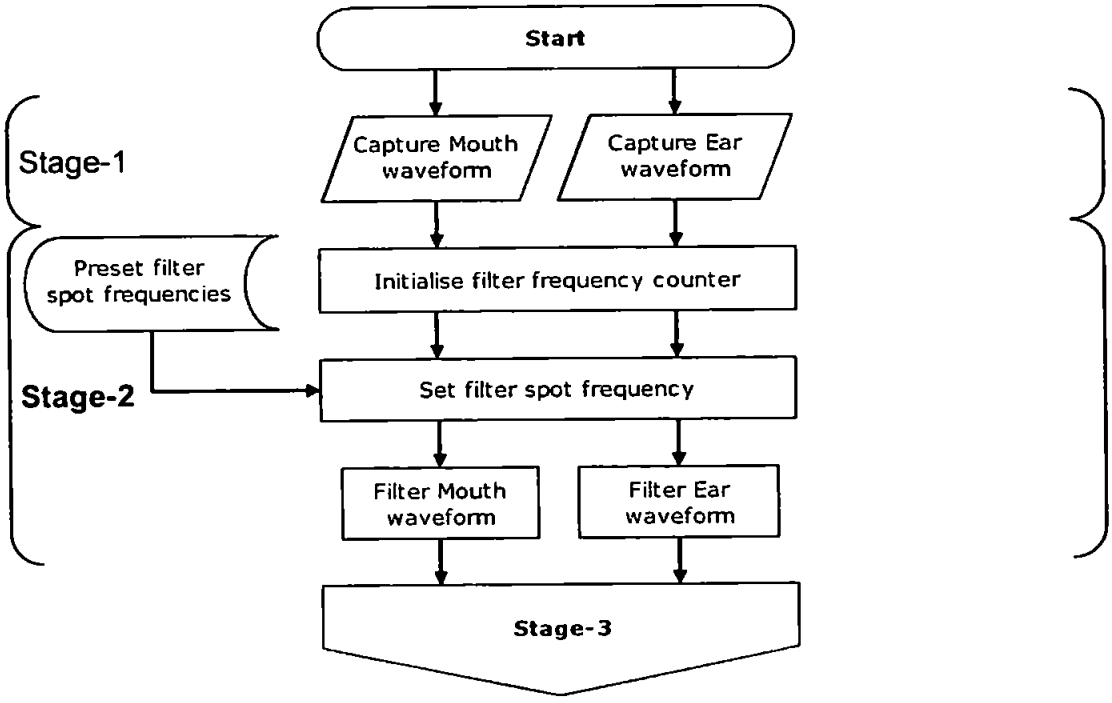


Figure 6-8 : HAT Stages flowchart - Stage-2 (Filter waveforms)

Note that the flowchart only shows one cycle of the filtering process, a single iteration of the HAT template creation process, the completed filter/absorption loop is illustrated in the description for Stage-3 RMS Absorption (Section 6.2.3).

6.2.2.1 Finite Impulse Response HAT Filter

The requirement for the HAT Stage-2 filter was for a design that would minimise the risk of spectral distortion, extracting only the desired signal spectrum. The digital filter design chosen was a Finite Impulse Response (FIR) filter with symmetrical coefficients and incorporating a Hamming window. The choice of symmetrical FIR filter with an odd number of coefficients was used so that the group delay of all frequencies passing through the filter would be an integer and be defined by the equation:

$$Group\ delay = \frac{filter\ coefficien\ ts - 1}{2}$$

A Hamming window was used so that out-of-band rejection would be greater than ~40dB (or less than 1%). Without the Hamming window there could be undesirable (Gibbs) ringing at the edges of the filter passband. The filter was developed initially in Matlab, before being ported into Visual Basic and the HAT Demonstration Tool (see Section 7.2). The filter development code has been included in Table 6-2.

```
function [coeff] = bpf(fa,fb,nc)

%BPF Bandpass-Filter polynomial coefficient generator (Hamming)
%  BPF(fa,fb,nc)
%    fa - lower corner frequency
%    fb - upper corner frequency
%    nc - n-count polynomial coefficients; group delay (nc-1)/2
%
%  Example: coeff=bpf(500,600,501);
%
%Author  : PMR
%File    : bpf.m (v.2)

%Local variables:
% coeff - filter polynomial (coeff)icients
%    fa - lower corner frequency of filter
%    fb - upper corner frequency of filter
%    lo - (lo)wer corner frequency of filter
%     n - (n)-count coefficients range
%    nc - (n)-count polynomial (c)oefficients
%    up - (up)per corner frequency of filter

n=(-(nc-1)/2 : (nc-1)/2);          %define n-count range
lo=min(fa,fb);                     %check lower corner frequency
up=max(fa,fb);                     %check upper corner frequency

%- core function ---------------------------------------------
%default hamming window function
hamming_window = (0.54 - 0.46*cos(2*pi*n./nc - pi));

%calculate n-count filter coefficients
coeff = hamming_window.*(2*up*sinc(2*up*n) - 2*lo*sinc(2*lo*n));
```

Table 6-2: Matlab Code for the HAT Stage-2 Filter

When deriving the performance of the digital filter, an important consideration was the processing payload of the filter cycle(s). Although it is possible to produce a HAT software filter with an almost ideal frequency response, an example of which is shown

in Figure 6-9 (0dB passband, greater than -60dB stopband), the processing payload is high; especially with the filter polynomial count of 6001 illustrated. As discussed previously in Chapter 2 (Section 2.3.7), all processing within a mobile device will have a negative effect on the recharge cycle time of the unit's power-pack. As basic HAT Stage-2 filtering is performed twenty-five times on two discrete waveforms, it was especially important to reduce processing to a minimum whilst maintaining overall system integrity; this was achieved through experimentation.

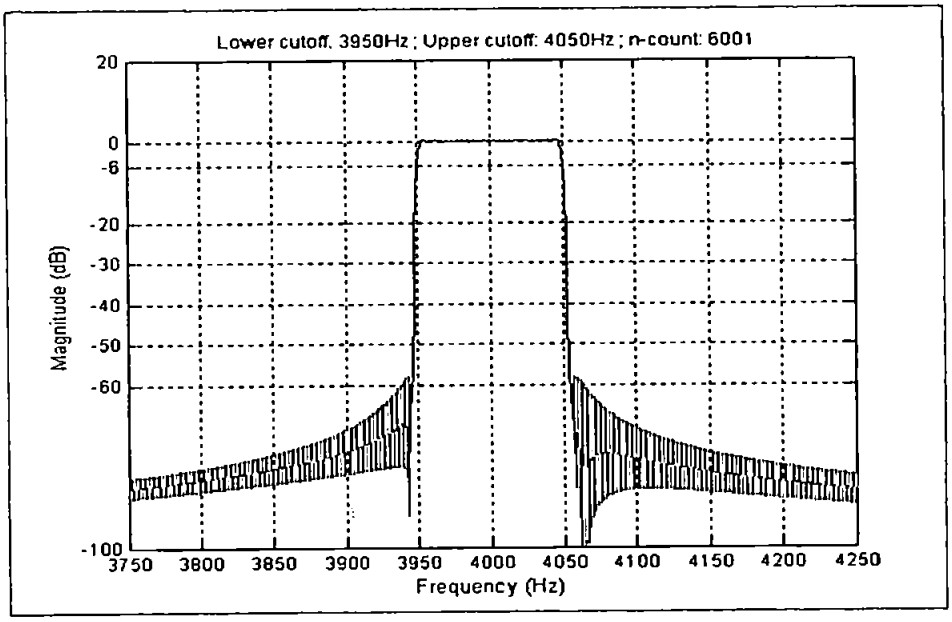


Figure 6-9 : Frequency response of an ideal HAT Stage-2 Filter (n = 6001)

Examining the other end of the performance curve, the filter frequency response curve shown in Figure 6-10 shows a very fast, low processing requirement, digital filter; with only 101 polynomial coefficients (n = 101). However, notice at least 6dBs of attenuation at the passband centre frequency of 4000Hz and the extremely poor roll-off. For the purposes of HAT, this particular filter was found to introduce unacceptable cross-contamination within the adjacent spot-frequency passbands data.

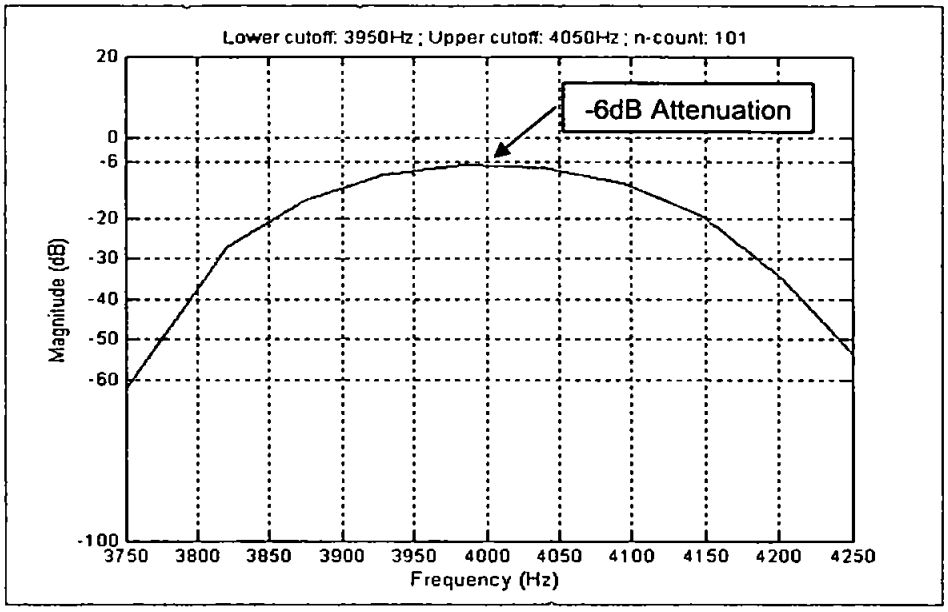


Figure 6-10 : Frequency response of an inadequate HAT Stage-2 Filter (n = 101)

By increasing the digital filters polynomial n-count above 500, see Figure 6-11, it can be seen that the filters frequency response improves dramatically, with:

- 0dBs attenuation at centre frequency (HAT spot-frequency) of passband.
- High roll-off with 6dBs of attenuation at the filter corner frequencies.
- Better than 50dBs attenuation (< 0.1%) in the filter stopband.

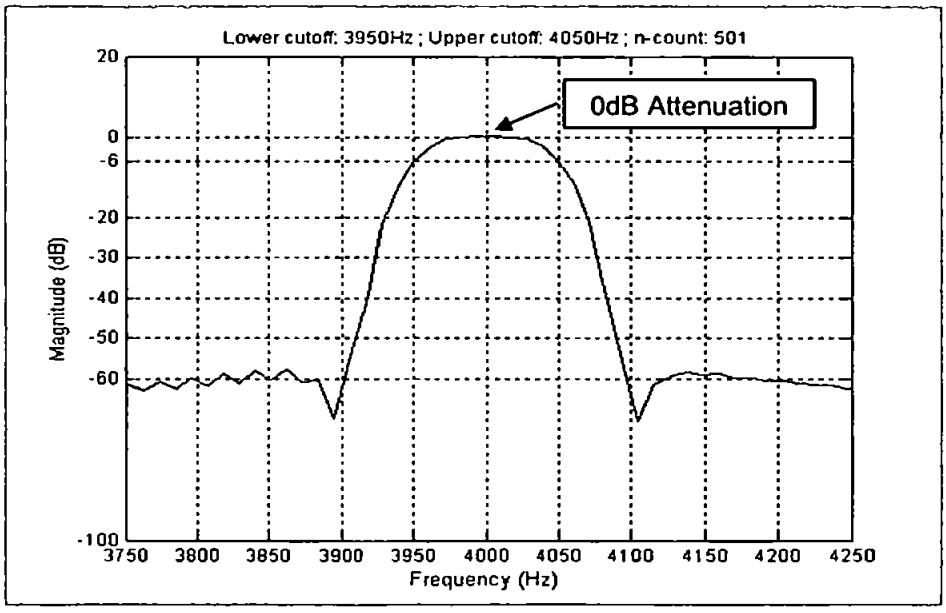


Figure 6-11 : Frequency response of an improved HAT Stage-2 Filter (n = 501)

Although the filter in Figure 6-11 was an improvement, it was determined through extensive experimentation, that the optimum filter performance balance **for the system as a whole** was achieved with a digital filter whose frequency response is shown in Figure 6-12 (n = 1301). It was discovered that although many filter designs produced what initially appeared to be good Stage-3 Absorption results, the Stage-4 Analysis neural-network could not reliably extract a signature from the sample data. It was discovered that the performance of HAT Stage-2 Filtering and HAT Stage-4 Neural-network analysis were in fact highly mutually dependent, and the design of the filter was heavily dependant on the design and subsequent performance of the neural-network in HAT Stage-4 Analysis (see Section 6.2.4).

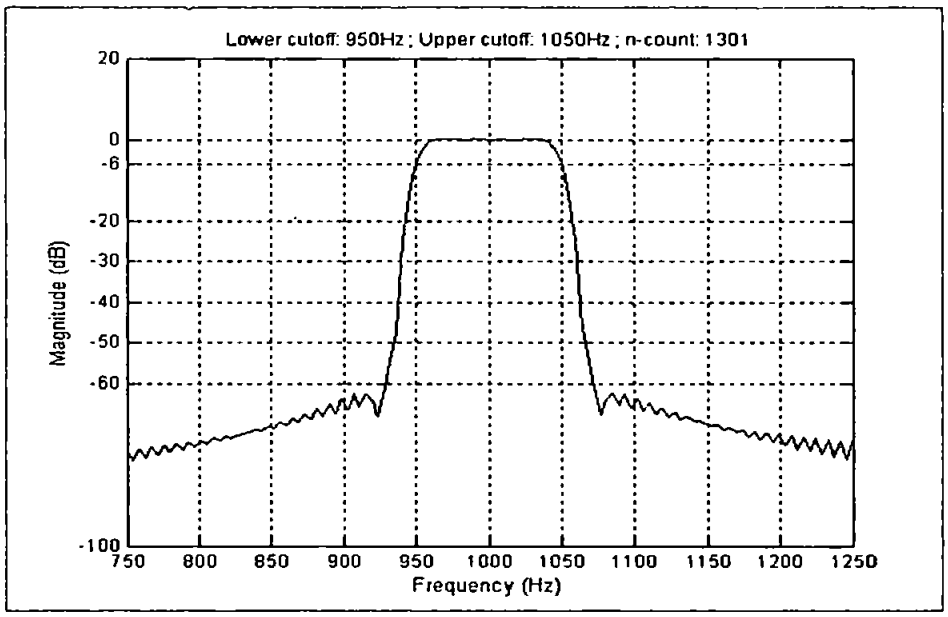


Figure 6-12 : Frequency response of the final HAT Stage-2 Filter (n = 1301)

HAT Filter Design Specifications

- FIR digital filter incorporating a Hamming Window (n = 1301).
- 100Hz bandwidth, with 0dB passband attenuation
- High roll-off with 6dBs attenuation at corner frequencies.
- 60dBs attenuation (< 0.01%) in stopband.

6.2.3 Stage-3 Absorption between Filtered Frequency Pairs

RMS absorption of frequencies within the human-head is essentially the novel aspect of basic HATs interpretation of head authentication. Although sample data must be: captured, filtered and subsequently analysed, classified and a suitable response issued, it is the RMS absorption figures of the multiple narrowband frequency spectra which determine and define the HAT biometric template.

HAT Stage-3 Absorption attempts to quantify any variance in RMS amplitude between a captured audio sample at a user's mouth, and a simultaneously captured audio sample at the user's ear, at pre-determined spot-frequencies. Any absorption is a result of the propagation effects of the 'ear-wave' through the intervening bio-matter (Section 5.3.1) in contrast to the more direct path of the 'mouth-wave'. The HAT absorption figure represents the preservation of the RMS value of a 100Hz snapshot of the 'ear-wave', at a pre-determined spot-frequency, compared to the value of the paired 'mouth-wave'.

Example: An absorption figure of 40% at a particular spot-frequency represents a 60% reduction in the RMS amplitude of the 100Hz bandwidth ear-wave spectrum, compared to the reference 'mouth-wave' spectrum, at that frequency point.

As mentioned in Section 6.2.1.3, an absorption calculation is performed between the filtered mouth/ear spectra within each cycle of the twenty-five cycle HAT Stage-2 Filter process. This is shown schematically in Figure 6-13, Stage-3 of the HAT Stages Flowchart. The Stage-3 flowchart also includes detail of the Stage-2/Stage-3 finite filter/absorption loop.

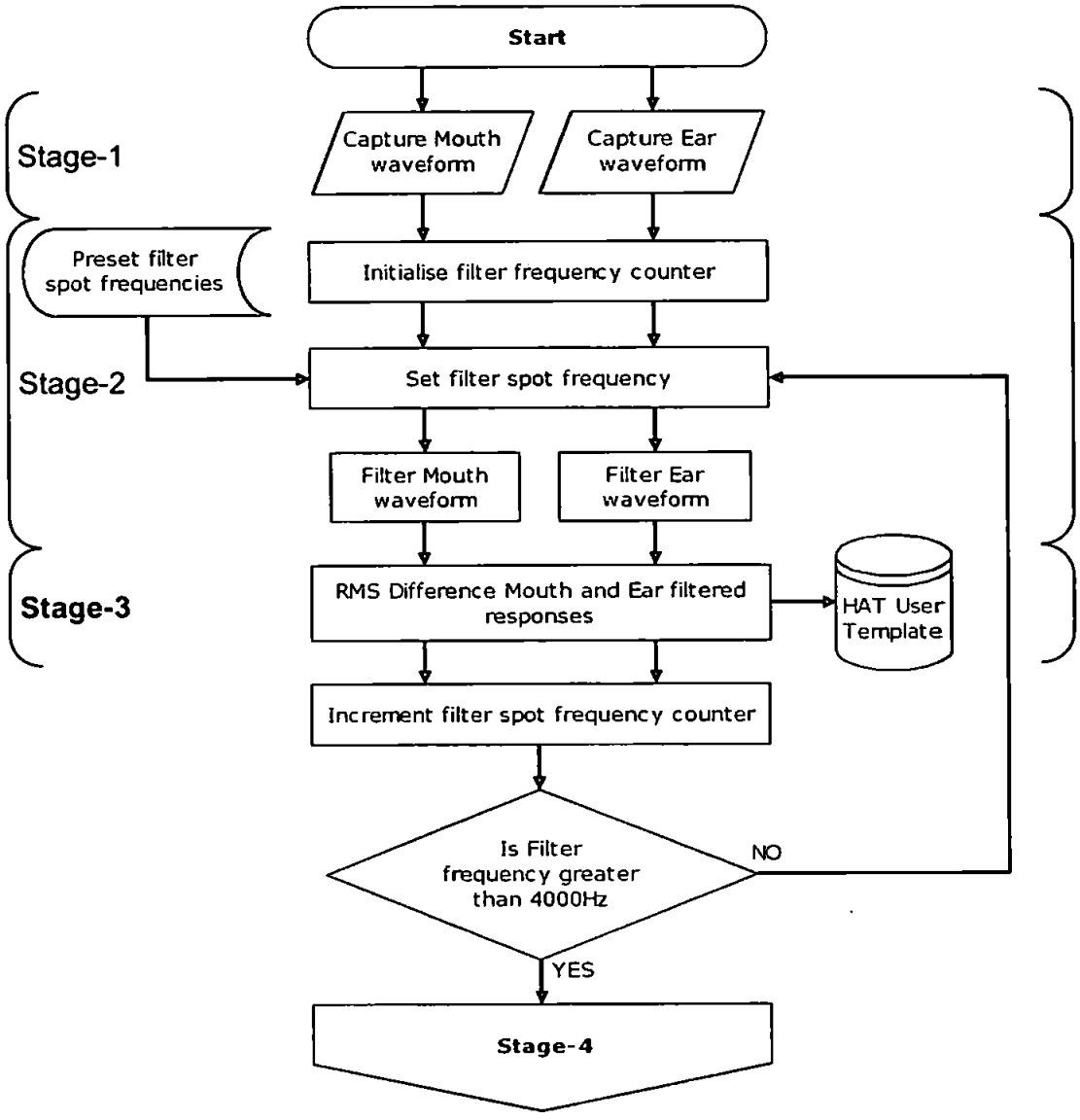


Figure 6-13 : HAT Stages flowchart - Stage-3 (Absorption calculation)

By following the Flowchart in Figure 6-13, it can be seen how HAT Stage-2 filtering and HAT Stage-3 Absorption cycle together to accumulate the HAT absorption template, within the 'HAT User Template' container. Upon completion of a HAT user template (twenty-file cycles), flow is passed to HAT Stage-4 Analysis for processing within a neural-network; either for Stage-4 network training (of a new user) or Stage-4 authentication (of an existing user), before passing to final Stage-5 Classification and response discussed in Section 6.2.5.

6.2.4 Stage-4 Neural-Network Analysis of Absorption Frequency Pairs

Each time a (basic) HAT authentication cycle is performed, HAT Stage-3 Absorption (or Stage-3 Correlation for the correlation method, see Section 6.3) produces a curve defined by a set of twenty-five non-integer variables; one for each of the HAT spot-frequencies. To analyse this set of biometric markers and extract the unique HAT user template, a neural-network was employed.

The choice to use a neural-network was based on a number of factors. A computer's ability to analyse the constantly varying data produced by a biometric system, even when it comes from the same user, traditionally lies in its computational speed (Table 6-3). Combined with custom analytical software, a computer can perform what in essence is a brute force attack on the data, to attempt to authenticate a user against a stored template.

Good at	Not good at
Fast Arithmetic	Handling noisy data
Following programme code precisely	Massive parallelism
	Fault tolerance
	Adapting to changing circumstances

Source: Centre for Cognitive and Computational Neuroscience (Link: CCCN)

Table 6-3: Computers traditional strengths and weaknesses

Neural-network differs in that they adopt a generic learning process when analysing sets of data. They are not programmed, in a traditional sense, but given examples of right and wrong behaviour and then allowed to configure themselves to *learn* the difference for future encounters. Although neural-networks are still computational engines they can appear to exhibit pseudo intelligence when processing data where:

- an algorithmic solution cannot be formulated;
- lots of examples of behaviour are available;
- we need to pick out the structure from existing data.

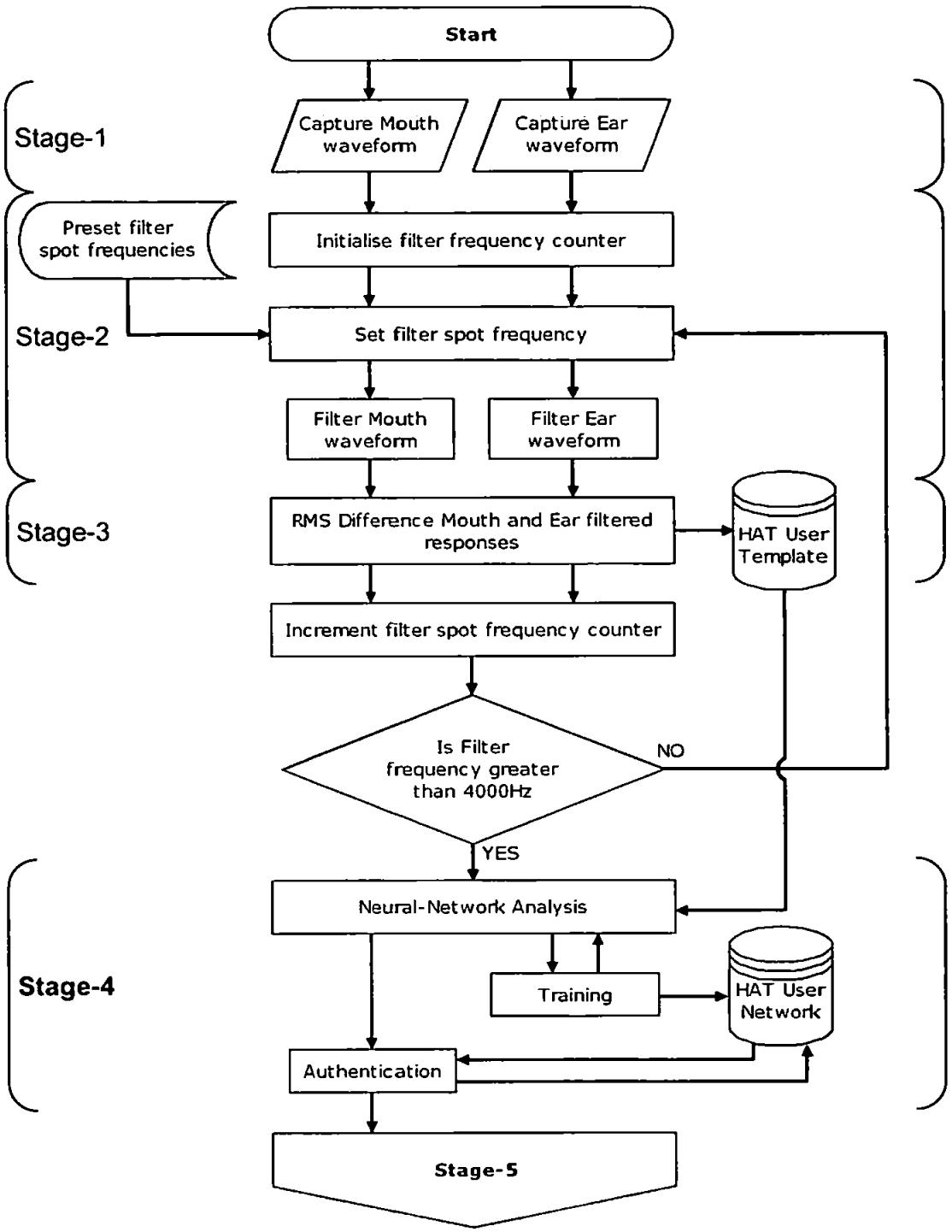


Figure 6-14 : HAT Stages flowchart - Stage-4 (Neural-network analysis)

The Stage-4 evolution of the HAT Stages flowchart is shown in Figure 6-14. To register a **new user**, a new neural-network is trained using their HAT template in opposition to all existing user templates. If authenticating an **existing user**, their HAT template will be processed within all existing user neural-networks, and the most positive results assumed.

6.2.4.1 A Neural-Network for HAT

The neural-network design used by HAT was determined through extensive network trials designed to optimise performance against speed of execution. The final design was a feed-forward single-layer neural-network consisting of twenty-five inputs, one for each of the HAT template spot-frequencies, twenty-five neurons, and a single output defined by a hyperbolic tangent-sigmoid transfer function[1] (An introduction to neural-networks and their transfer functions is included in Appendix E). A schematic of the 25-25-1 neural-network is shown in Figure 6-15, the enlargement illustrating the complex web of connections for each neuron providing the network with its inherent analytical power.

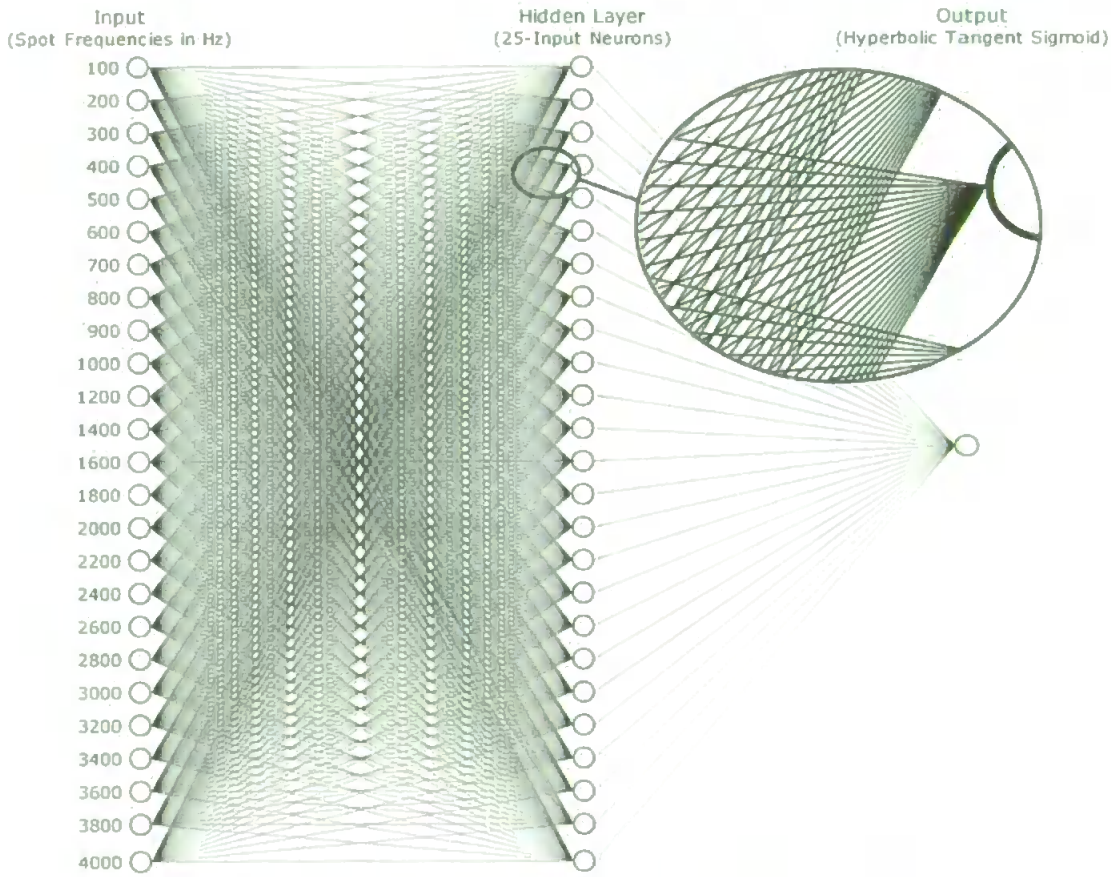


Figure 6-15 : The single layer, twenty-five neuron neural-network adopted by HAT

Each individual neuron of the single *hidden-layer* contains twenty-five inputs and one output; this is illustrated in the single neuron example in Figure 6-16.

[1] The tansig transfer function is a logsig transfer function symmetrical about the X-axis (see Appendix E).

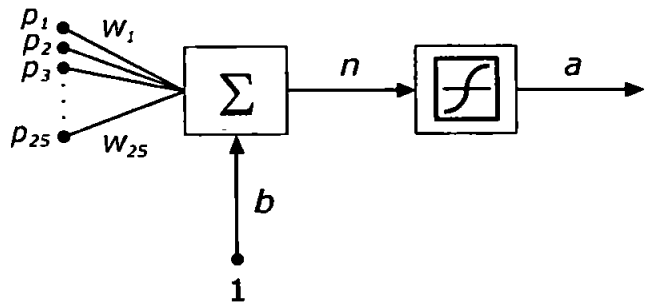


Figure 6-16 : A twenty-five input HAT neuron

The HAT neuron incorporates a symmetrical tan-sigmoid transfer function, which scales the neuron output into the range -1 a 1, where a is defined by the function:

$$a = \frac{e^n - e^{-n}}{e^n + e^{-n}}$$

The final neural-network configuration, illustrated in Figure 6-15, was refined through extensive experimentation, in order to realise the best balance of performance against process cycle time: a key variable within this balance was the networks training error rate. Although it is feasible to specify error rates in excess of 1 in 1000 (1e-4), the processing time can easily exceed acceptable limits, as shown in the next example.

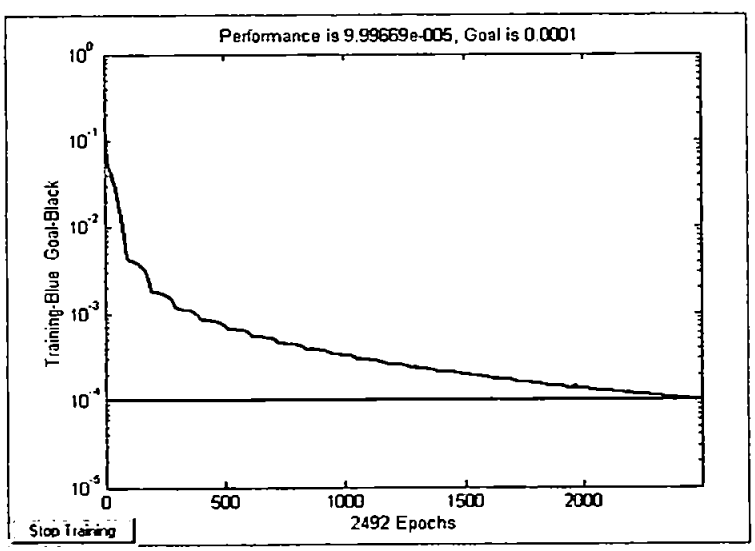


Figure 6-17 : Training a new user's HAT neural-network for 1 in 10,000 errors

Example: The processing time of the HAT neural-network for a new user, within a user-base[1] of only *four* users, at an error rate of 1 in 10,000 (1e-4), is in excess of 2500 epochs[2] (Figure 6-17). This equates to around 30 seconds processing time on a current (2005) desktop PC, with a CPU typically drawing in excess of 50 watts; by comparison mobile handset CPUs generally draw less than 1 watt (AMD 2005). It is acknowledged that the power/performance profile of desktop and mobile CPUs is constantly being improved.

HAT therefore defines a performance error goal during training of 1 in 1000 (1e-3). With a user group of around twenty users, and the available hardware, this was found to offer the best performance/processing-time balance, with a full training cycle consistently taking around 400 epochs (Figure 6-18), less than 20 seconds.

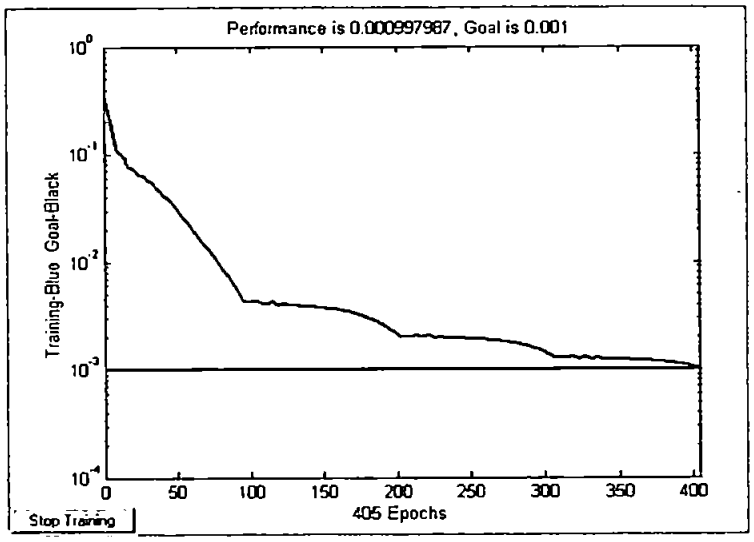


Figure 6-18 : Training a new user's HAT neural-network for 1 in 1000 errors

Although a new user only has to train their personal neural-network once at registration, all biometric templates require refining over time due to the changing character of their owner (Section 4.2.2). System accuracy also benefits from training a user's template(s) against as many of the systems user-base templates as is practicable, identifying *good* and *bad* training data (behaviour): HAT trains all users against all other users in the user-base.

[1] The complete set of registered system users: for HAT, this is the set of twenty trial users in Section 7.3.
[2] An epoch is a neural-network processing cycle.

6.2.5 Stage-5 User Classification and System Response

The final stage of the HAT authentication process is the classification of the neural-network output data. The authentication stage involves the comparison of the HAT Stage-4 output against a pre-determined authentication threshold.

It is an aspect of the HAT authentication technique that the threshold(s) defined by HAT for user authentication are unique to each registered user, and are dependent upon:

- the consistency of individual users' templates (data sets);
- the variance in users' templates across the entire user-base;
- the performance error of individual users' HAT Stage-4 neural-networks.

An individual user's authentication threshold is calculated during HAT Stage-4 Analysis by feeding examples of known good and bad data into the neural-network, monitoring the resultant outputs, and setting a value which minimises FMR and FNMR (Section 4.2.3). The variance in user-base templates, generic threshold values and match error rates are mutually exclusive and defined by the relationship shown in Figure 6-19.

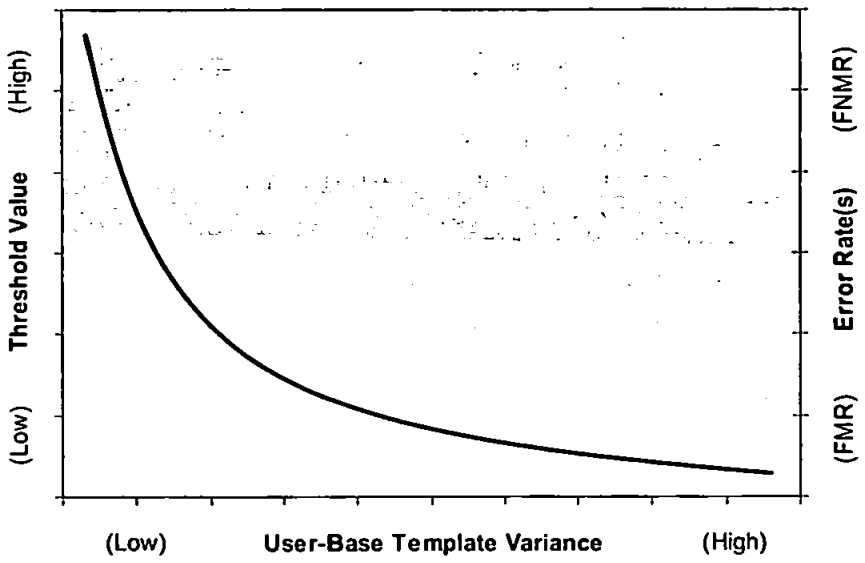


Figure 6-19 : The mutually exclusive relationship between HAT authentication thresholds and match error rates vs. user-base template variance

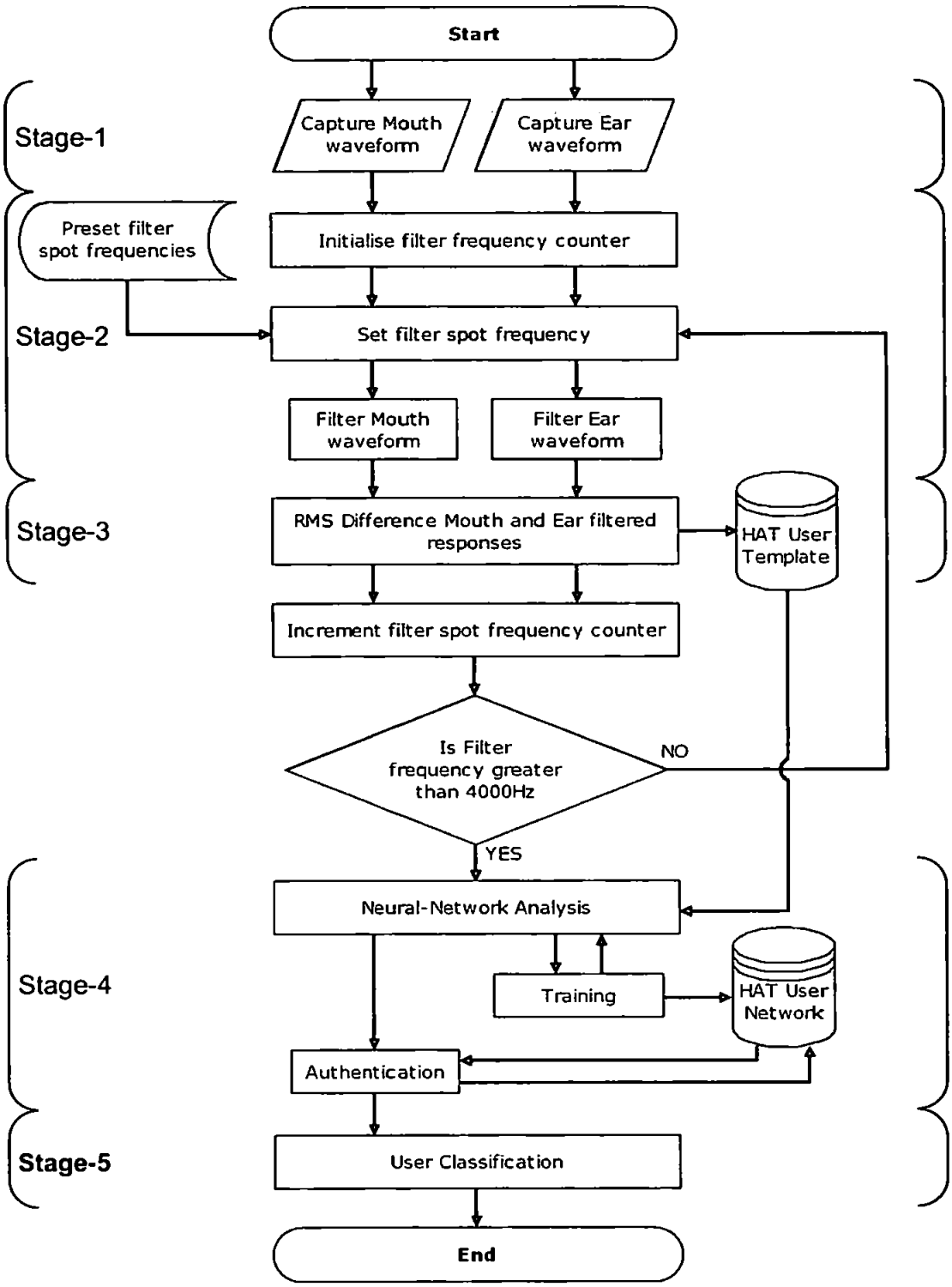


Figure 6-20 : Complete HAT Stages flowchart - Stage-5 (User Classification)

HAT Stage-5 User Classification is the final stage in the HAT authentication process and is placed in context within the HAT stages flowchart illustrated in Figure 6-20: this flowchart now describes the complete HAT process.

6.2.6 The HAT Template

The HAT absorption[1] template is defined by the unique shape contained within mouth-to-ear absorption curves of an individual user, and is governed by:

- the number and specifications of spot-frequencies[2] discussed in HAT Stage-2;
- the consistency of individual users' mouth-to-ear absorption responses.

Each of the twenty-five spot-frequencies (Section 6.2.1.3) is used to determine a discrete bio-metric, which collectively define a user's HAT template. Each spot-frequency mouth-to-ear (MEa) absorption metric is described by the following formulae:

$$MEa(\%) = \frac{Ear}{Mouth} * \frac{100}{1}$$

...where the *Mouth* and *Ear* values are defined as the RMS value of the relevant spot-frequency passband (Figure 6-12). The root-mean-square (RMS) interpretation is required to accommodate for the signed quantisation levels[3] of 16-bit wave files. The resultant MEa value is preserved as a percentage, rather than a difference value, to allow for amplitude fluctuations in the individual spot-frequency stimuli. In Figure 6-21 and Figure 6-22, two examples of Mouth and Ear input stimuli are shown along with their associated HAT absorption template, for the individual numbers '0' and '3' respectively. These plots are extended in Figure 6-23 and Figure 6-24, to include full sets of fixed (number '1') and variable (numbers '0' to '9') stimuli respectively on a single axis. By inspection of this pair of graphs, the fixed stimuli *control* set exhibits very little spread, compared to the greater spread of the variable data set. However in both cases, and allowing for the varying input stimuli, the HAT template(s) show consistent shape.

[1] Although absorption is not the only factor effecting mouth-to-ear variance, it is the predominant modifier, and hence the method was named as such.
[2] HAT Stage-2 'spot frequencies' are referred to in some analyses plots as 'centre frequencies'.
[3] Quantisation levels of 16-bit wave file samples are in the range: -32768 to +32767.

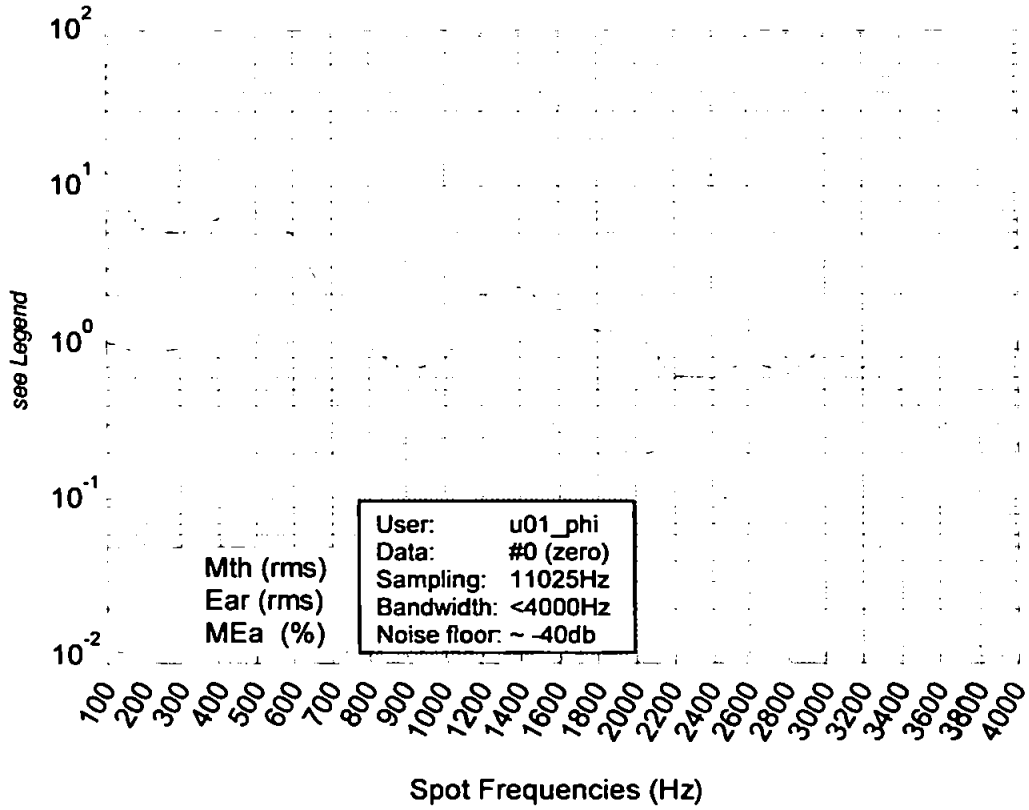


Figure 6-21 : Mouth, Ear *input* and HAT template *output* curves of the number '0' HAT trial user 'u01_phi' (100Hz < bw < 4000Hz)

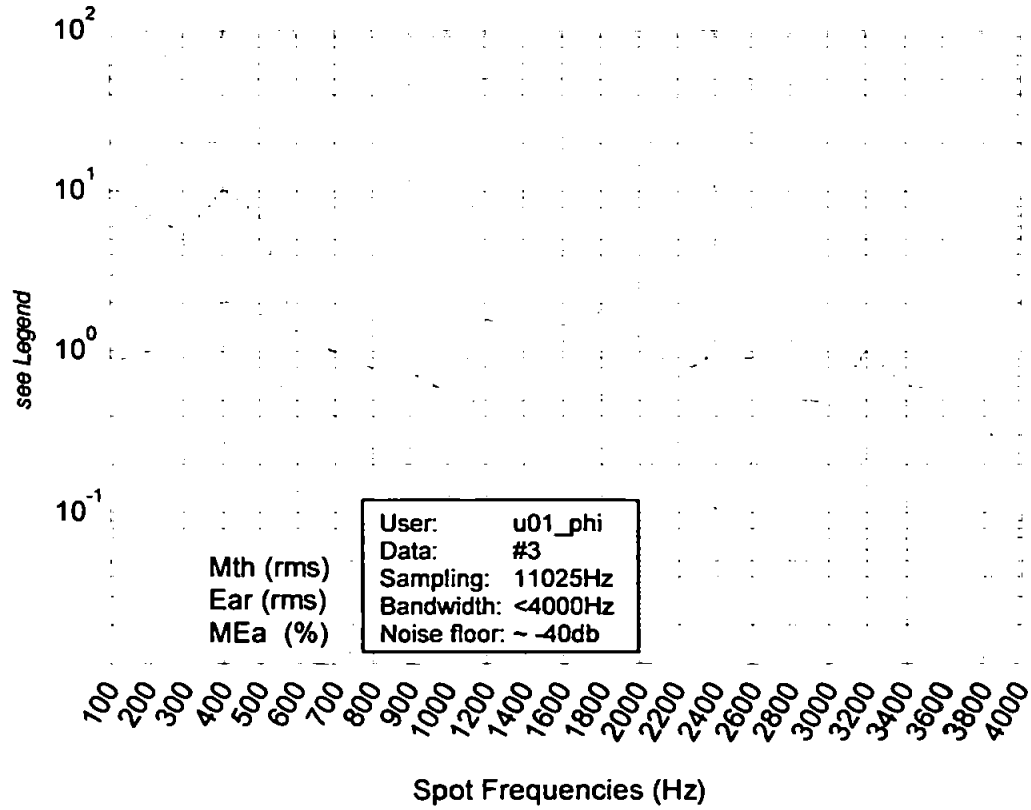


Figure 6-22 : Mouth, Ear *input* and HAT template *output* curves of the number '3' HAT trial user 'u01_phi' (100Hz < bw < 4000Hz)

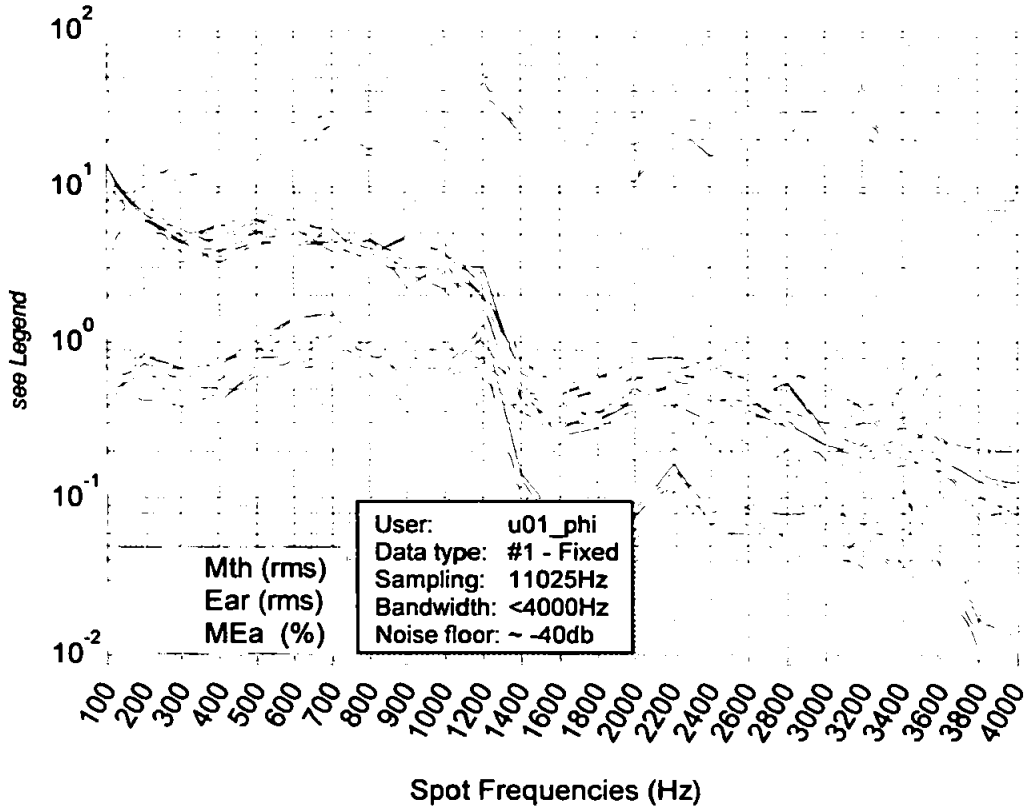


Figure 6-23 : Compound Mouth, Ear *input* and HAT template *output* curves of the number '1'. HAT trial user 'u01_phi' (100Hz < bw < 4000Hz)

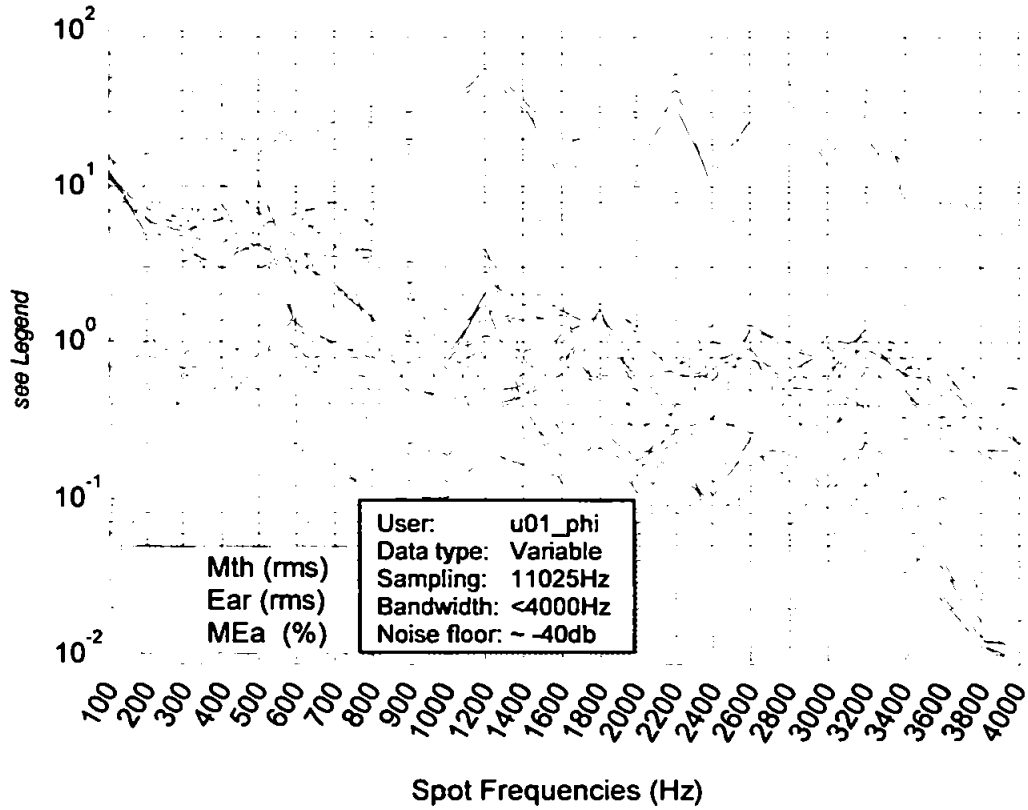


Figure 6-24 : Compound Mouth, Ear *input* and HAT template *output* curves of the numbers '0' to '9'. HAT trial user 'u01_phi' (100Hz < bw < 4000Hz)

By comparing the HAT templates in the previous example, with those of another user from a series of trials (see Section 7.3), Figure 6-25 through to Figure 6-28 show that for both a fixed stimuli control set (using just the number '1'), and for the numbers '0' to '9'[1], trial participants' individual response curves exhibit a clear collective pattern match or correlation with themselves; even though the numbers are phonetically quite different. The key observations are summarised as:

- the consistent shape of the individual users' sets of discrete curves;
- the unique shape of the individual user's collective response;

6.2.6.1 The 4000Hz Cut-off

In Section 6.2.1.2 (Figure 6-4), the 4000Hz information roll off was introduced. Through experimentation, this was found to be the upper limit of unique head authentication data. By further inspection of the wideband (100Hz < bw < 8000Hz) plots shown in Figure 6-25 through to Figure 6-28, this trend can be observed above the 4000Hz spot-frequency. It was also found during HAT development that an alternate cross-correlation head authentication methodology (see Section 6.3) exhibited the same information break down above 4000Hz. Following the Nyquist[2] sampling principle, with the highest HAT Stage-2 spot-frequency set optimally at 4000Hz, a system sampling rate of at least 8000Hz was required: the nearest *standard* sampling rate[3] to this was 11025Hz. This optimisation of the system sampling rate offered the following advantages:

- smallest efficient sample sizes (in bytes);
- removal of unnecessary (unproductive) system resolution (above 4000Hz);
- reduced HAT analysis time, resulting in reduced system authentication cycle time;
- reduced processing requirements, resulting in reduced system power requirements.

[1] The captured sample filenames are displayed in the individual plot legends, and adopt the following syntax: <name (3 characters)>_<capture set (1 character)>_<spoken text (2 characters)>
[2] The Nyquist rate is the minimum sampling rate required to recover all Fourier components of a periodic waveform. It is calculated as at least twice the highest frequency component of the capture waveform.
[3] A factor of 44.1KHz, the domestic CD sampling rate and a standard Windows® supported rate.

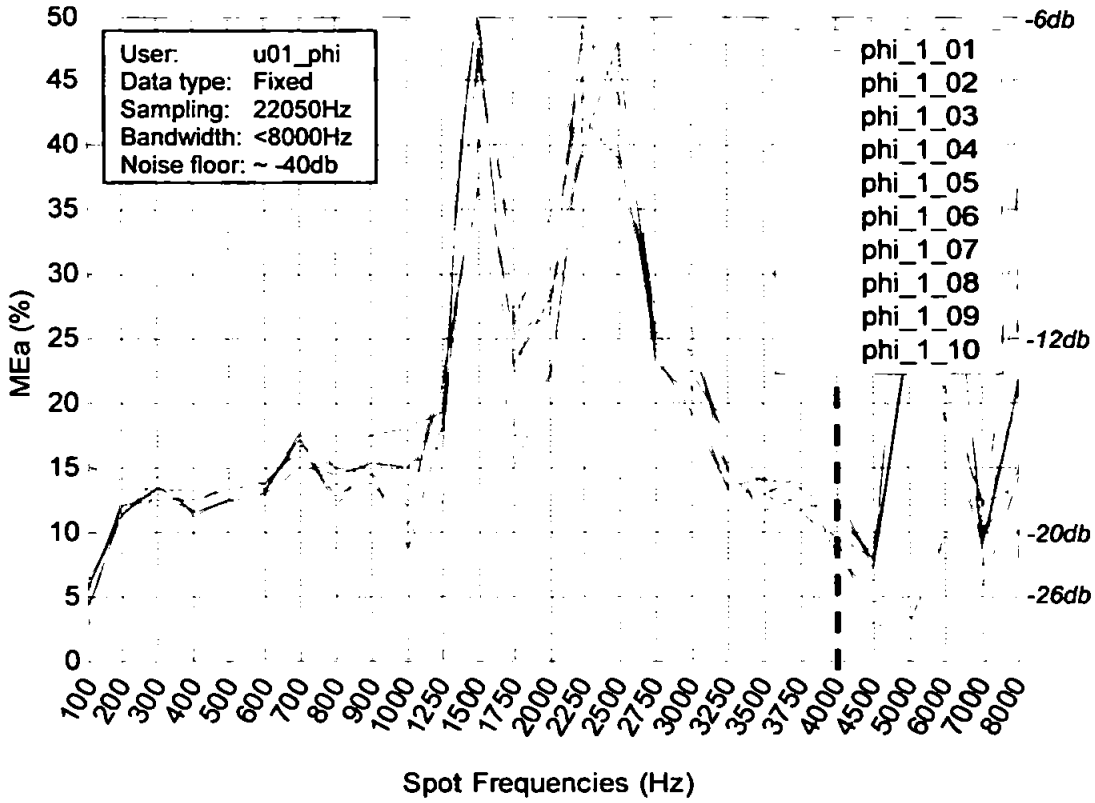


Figure 6-25: Compound frequency absorption curves of the number '1' (x10) - HAT trial user 'u01_phi' (100Hz < bw < 8000Hz)

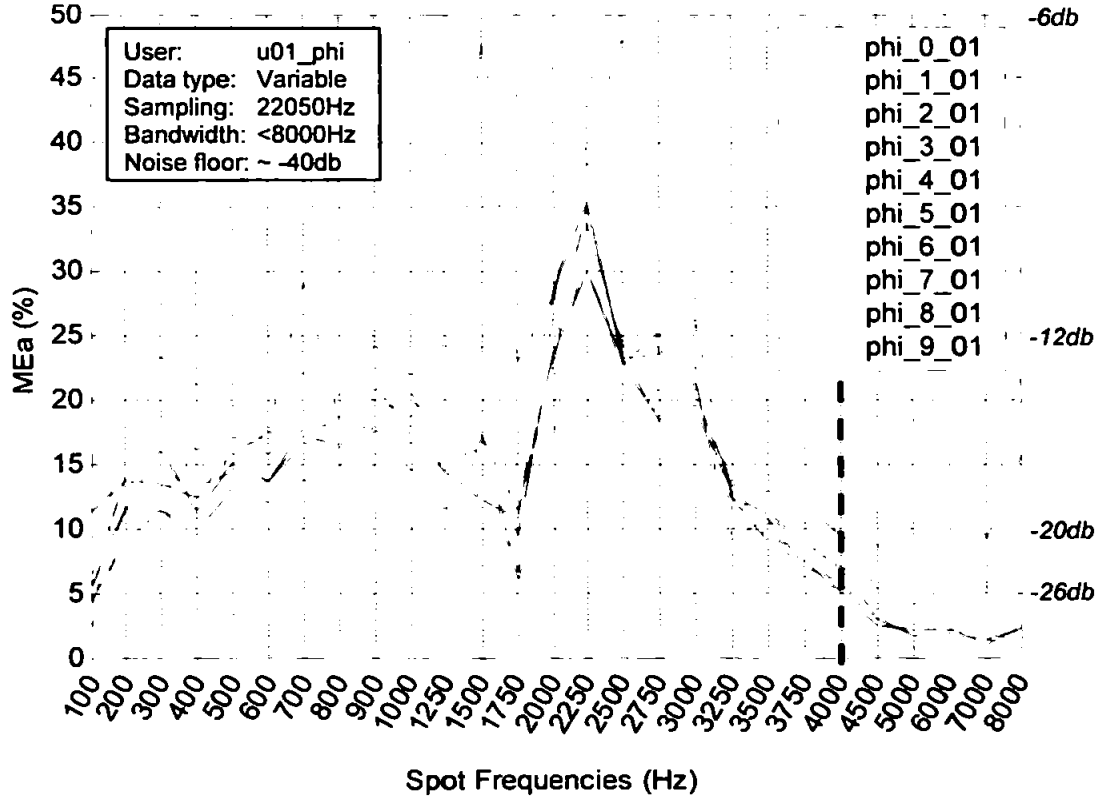


Figure 6-26: Compound frequency absorption curves of the numbers '0' to '9' - HAT trial user 'u01_phi' (100Hz < bw < 8000Hz)

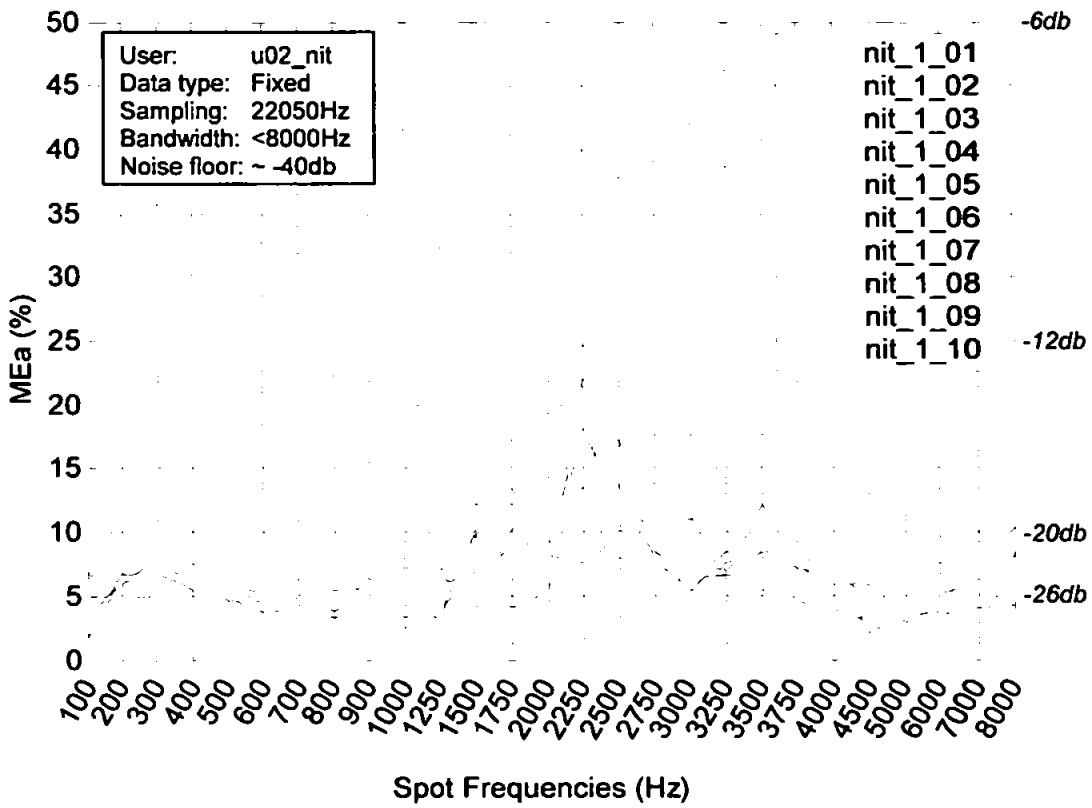


Figure 6-27: Compound frequency absorption curves of the number '1' (x10) - HAT trial user 'u02_nit' (100Hz < bw < 8000Hz)

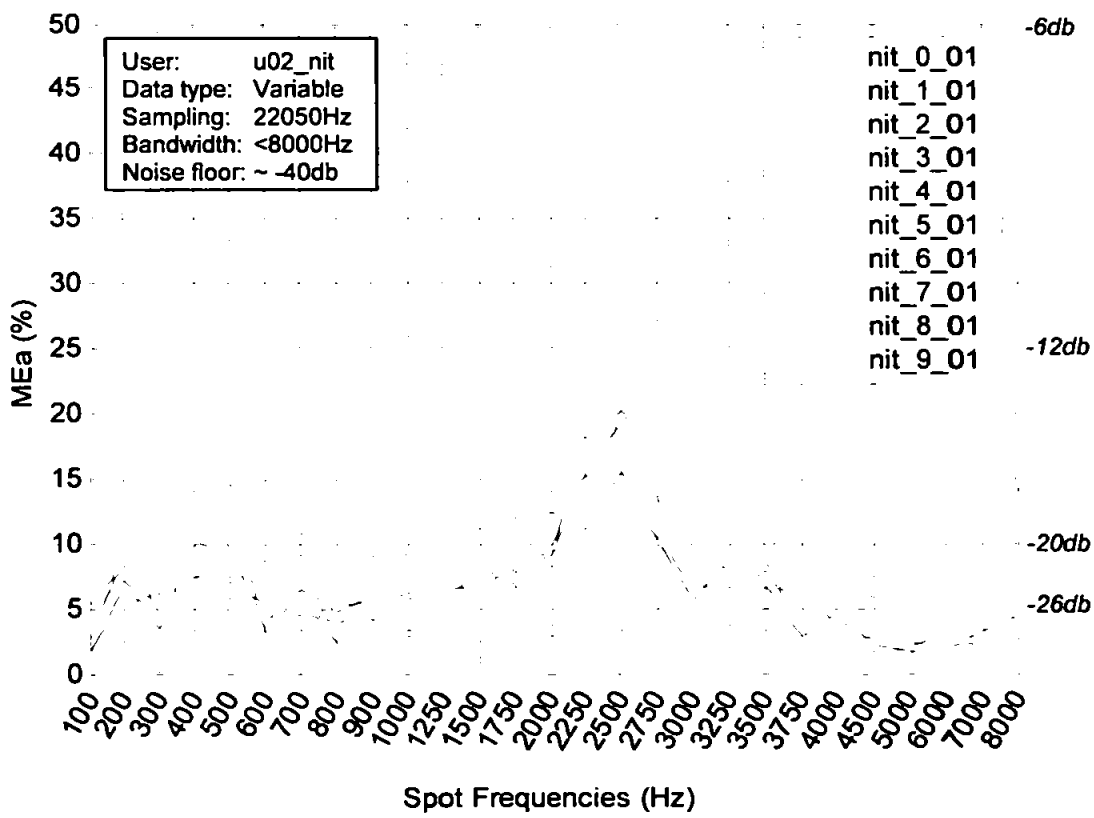


Figure 6-28: Compound frequency absorption curves of the numbers '0' to '9' - HAT trial user 'u02_nit' (100Hz < bw < 8000Hz)

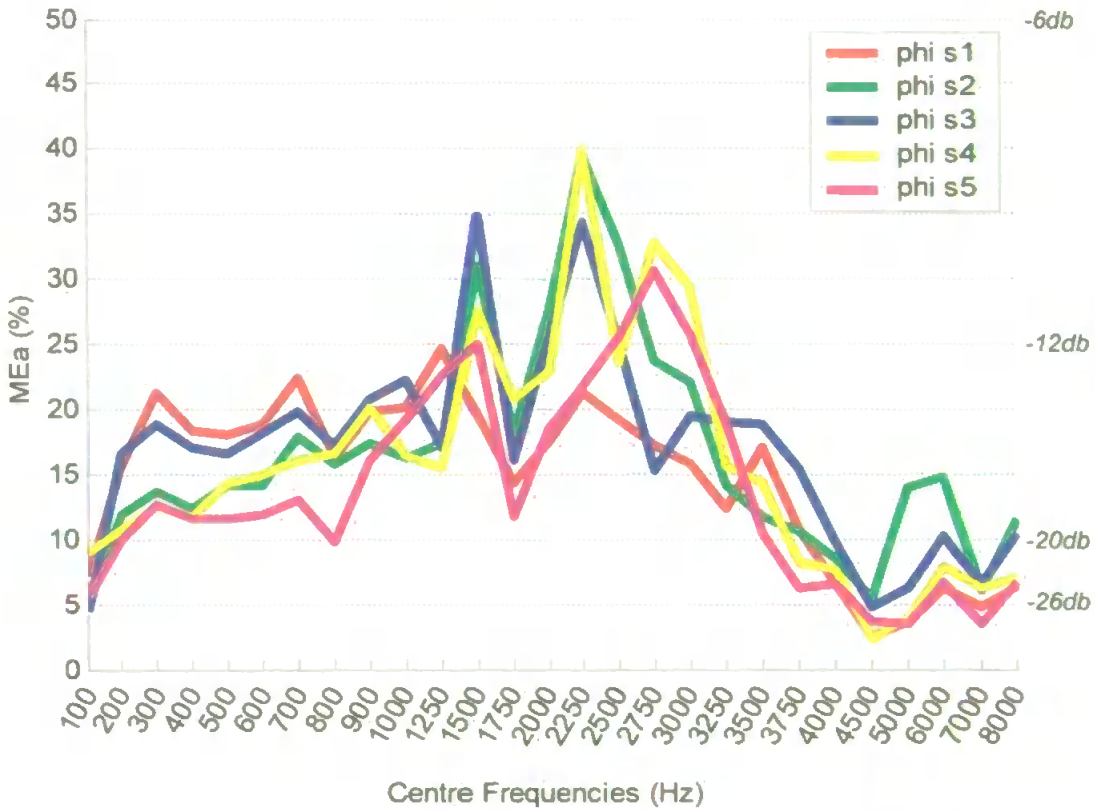


Figure 6-29 : Five mean frequency absorption curves of the numbers '0' to '9' - HAT trial user 'u01_phi' (100Hz < bw < 8000Hz)

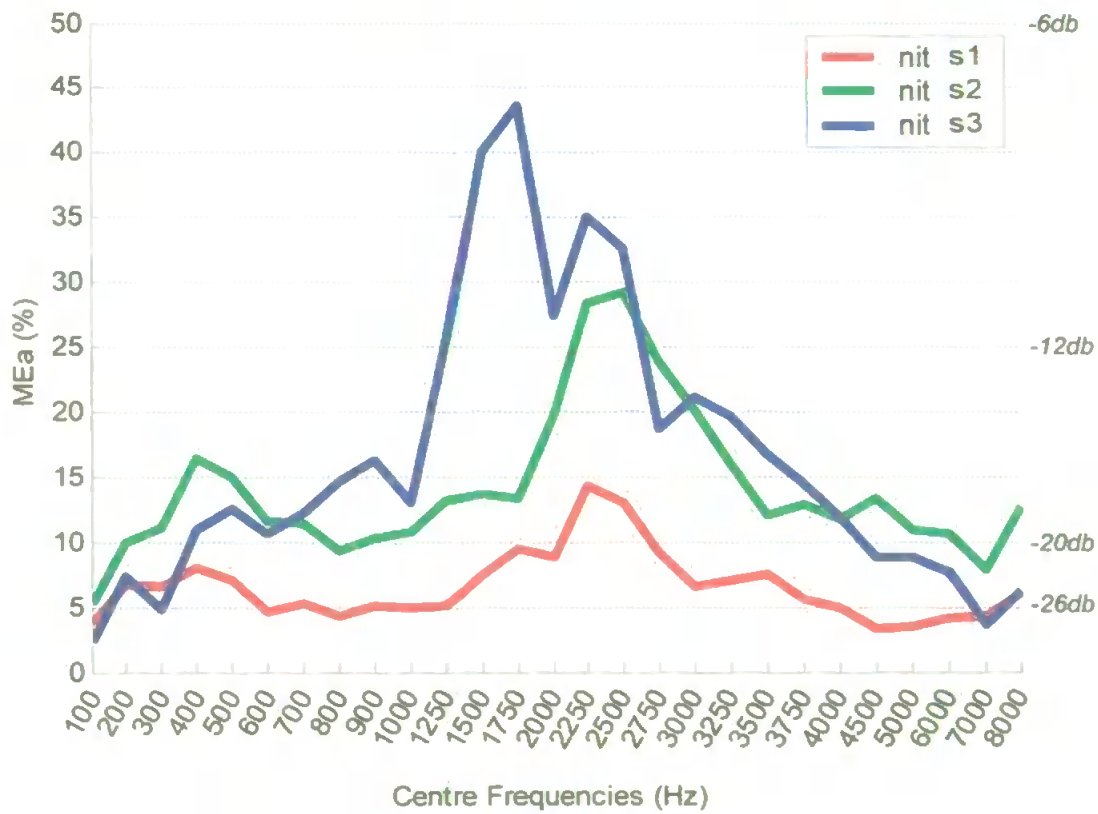


Figure 6-30 : Three mean frequency absorption curves of the numbers '0' to '9' - HAT trial user 'u02_nit' (100Hz < bw < 8000Hz)

When the same two users were subjected to multiple testing sessions over a number of days, statistical mean response curves were calculated for each session, and the results are displayed collectively in Figure 6-29 and Figure 6-30 respectively. These results, along with the results for other trial participants in Section 7.3.4, present a strong case in support of the consistent and unique shape of individual user's HAT responses. It is these unique mean biometric absorption spectra which form the **HAT templates.**

6.2.6.2 Statistical Analysis of a HAT Template

As part of HAT template analysis, statistical calculations on sets of absorption curves were also performed, calculating mean, median and standard-deviation at each spot-frequency; an example of a statistical analysis plot is shown in Figure 6-31.

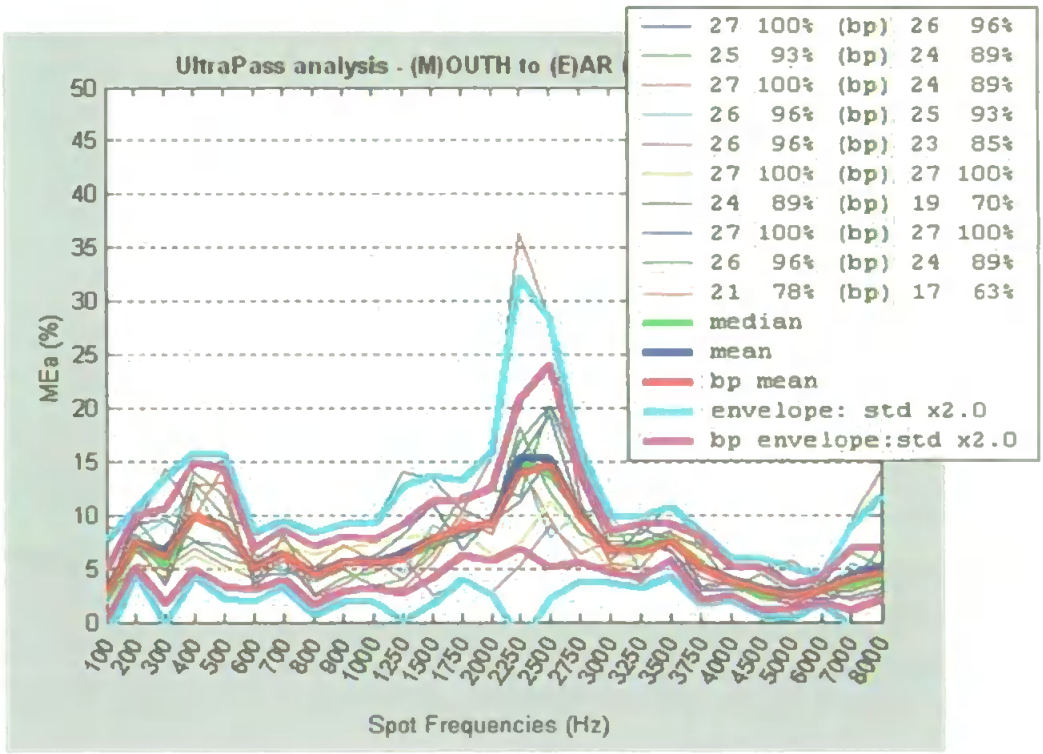


Figure 6-31 : Statistical analysis curves for a HAT capture waveform set

By comparison with the example, it was found that for the majority of cases, the mean curve (in blue) and the median curve (in green) followed almost identical paths.

Two sets of standard deviation curves were also calculated and plotted, a complete capture set (in cyan), and a band-pass[1] (bp) processed set (in magenta), producing an effective user's authentication envelope. Recall that standard deviation[2] (σ) is proportional to variance (σ^2) and indicates how tightly a set of sample data is clustered around its mean, where:

- 68% of samples lie within 1 standard-deviation of the mean ($\mu-\sigma \rightarrow \mu+\sigma$);
- 95% of samples lie within 2 standard-deviations of the mean ($\mu-2\sigma \rightarrow \mu+2\sigma$);
- 99.7% of samples lie within 3 standard-deviations of the mean ($\mu-3\sigma \rightarrow \mu+3\sigma$).

This operational envelope was later used to help determine system response thresholds to authentication sample data, discussed in HAT Stage-5 Thresholds (Section 6.2.5).

By inspection of the plot legend in Figure 6-31, the number of samples within two standard-deviations of the mean is shown; as both a number (column_1) and as a percentage (column_2). Bandpass values are also shown in column_3 and column_4 respectively. The higher the percentage, in each case, the tighter and more consistent the capture set, and the more unique the user's HAT signature. By observation, this example shows a very good response, with 70% of full sample sets falling within 90% of the defined envelope, and an even better 90% of bandpass processed samples. In relation to the HAT system, these figures translate into reduced false match (FMR) and false non-match (FNMR) error rates (Section 4.2.3) experienced by the user.

[1] In this context, band-pass refers to a set of data with singular sample outliers removed.
[2] A full explanation of statistical terms and analyses is beyond the scope of this text, and is covered extensively in literature and on the Internet (Link: Statistics).

6.3 The Head Authentication Correlation Method

The *correlation method*[1] of head authentication is an alternative novel way of extracting a unique biometric template from multiple audio data streams captured from points on a user's head. The technique utilises temporal (or phase) variations between discrete narrowband spectra within the audio data stream introduced by the propagation path.

The process can be broken down into five distinct stages of operation, in a similar way to the absorption method discussed previously in Section 6.2. Although Stage-1 Capture now includes some pre-processing, it is Stage-3 which essentially differs:

1. **Capture** multiple voice stimulated PCM audio data streams. Basic HAT[2] utilises two external capture points: the Mouth and the Ear. *Normalise Ear waveform.*
2. **Filter** each data stream discretely at multiple pre-selected frequencies using a high roll-off, narrowband FIR filter. Basic HAT utilises twenty-five spot-frequencies.
3. **Correlation** calculates the temporal variation between captured waveforms at each spot-frequency. Basic HAT compares discrete frequency pairs of Mouth and Ear.
4. **Analysis** of the RMS difference output, by feeding the resultant data array into a pre-trained neural-network. The training data for the HAT neural-network consisted of one of the data sets collected during the HAT field trials in Chapter 7.
5. **Classification** of the neural-network result by comparison with a preset authentication threshold. The HAT authentication threshold was determined during network training.

This section discusses the changes Stage-1 pre-processing and Stage-3 Correlation introduce into the HAT authentication methodology, drawing parallels where appropriate with the absorption methodology. The alternate five stages of the correlation method are shown schematically in Figure 6-32.

[1] Not generally referred to as the 'HAT correlation method' as it was not a part of the final HAT process.
[2] 'Basic HAT' describes the *minimum* operational requirements of the HAT process. The technique does however have the potential for increasing the systems resolution; see future work in Section 8.3.

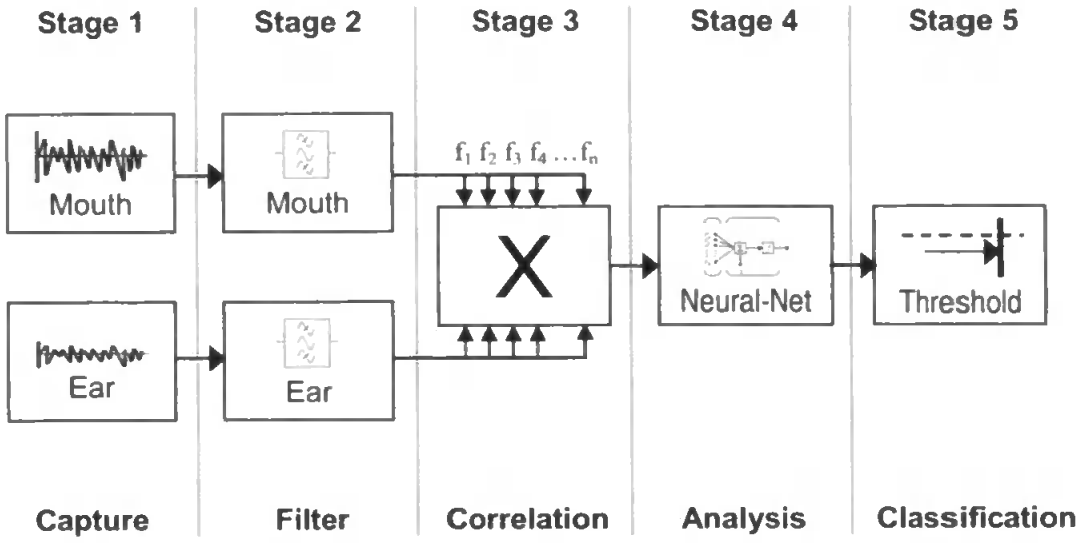


Figure 6-32 : The five discrete stages of the correlation authentication process

6.3.1 Stage-3 Correlation of Filtered Frequency Pairs

To determine the amount of temporal shift introduced into the ear-wave after propagation through the head, the correlation method sequentially cross-correlates all individual samples from each waveform. This is achieved by effectively sliding the two waveforms past each other, end to end, one sample at a time, performing a correlation at each stage (Figure 6-33).

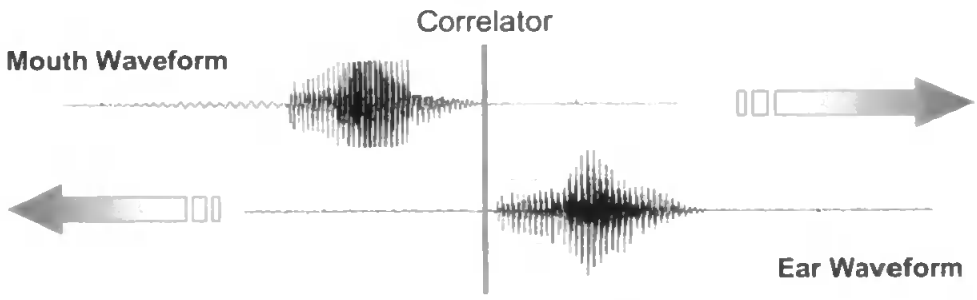


Figure 6-33 : Cross-correlation of Mouth and Ear waveforms

Recall that given a pair of related measures for a set of items, the correlation coefficient provides a measure of the degree to which the paired measures linearly co-vary. The correlation coefficient is usually a value between zero and one, where zero represents no detectable correlation between the two items and one represents no detectable difference.

By comparing the cross-correlation value of the mouth and ear waveforms at each stage, it is possible to determine the point at which the waveforms align, and hence determine the slippage (in samples) between the two waves. Examples of waveform offset can be seen in the correlation plots (X-Correlation) within Figure 6-38 to Figure 6-45 inclusive. By dividing the sample offset by the sampling rate it is possible to calculate the amount of slippage in actual time (Example: 50 samples = 4.5milliseconds @ 11025Hz).

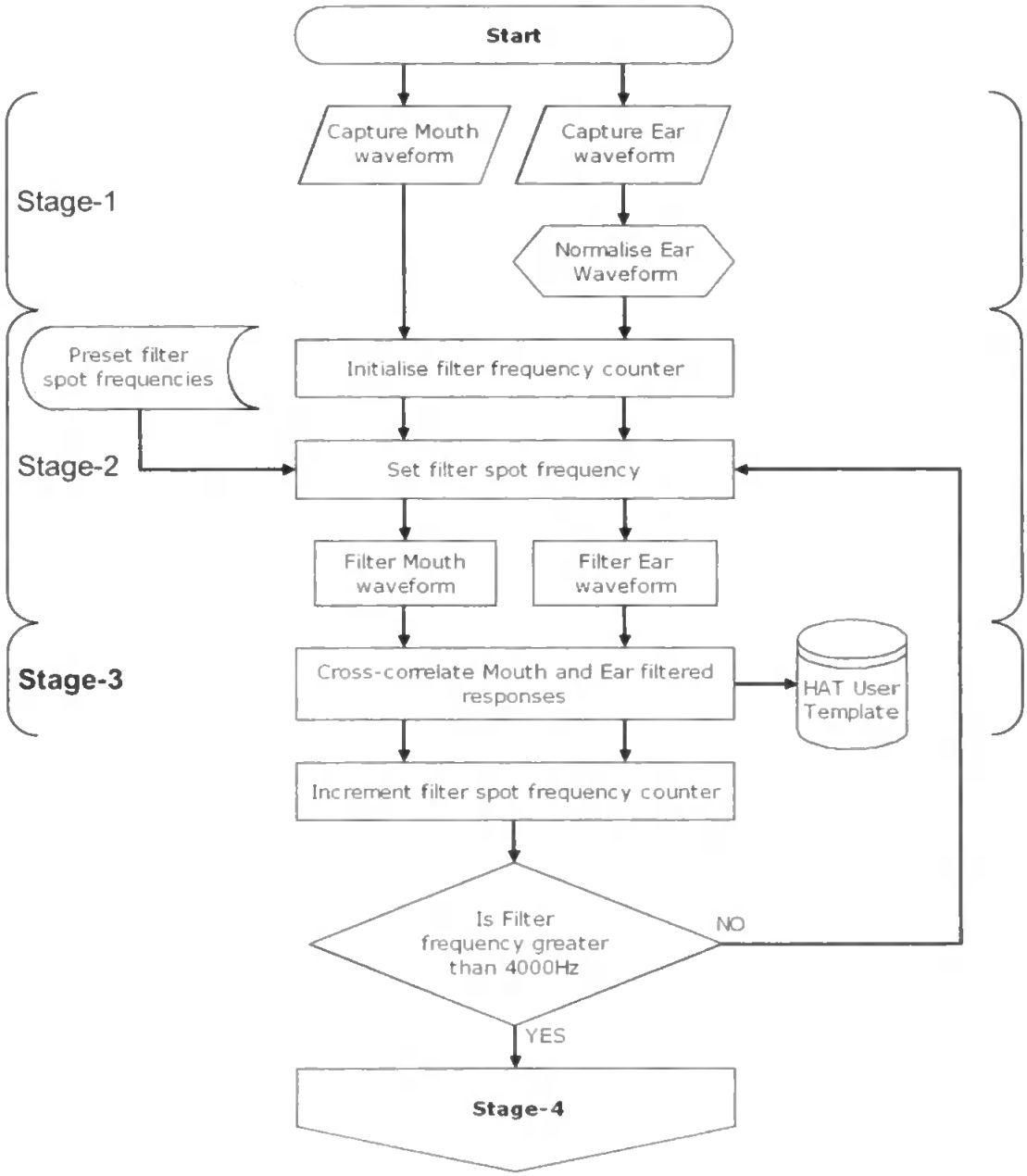


Figure 6-34 : Modified HAT Stages flowchart - Stage-3, showing additional correlation method Stage-1 Normalisation and Stage 3 Correlation.

The modified HAT Stages Flowchart illustrated in Figure 6-34 shows Stage-3 Correlation in place of the HAT Stage-3 Absorption process. Stage-4 Analysis is not affected by the change, as the neural-network does not distinguish between an absorption value between '0' and '1' (0 – 100%) and a correlation coefficient between '0' and '1'. The flowchart also includes an additional normalisation process within the Stage-1 Capture; this is discussed in the next section.

6.3.1.1 Normalisation of the Ear Sample Waveform

For HAT to effectively identify the temporal shift introduced by the audio propagation path between voicebox and mouth and voicebox and ear through cross-correlation, it was found that the process benefited from amplitude normalisation of the ear sample to the mouth sample. Captured HAT ear samples naturally suffer, on average, 12dBs of attenuation by comparison with the mouth sample, illustrated in Figure 6-35.

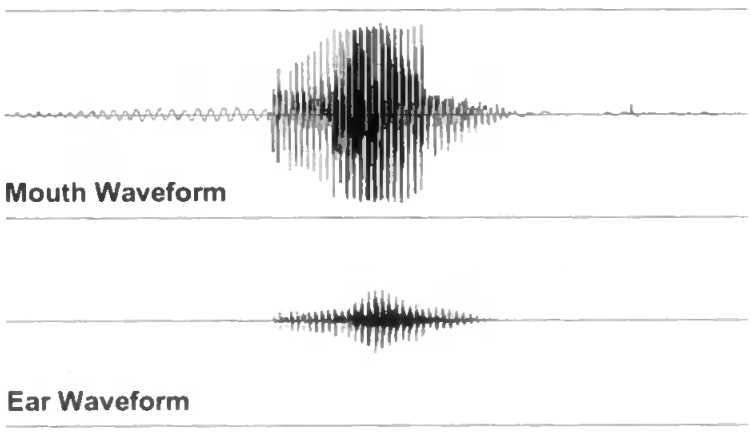


Figure 6-35 : Captured HAT waveform pair (Mouth & Ear) of the number '2'

Sample normalisation is considered a part of the Stage-1 Capture process and is performed in preparation for the latter filtering and cross-correlation stages. Normalisation of the ear sample is based on a peak value analysis of the mouth sample; the processed waveform from the previous example is illustrated in Figure 6-36.

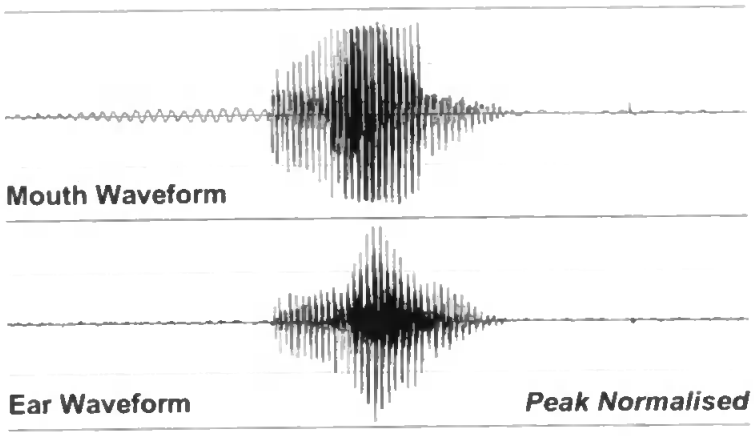


Figure 6-36 : Normalised HAT waveform pair (Mouth & Ear) of the number '2'

6.3.1.2 The 4000Hz Cut-off

It was found that the correlation analysis method also suffered the same reduction in performance above around 4000Hz, as the HAT absorption method discussed in Section 6.2.6.1. In fact, not only did cross-correlation performance reduce at 4000Hz, it was found that the correlation process failed, with no discernable correlation detectable. This is clearly illustrated in the set of compound analyses plots (presented in 1000Hz increments) shown in Figure 6-38 to Figure 6-45 inclusive. The plots indicate:

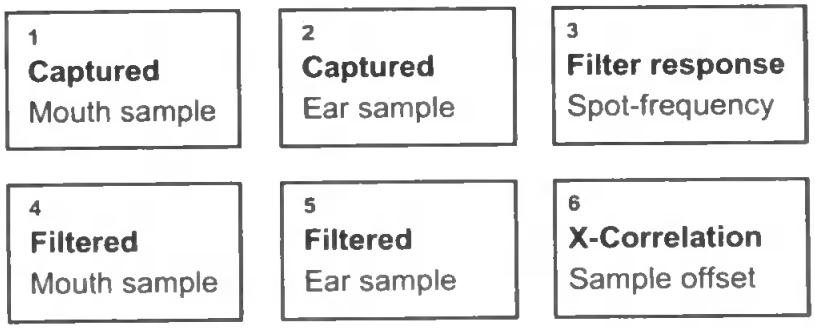


Figure 6-37 : Legend of correlation Figure 6-38 to Figure 6-45 inclusive

By inspection, mouth-to-ear cross-correlation (X-Correlation) shows clear correlation at all frequencies up to 4000Hz, indicated by the clear central peak rising out of the non-correlation noise floor (Legend: Figure 6-37). Above 4000Hz (Figure 6-42), it can be seen correlation is lost and the resultant plot consists entirely of uncorrelated noise.

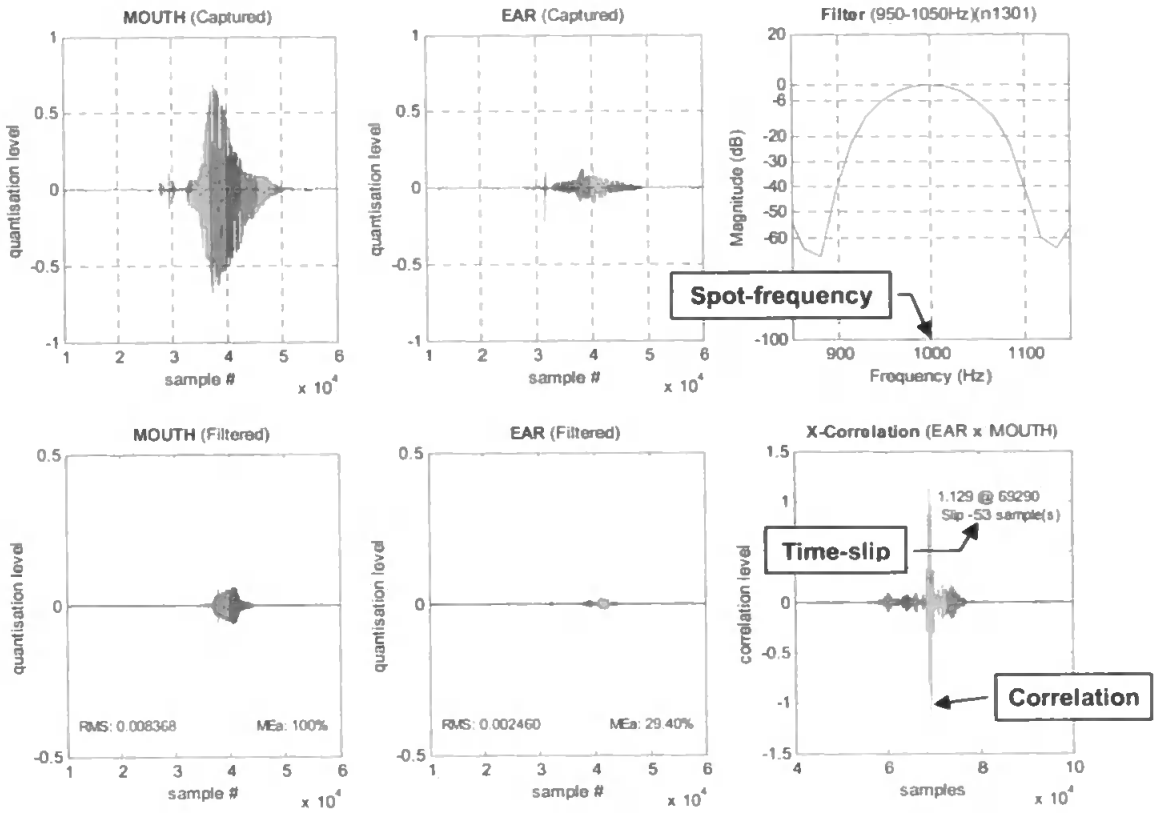


Figure 6-38 : HAT Analysis - Capture, Filter and Correlation @ **1000Hz**

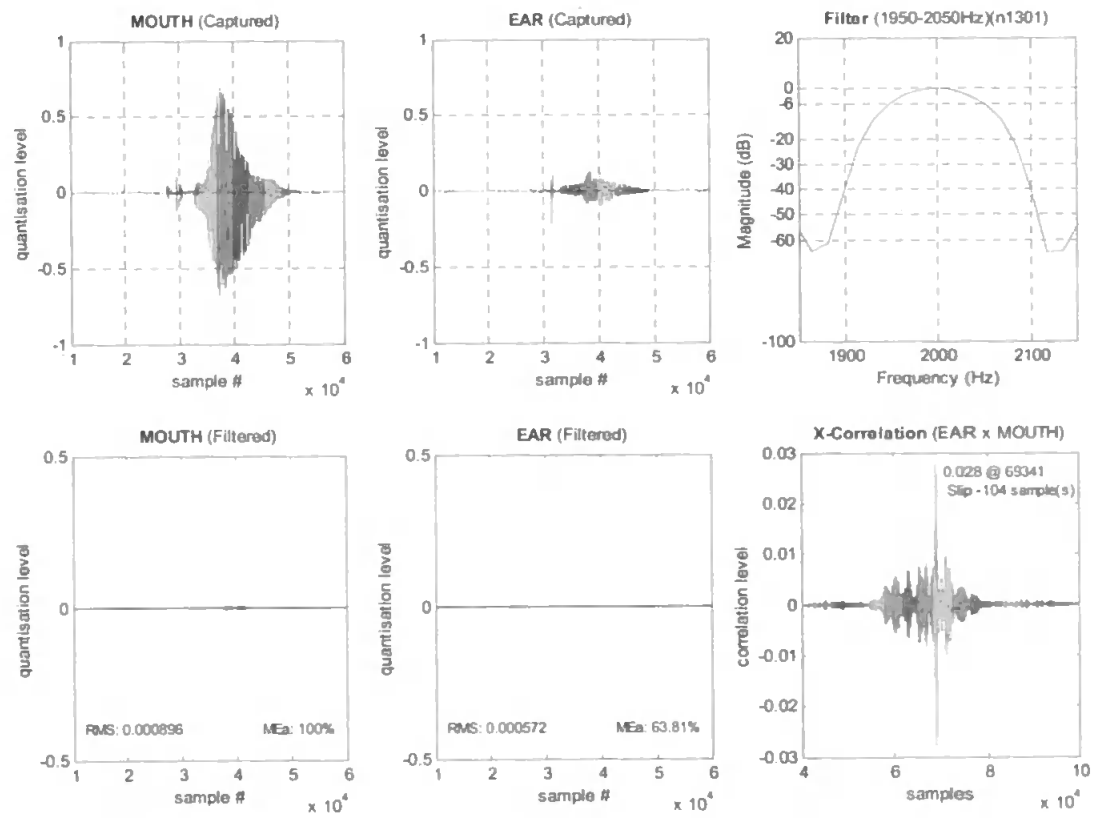


Figure 6-39 : HAT Analysis - Capture, Filter and Correlation @ **2000Hz**

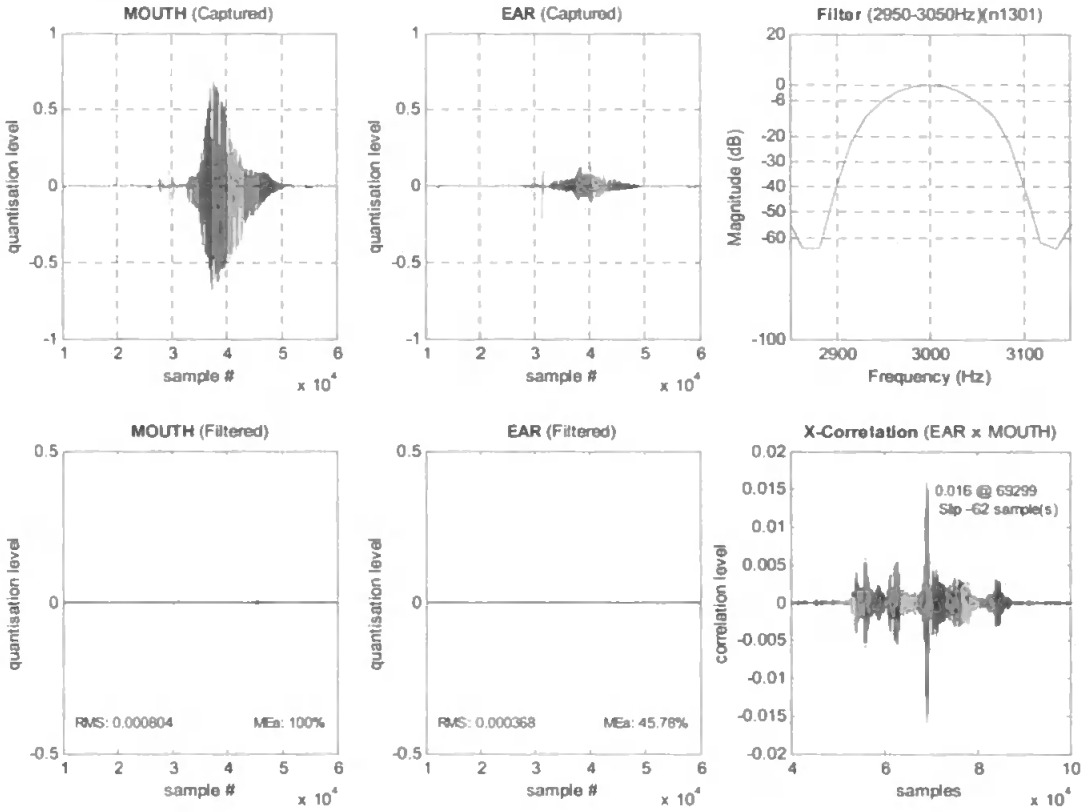


Figure 6-40 : HAT Analysis - Capture, Filter and Correlation @ **3000Hz**

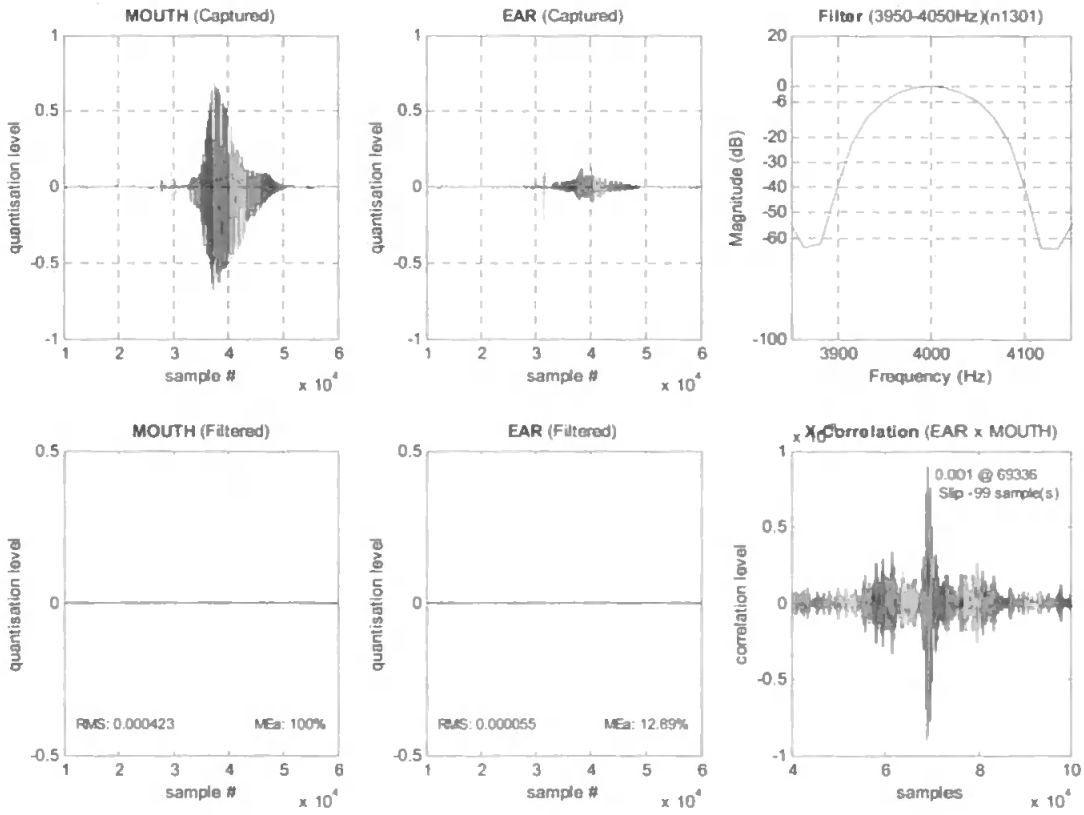


Figure 6-41 : HAT Analysis - Capture, Filter and Correlation @ **4000Hz**

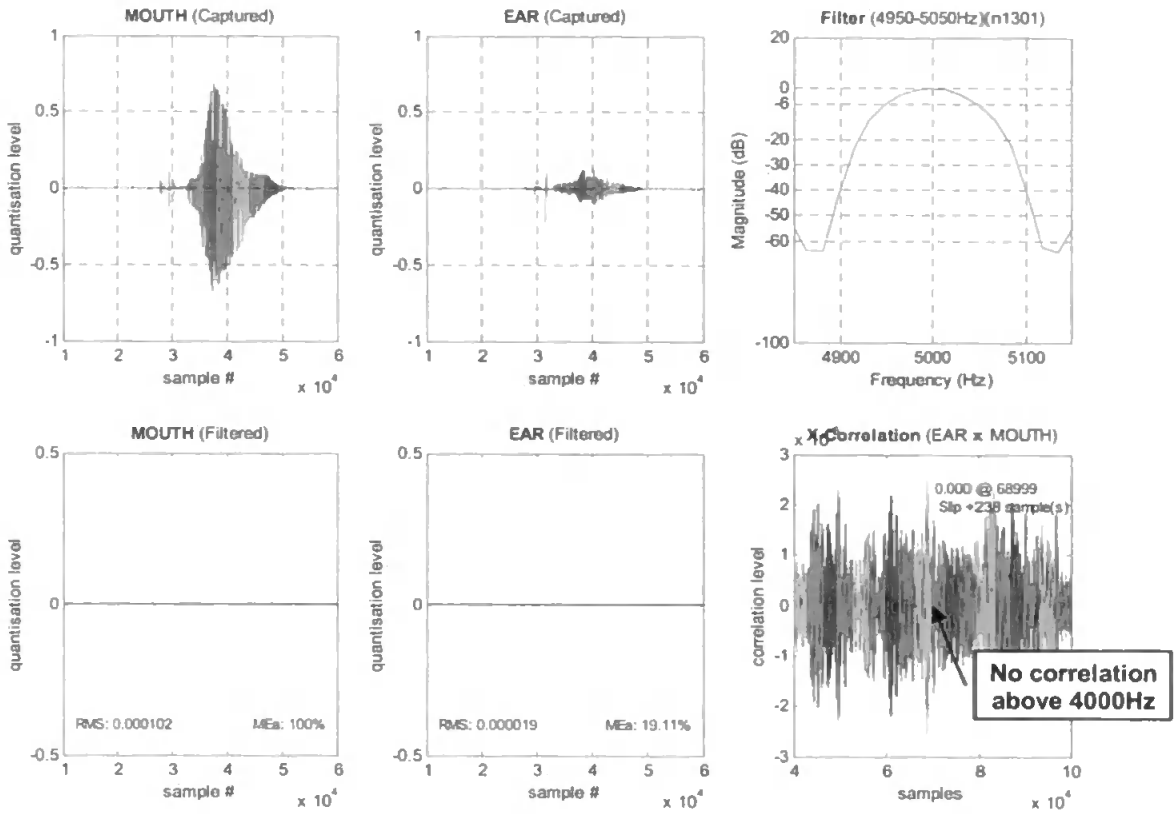


Figure 6-42 : HAT Analysis - Capture, Filter and Correlation @ **5000Hz**

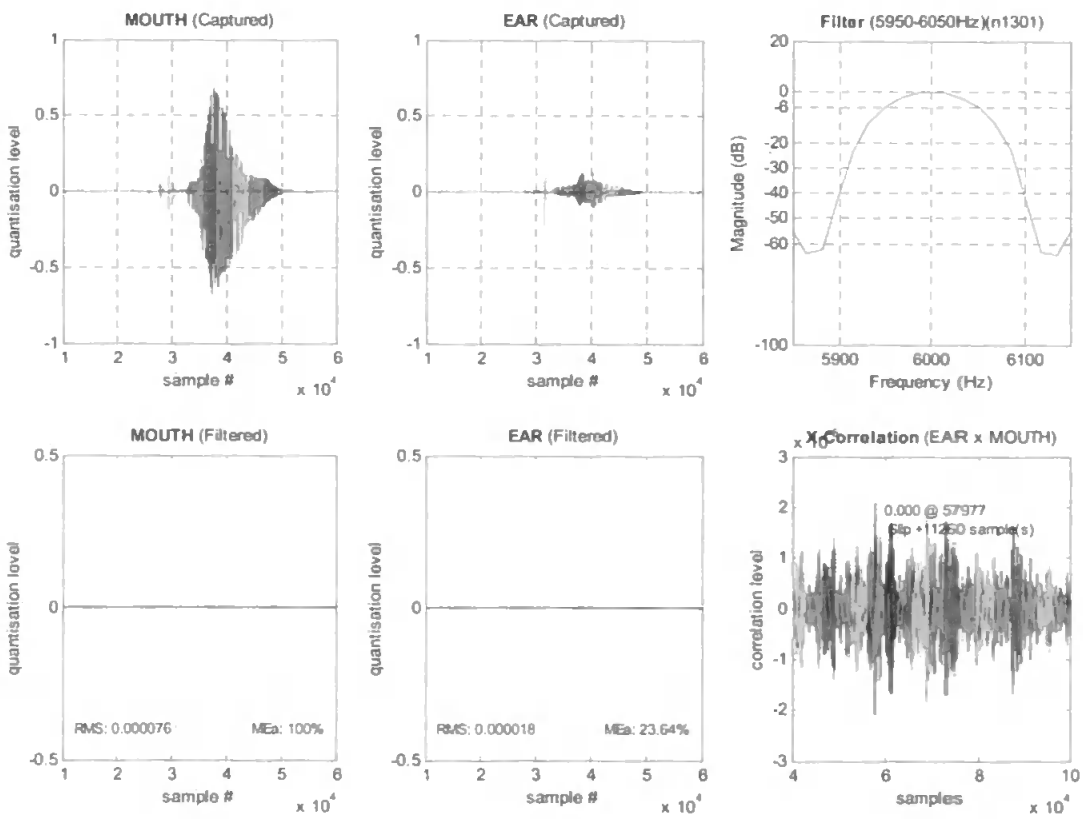


Figure 6-43 : HAT Analysis - Capture, Filter and Correlation @ **6000Hz**

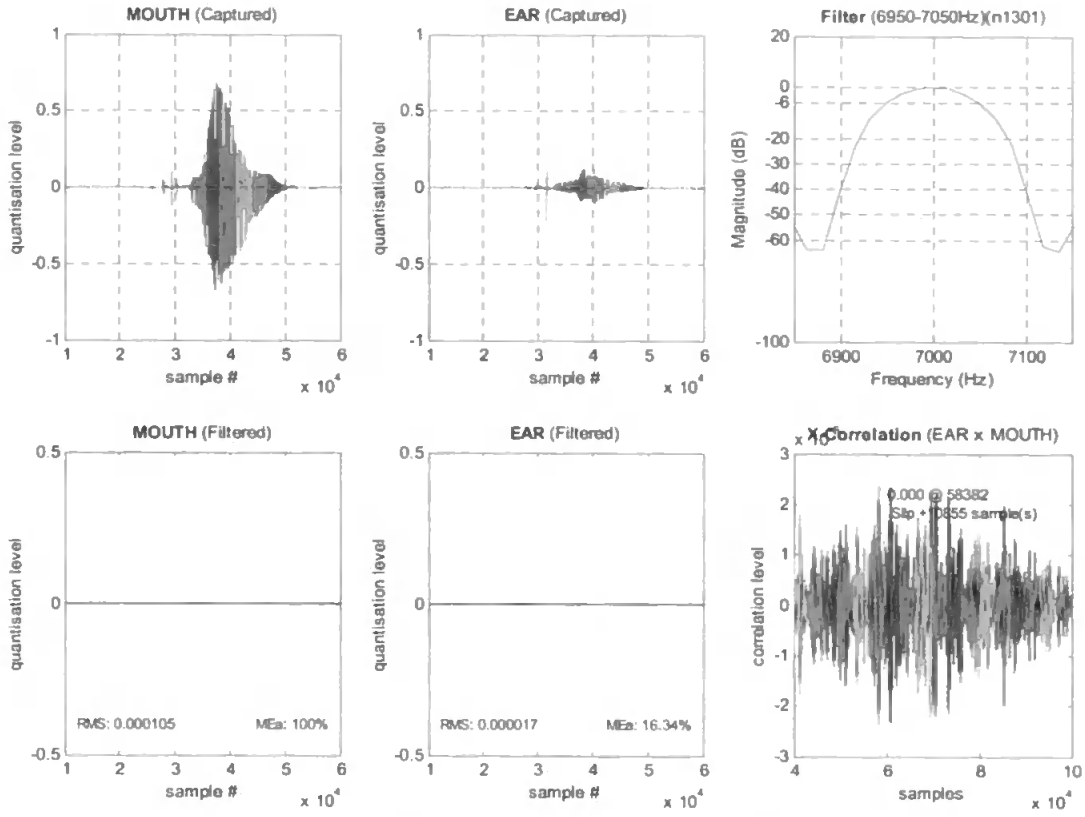


Figure 6-44 : HAT Analysis - Capture, Filter and Correlation @ **7000Hz**

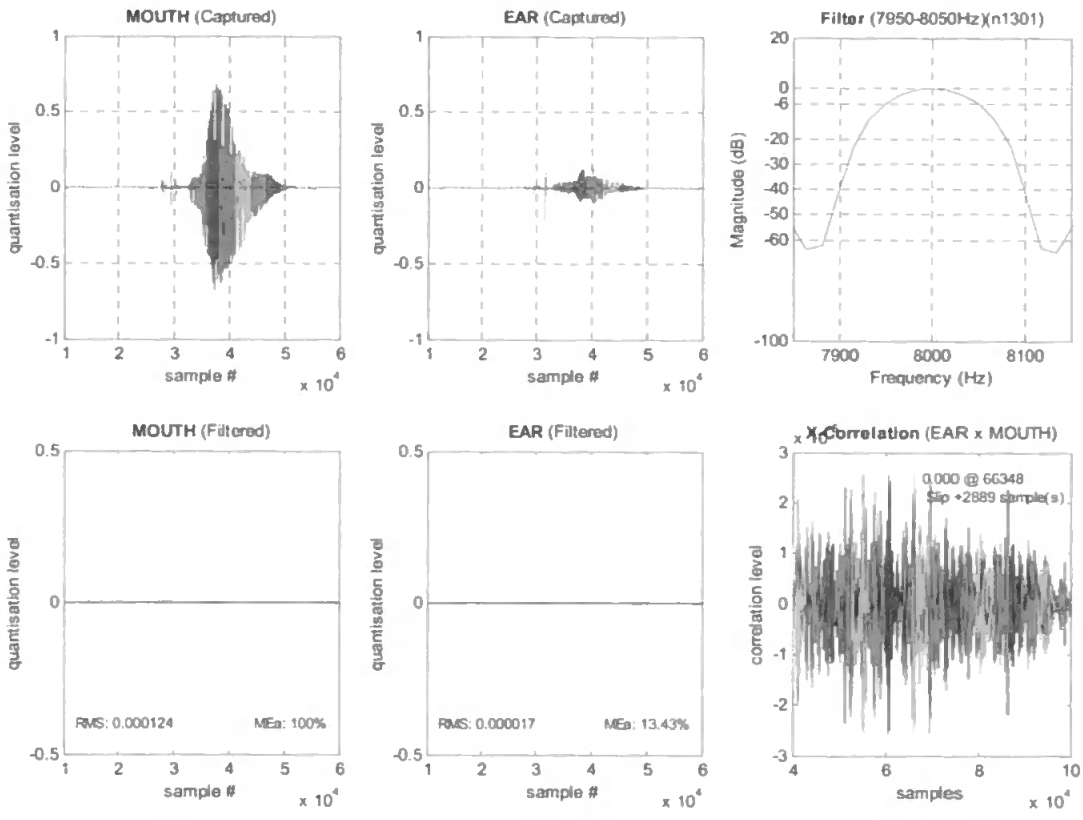


Figure 6-45 : HAT Analysis - Capture, Filter and Correlation @ **8000Hz**

6.3.2 Correlation Analysis

The correlation template is the unique shape (pattern) contained within the ear-to-mouth correlation offsets (time slippage) of an individual user, and is controlled by:

- the system spot-frequencies discussed in HAT Stage-2;
- the shape and consistency of individual user's mouth-to-ear correlation offset response, as a number in samples, at each spot-frequency.

The theory behind the approach was to utilise the principles discussed in Section 5.3.1, where the speed of propagating sound waves in matter are dependent on the frequency of the propagating waves and the fundamental properties of the medium. Combined with the unique audio spectrum of the user's voicebox, the heterogeneous bio-matter of their head (Figure 5-6) uniquely shapes spot-frequency timings as illustrated in Figure 6-46.

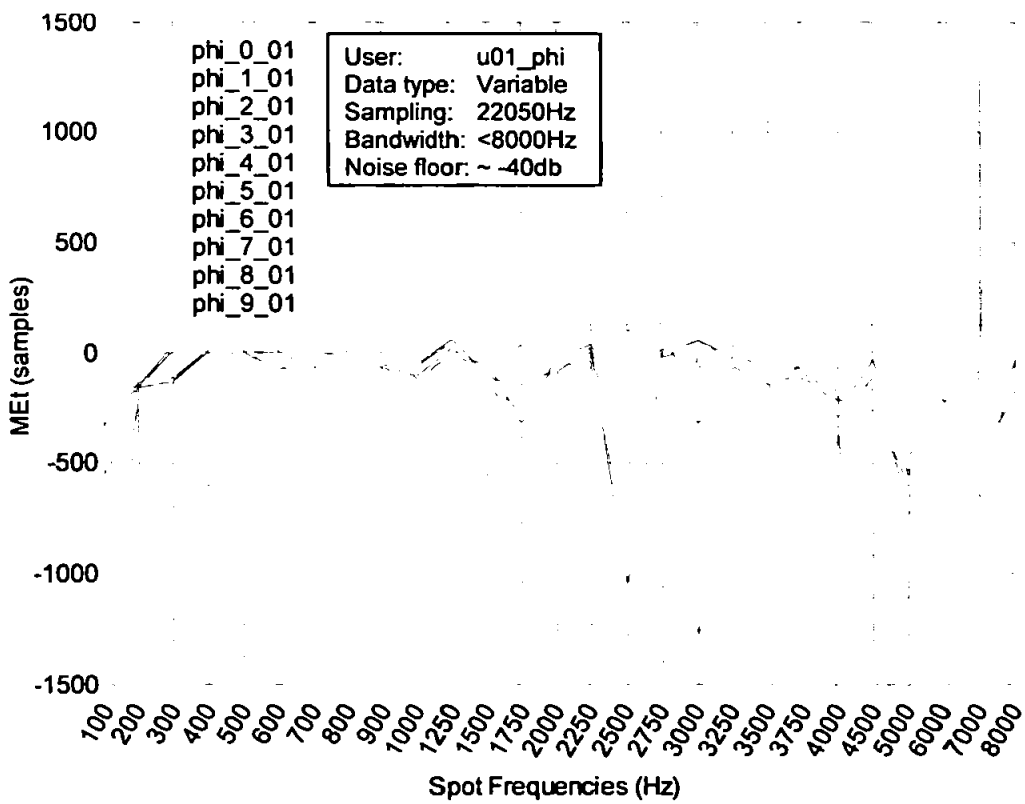


Figure 6-46: Compound timing variation curves of the numbers '0' to '9' - HAT trial user 'u01_phi' (100Hz < bw < 8000Hz)

By inspection of the plots Figure 6-46 and Figure 6-47, although there was some evidence of capture set correlation, **using the same users and numerical stimuli** as previously in Figure 6-26 and Figure 6-28, there was less evidence of unique individual user behaviour when compared to the (mouth-ear) absorption method. In addition, individual curves exhibited less consistent behaviour (compared to absorption plot curves), resulting in higher standard-deviation figures and broader statistical variance.

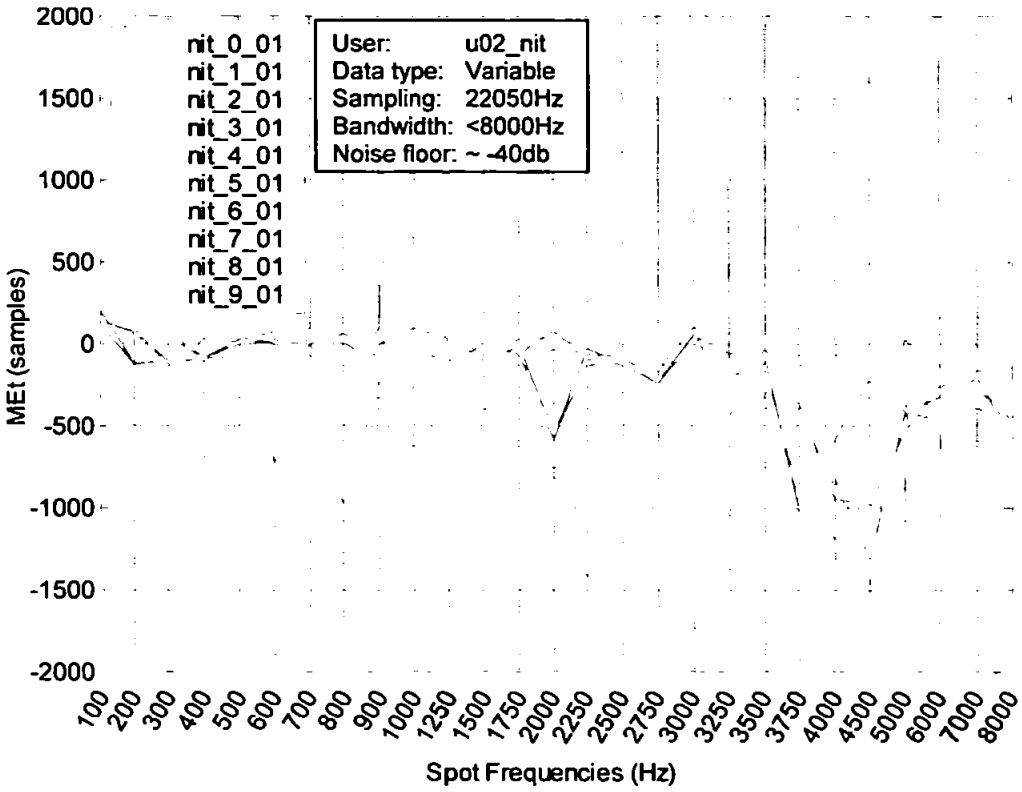


Figure 6-47: Compound timing variation curves of the numbers '0' to '9' - HAT trial user 'u02_nit' (100Hz < bw < 8000Hz)

As a consequence of the negative aspects exhibited by this approach and the more promising results of the absorption analysis approach, correlation analysis was subsequently discarded as the first choice HAT analysis technique and not pursued beyond comparative evaluation with the chosen absorption method.

HAT exclusively adopts the **absorption** analysis method, with correlation analysis not considered further within the thesis beyond a mention in Section 8.3 on future work.

6.4 Conclusion

Following on from the conceptual discussions defining the HAT development pathways, this chapter introduced and discussed in depth the methodology behind the final HAT authentication process, along with a complete systematic breakdown of the five stages that define HATs interpretation of a head authentication system:

- **Capture** of biometric audio waveform pairs from a user.
- **Filter** of audio waveform pairs at discrete spot-frequencies.
- **Absorption** comparison of discrete waveform spectra defining a HAT template.
- **Analysis** of the HAT absorption template within a neural-network.
- **Classification** of the neural-network output through threshold comparison.

The chapter identified and explained the fundamental differences between the two main biometric analyses techniques borne out of the HAT development process: the absorption technique, and the correlation technique. After discussing the advantages and disadvantages of both techniques, the better performing absorption technique was selected in preference to the correlation technique and forms one of the two novel aspects of the research, namely:

- The HAT method of biometric capture.
- The HAT absorption method of biometric analysis.

The next chapter focuses on an extended proof of concept of the HAT absorption technique through a series of trials involving a diverse group of volunteers: to enable the trials, a HAT demonstration tool was conceived and developed. Along with a description and walkthrough of the HAT demonstration tool, the HAT trials results are presented and discussed in detail.

Chapter 7

Evaluation of the Head Authentication Technique

7 Evaluation of the Head Authentication Technique

As there is no precedent for the novel head authentication ideas introduced in Chapter 5 or the resultant HAT authentication methodology presented in Chapter 6, it is an essential part of the research to demonstrate proof of concept. This chapter presents an extended proof of concept of the Head Authentication Technique through use of a HAT demonstration tool, enabling a set of controlled trials.

The chapter is divided into two sections: an introduction and overview of the custom designed HAT demonstration tool and its usage; and an outline of the HAT field trials utilising the demonstration tool, involving a discussion on the field trial results. The chapter concludes by introducing the research conclusions on the HAT authentication process, which are discussed in depth in Chapter 8.

7.1 Introduction

In order to prove the Head Authentication Technique outside of its artificially controlled and ideal research environment, a robust HAT demonstration tool was developed to enable a set of field trials for the technique. The HAT demonstration tool was in fact an evolution of an experimental research platform originally conceived to test the viability of a number of original ideas, many of which did not make it beyond conception. Once the fundamental principles of head authentication were established (Section 5.3), two variations on the basic technique emerged that showed consistent promise throughout initial testing, these were the absorption method, discussed in Sections 6.2, and the correlation method, discussed in Section 6.3. These two HAT Stage-3 Analysis methods

were developed in parallel for the majority of the research, and a preferred method only selected in the final stages of the demonstration tool development[1]. The single method eventually selected for the HAT demonstration tool was the absorption method, which was not only providing more consistent results, but also proving easier to process within evolving software analysis tools.

By the time the HAT trials were performed, the demonstration tool had developed far beyond a highly specialised experimental research platform requiring intimate knowledge of the research, into a user friendly tool incorporating an audio headset managed by a generically styled Microsoft Windows application (Section 7.2.2.2). The HAT demonstration tool requires no specialised knowledge of the PhD research, and only minimal understanding of the authentication methodology and processing performed by the tool; in fact, the tool includes a simple wizard to guide users through the registration and authentication processes.

The HAT trials were performed over two sessions, separated by a period of at least 24 hours, in an attempt to acknowledge some aging of the biometric templates. Twenty trial volunteers were selected to represent a diversity of:

- **sex**: in Chapter 5 Figure 5-12 it is illustrated how the male and female vocal ranges can differ by up to 100Hz;
- **age**: (ranging from 24 to 64 years), in Chapter 5 Figure 5-1 it is illustrated how the human auditory range varies with age;
- **nationality**: to demonstrate that the HAT process is language independent, utilising variations in sound, not comprehension, for its biometric markers.

[1] Although combining the absorption and time-slip methods was considered, further experimentation into multimodal biometrics was considered beyond the scope of the project; see future work in Section 8.3.

7.2 The HAT Demonstration Tool

The HAT demonstration tool is a non-intrusive authentication platform developed to demonstrate and evaluate the principles of the Head Authentication Technique. The tool combines a specially configured hardware headset, henceforth called the **HAT Headset**, with a proprietary Microsoft Windows software application, henceforth the **HAT Application.** The tool was developed out of an experimental test-bed for the many head authentication ideas proposed at the beginning of the research and discussed in Chapter 5. The tool was later modified for general use in a series of HAT trials.

7.2.1 The HAT Headset

An integral part of the HAT demonstration tool is the custom designed headset which collects the audio waveform sample pairs for processing by the software element of the tool. Although similar in appearance to a standard lightweight computer headset, critically the HAT headset replaces the ear transducer with a suitable high quality lavalier[1] microphone, as shown in Figure 7-1.

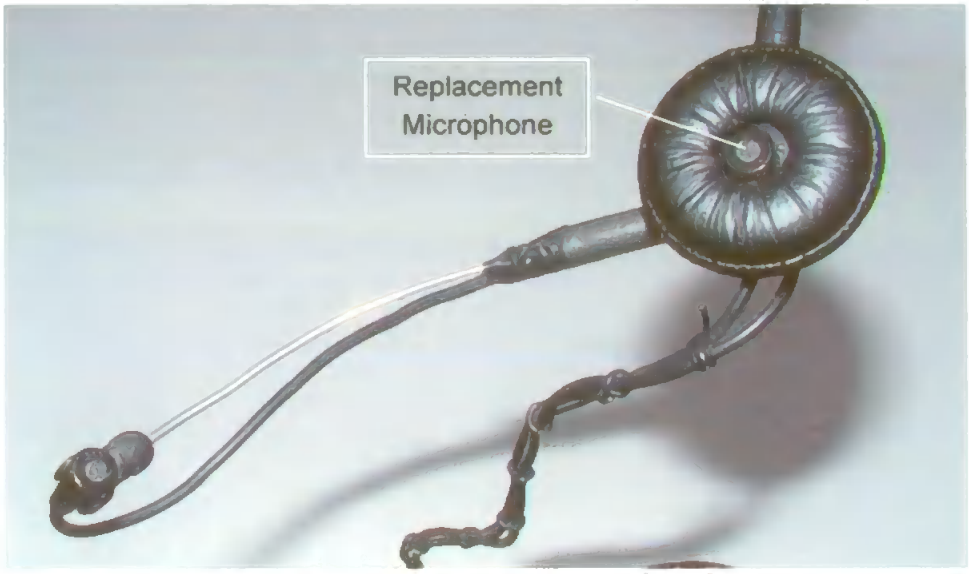


Figure 7-1 : The replacement ear microphone of the HAT Headset

[1] A lavalier (tie-clip) microphone was selected for its compact size and optimised voice characteristics.

As a HAT authentication template is dependent upon the calculated variance between mouth- and ear-captured waveforms (basic HAT), it was also decided to replace the mouth microphone with a matching high quality voice microphone to ensure that the hardware itself did not contribute any variance of its own into the HAT template.

The HAT headset replacement microphones were high quality electret[1] lavalier microphones (Figure 7-2), selected for their:

- excellent frequency response; covering the full vocal range;
- high sensitivity; for use with the low amplitude ear waveform;
- diminutive size; for use in a headset without adding additional bulk or weight.

Figure 7-2 : A HAT headset high-quality electret lavalier microphone

The technical specifications of the HAT lavalier microphones are shown in Table 7-1.

Type:	Electret
Polar response:	Omni
Frequency response:	50 to 16KHz
Impedance:	600 ohms
Sensitivity:	-64dB
Lead/plug:	6m/6.35mm jack[2]

Table 7-1 : Technical specifications of the HAT headset microphones

[1] Electret microphones are an FET driven variation on the classic condenser microphone.
[2] The microphone is powered by an LR44 power cell contained within the jack-plug.

As the replacement lavalier microphones of the HAT headset are not *standard* computer peripherals, they do not naturally interface with a typical computer setup. Combining this issue with need for good quality amplification to match the performance of the microphones, a small booster amplifier was purchased which could interface directly with the line input of a computer soundcard[1], illustrated in Figure 7-3.

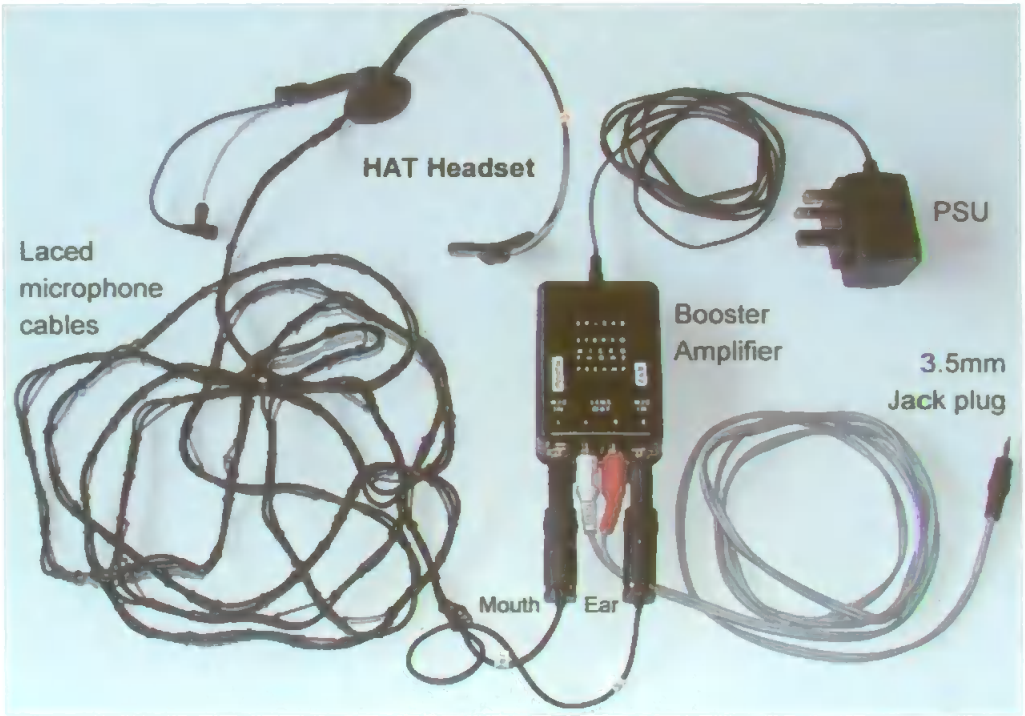


Figure 7-3 : The hardware composing the HAT Headset

Although the HAT headset uses identical microphones for the capture of both the mouth and ear waveforms, the operational principles behind microphones and transducers are not fundamentally different and it is not inconceivable to imagine a development of the headset using a suitably modified ear transducer for capture of the ear wave, enabling the ear-piece to also remain active as a speaker. Although this would introduce a variation in the resultant mouth to ear hardware responses, and timing of authentication cycles would depend on fast switching of the ear transducer from transmit to receive at appropriate intervals, both of these issues could be compensated for in software.

[1] The HAT development PC utilised a high quality Creative SoundBlaster Audigy-2 soundcard.

7.2.2 The HAT Application

The HAT Application is the software element of the HAT Demonstration Tool. It is a Microsoft Windows application developed initially as part of an experimental research platform to explore the potential of the various approaches to head authentication discussed in Chapter 5, and later modified as a part of the HAT demonstration tool to manage the registration and authentication of users in a HAT based authentication system.

The HAT Application is an evolution of a number of individual HAT developmental software tools discussed in Section 7.2.2.1. It has the ability to demonstrate empirically all of the stages of the HAT process, either discretely or in sequence as part of a full HAT processing cycle. Underneath the user friendly graphical interface optimised for use in the HAT trials, discussed in Section 7.3, is a powerful HAT research tool capable of displaying graphical outputs of each individual stage of the HAT process.

7.2.2.1 Foundations of the HAT Application

It was realised early on in the research that although the majority of the analytical work could be modelled within established research tools such as Mathsoft Matlab, all of the head authentication concepts under investigation required similar biometric capture procedures. To establish a common capture procedure and automate the capture process, a software tool was developed to interface with the HAT Headset, efficiently capturing and storing multiple biometric samples from volunteers; this first tool was called a 'Collector'. In common with all subsequent HAT software developments, the first Collector was developed in Microsoft Visual Basic owing to the programming languages speed of development. An example of an early software collector was termed the 'Correlation Authentication Rig' (CoAuR): a view of this applications main operational window (v.C10) is shown in Figure 7-4.

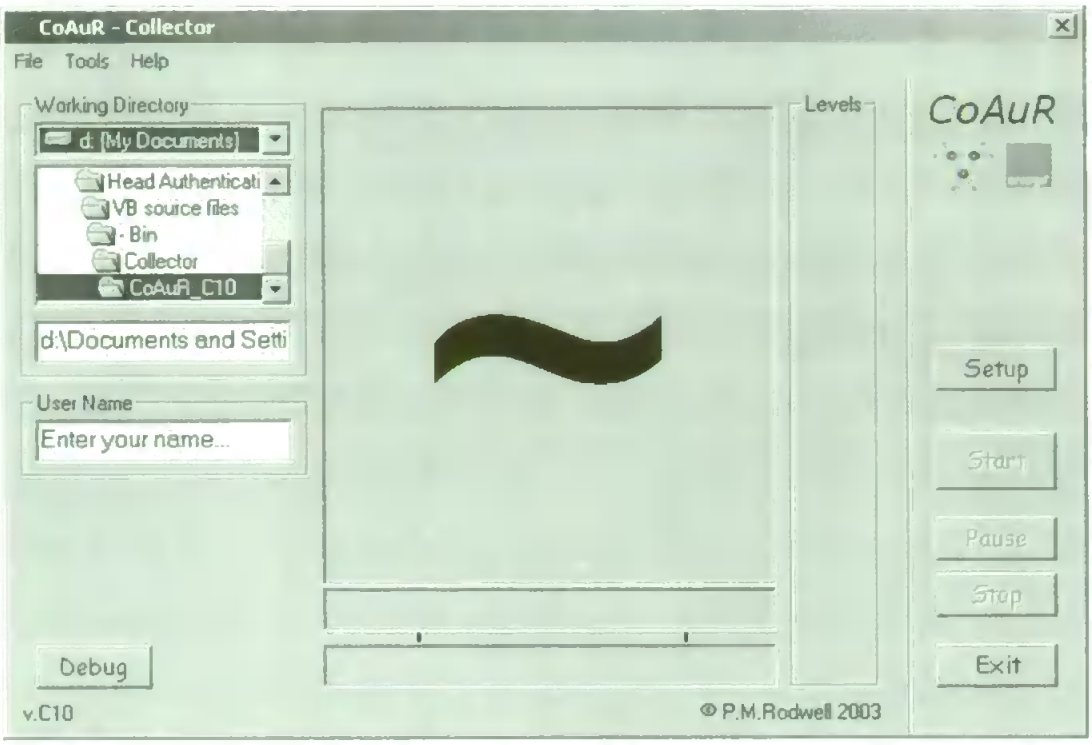


Figure 7-4 : Correlation Authentication Rig - Collector

As the basic head authentication principles were established (Section 6.1), and the two chosen analytical methodologies (absorption and correlation) emerged, a further software tool was developed to link with Matlab and automate many of the time consuming steps of the analysis process; this tool was called an 'Analyser'. Although Microsoft Visual C was considered for development of the Analyser due its improved execution speed (compared to Visual Basic), this advantage was unrealisable as the complex analytical HAT Stages were retained within Mathsoft Matlab.

The matching CoAuR analyser (v.A8) for use with the Collector in the previous example is shown in Figure 7-5. By inspection of the Analyser interface, note that:

- the analyser example is a correlation (time-slippage) analyser (Section 6.3);
- the sampling rate is 44100Hz, later refined to 11025Hz (Section 6.2.6);
- ear-waveform normalisation is active and set to 95% (Section 6.3.1.1);
- the experimental bandpass filter being applied to spot-frequencies (Section 6.2.1.3).

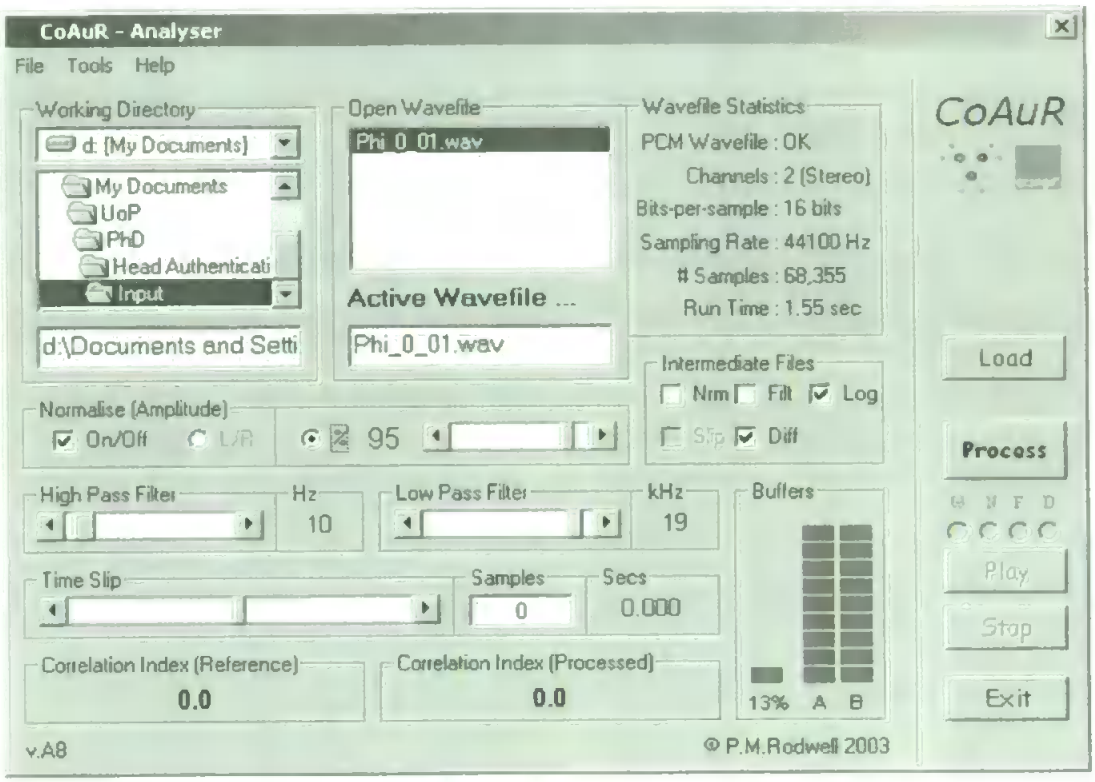


Figure 7-5 : Correlation Authentication Rig - Analyser

As the research progressed and refined the chosen head authentication technique into what became known as the HAT process, the software tool(s) were developed in parallel, eventually being merged into a single application, the HAT Application, an example of which (v.C13.5) is shown in Figure 7-6.

By inspection of this revised layout, it can be seen that the tool now includes both the collector (renamed 'Train') and the analyser (renamed 'Identify') functionality of the previous tools. Later development of the HAT Application focused on optimising the GUI for minimal technical impact in preparation for the HAT trials (Section 7.3); removing discrete buttons to a toolbar and internal adjustments to menu triggered child-frames.

By comparing these developmental examples (CoAuR Collector in Figure 7-4; CoAuR Analyser in Figure 7-5; HAT Application in Figure 7-6) with the HAT Application window in Figure 7-7, the provenance of the HAT Application is clearly demonstrated.

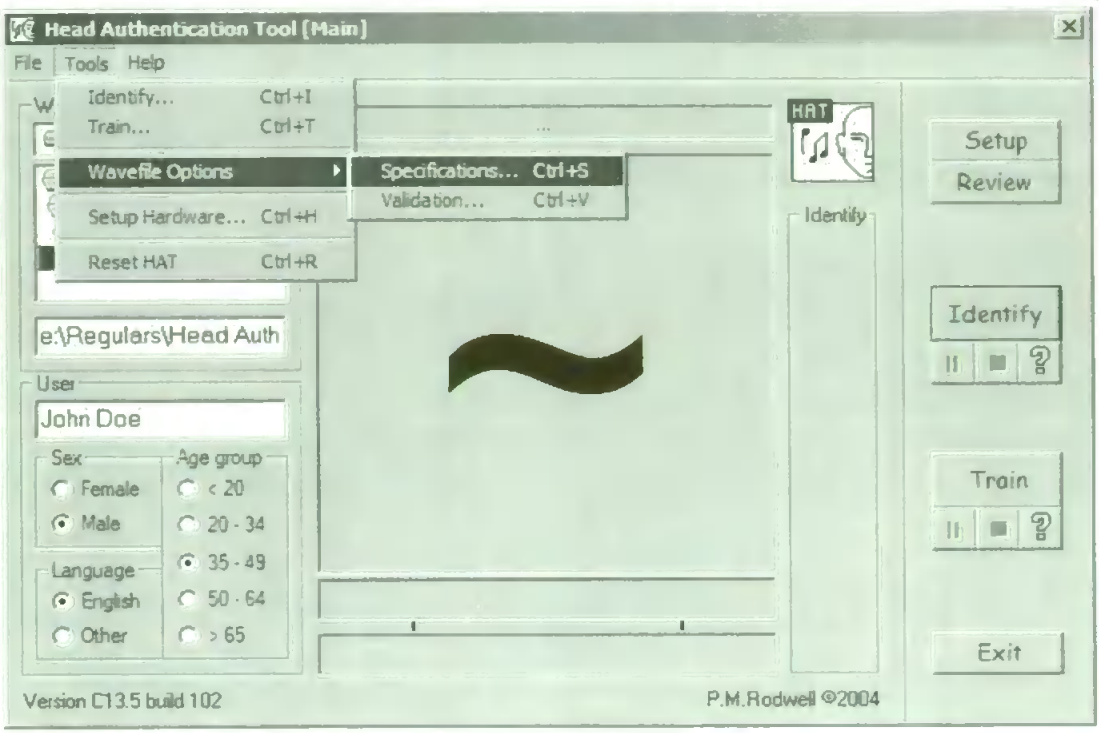


Figure 7-6 : Early example of the HAT Application

7.2.2.2 Navigating the HAT Application Interface

For the novice user, the HAT Application essentially performs two functions:

- **Registration** of new users (Section 7.2.2.3).

  Registration involves Capture, Analysis and training of a *new* neural-network to add the to the system user base.

- **Authentication** of existing users (Section 7.2.2.4).

  Authentication involves Capture, Analysis and processing within an *existing* neural-network in order to verify the claimed identity of the current user.

The annotated HAT Application window is shown in Figure 7-7, during a HAT Stage-1 Capture cycle. In addition to the fairly self explanatory layout, the application interface adopts familiar Microsoft Windows conventions through use of menus, toolbars, progress-bars etc., taking advantage of user's established learnt behaviour from other Windows applications.

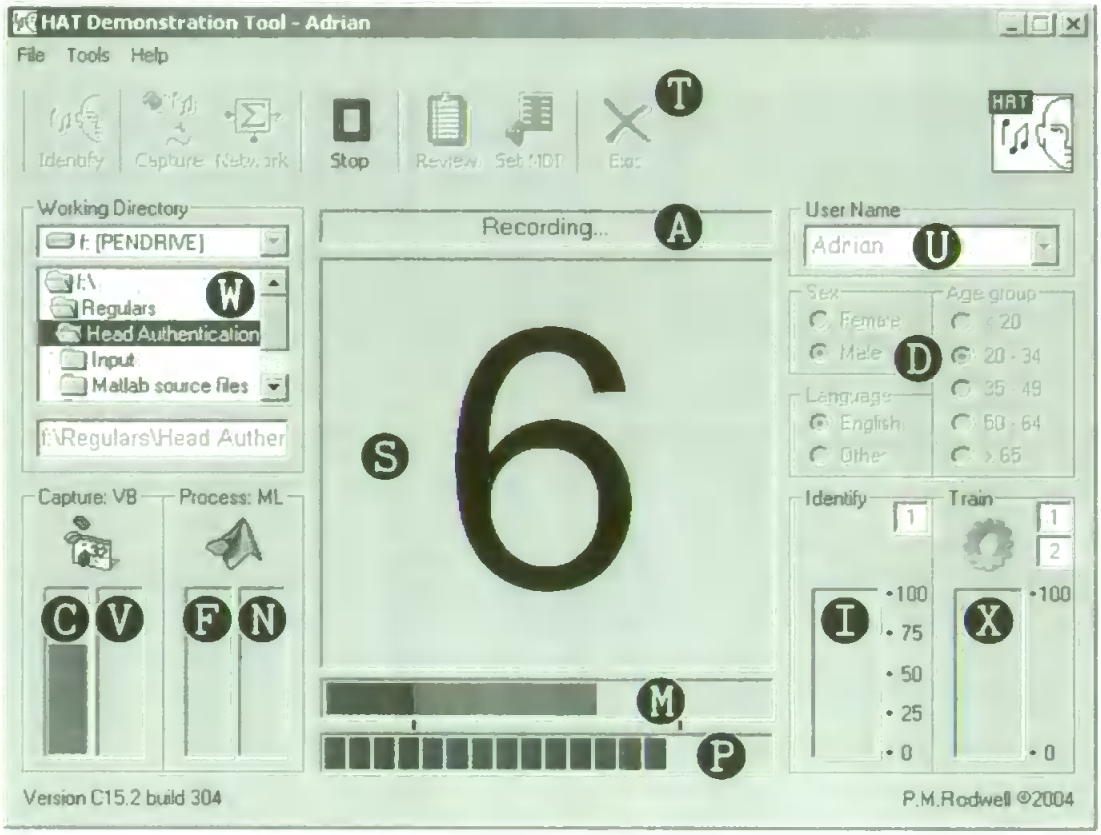


Figure 7-7 : The HAT Application main interface during a HAT Capture cycle

T The live[1] main window toolbar provides easy access to all of HATs primary functions, without the need to enter the tools menus; illustrated below.

- **Identify**: Authenticate the current user.
- **Capture**: Register a new user.
- **Network**: Build a new neural-network (automatic as part of Capture)
- **Stop**: Stop the current process.
- **Review**: Review ALL of the HAT Application settings in one screen.
- **Set MDI**: Adjust the capture hardware settings (PC soundcard).
- **Exit**: Exit the HAT Application.

[1] The availability of individual HAT toolbar elements is dynamically controlled by the active process.

- **W** The path to the HAT working directory containing the HAT Application executable and additional HAT resources: HAT.ini etc.
- **A** The HAT activity indicator constantly reports the operational state of the tool.
- **U** A user can either manually enter a new user name for registration, or conveniently select their name from the static pull down list of included HAT trial participants.
- **D** A small selection of the active user's demographic data; also saved as 'user_id.txt' for each user. The 'language' option is the captured language not the user nationality.
- **S** The tools central display window is used to prompt the user with example text to speak during a capture cycle, or random text during an authentication cycle.
- **C** The HAT capture progress-bar (green) indicates the progress of a HAT Stage-1 Capture (Section 6.2.1), working in tandem with the timing-bar **M**.
- **V** The HAT waveform validation progress-bar (yellow) indicates the progress of the amplitude validation cycle performed on each new waveform.
- **F** The HAT filter progress-bar (light-blue) indicates the timing of the HAT Stage-2 Filter (Section 6.2.1.3), HAT Stage-3 Absorption (Section 6.2.3) processing loop.
- **N** The HAT analysis progress-bar (dark blue) indicates the progress of the HAT Stage-4 Analysis (Section 6.2.4) using the HAT neural-network (Section 6.2.4.1).
- **M** The timing-bar is used to prompt the user when to speak during Capture or Identify cycles: 'green' indicates when to speak and 'red' when to wait.
- **P** The current operation progress-bar indicates the progress of the complete active operation: for example, the five stages of an authentication cycle (Section 6.2).
- **I** The identity confidence-bar is used to indicate HATs confidence in the claimed identity of the active user in four steps: 0, 25%, 50, 75% & 100%. Each step increment indicates either a passed or failed authentication cycle.
- **X** The auxiliary progress-bar is used to indicate the progress of *en-mass* operations; for example, HAT Stage-4 Analysis of ALL the HAT trial participants

In addition to the visual improvements to the application interface, all of the applications important internal settings can be adjusted through use of the extensive tabbed Options screens accessed via the Tools menu. The four primary settings tabs are shown in Figure 7-8 (a complete list is shown in the HAT manual in Appendix F) and cover:

- **Wavefile format**: Channels, Sampling rate and bps (Section 6.2.1.2).
- **Wavefile validation**: Minimum and maximum capture amplitudes and tolerance.
- **Spectral analysis**: Spot-frequency, filter coefficients, bandwidth (Section 6.2.2.1).
- **Neural-network**: Default analysis set, target error rate, epochs (Section 6.2.4.1).

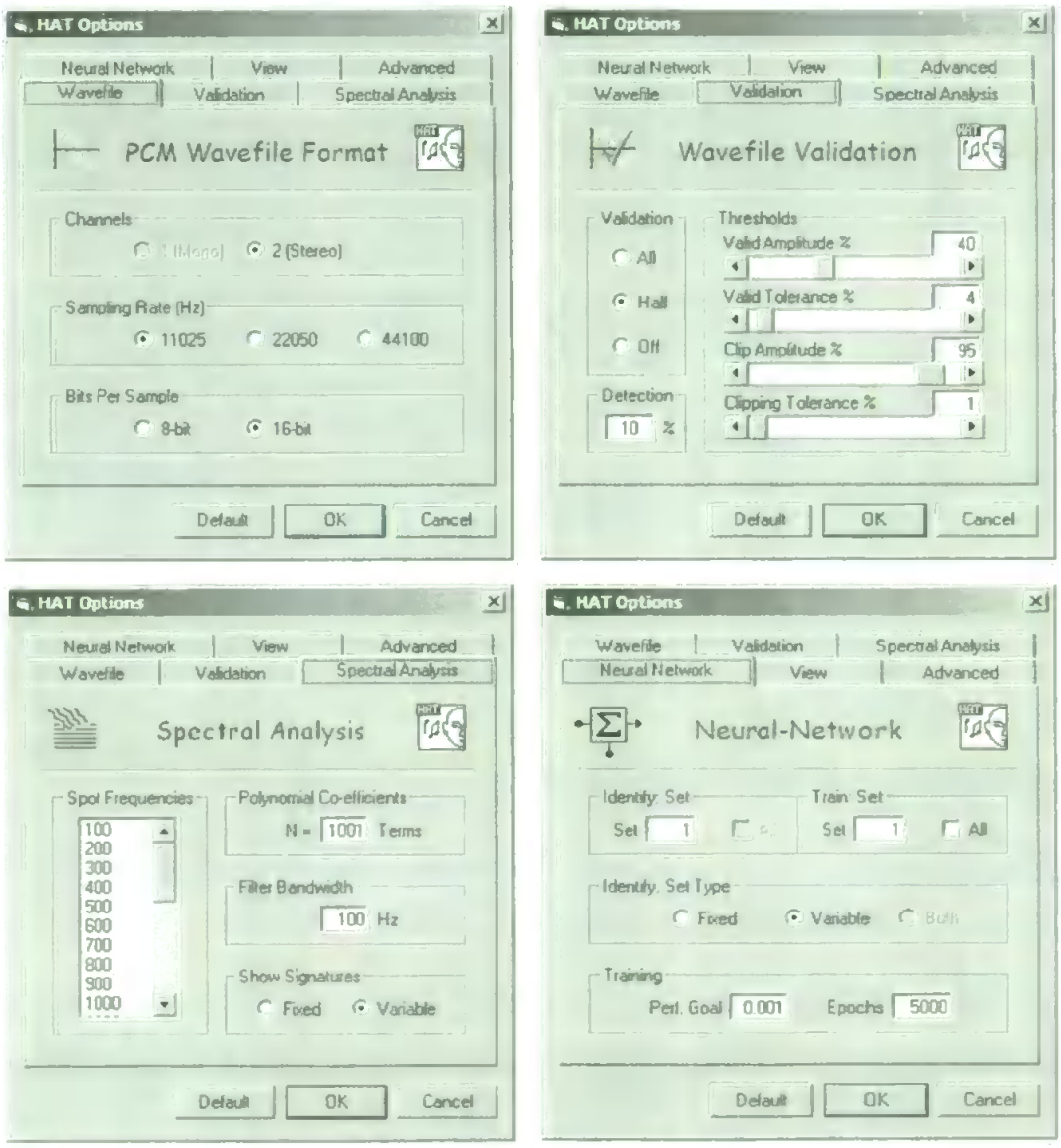


Figure 7-8 : HAT Application tabbed options frames

A complete set of help screens is also available within the HAT Application via the Help menu (see the example in Figure 7-9), covering the most important aspects of the HAT process, including full step-by-step instructions on the usage of the HAT Application during each stage of the registration or authentication process.

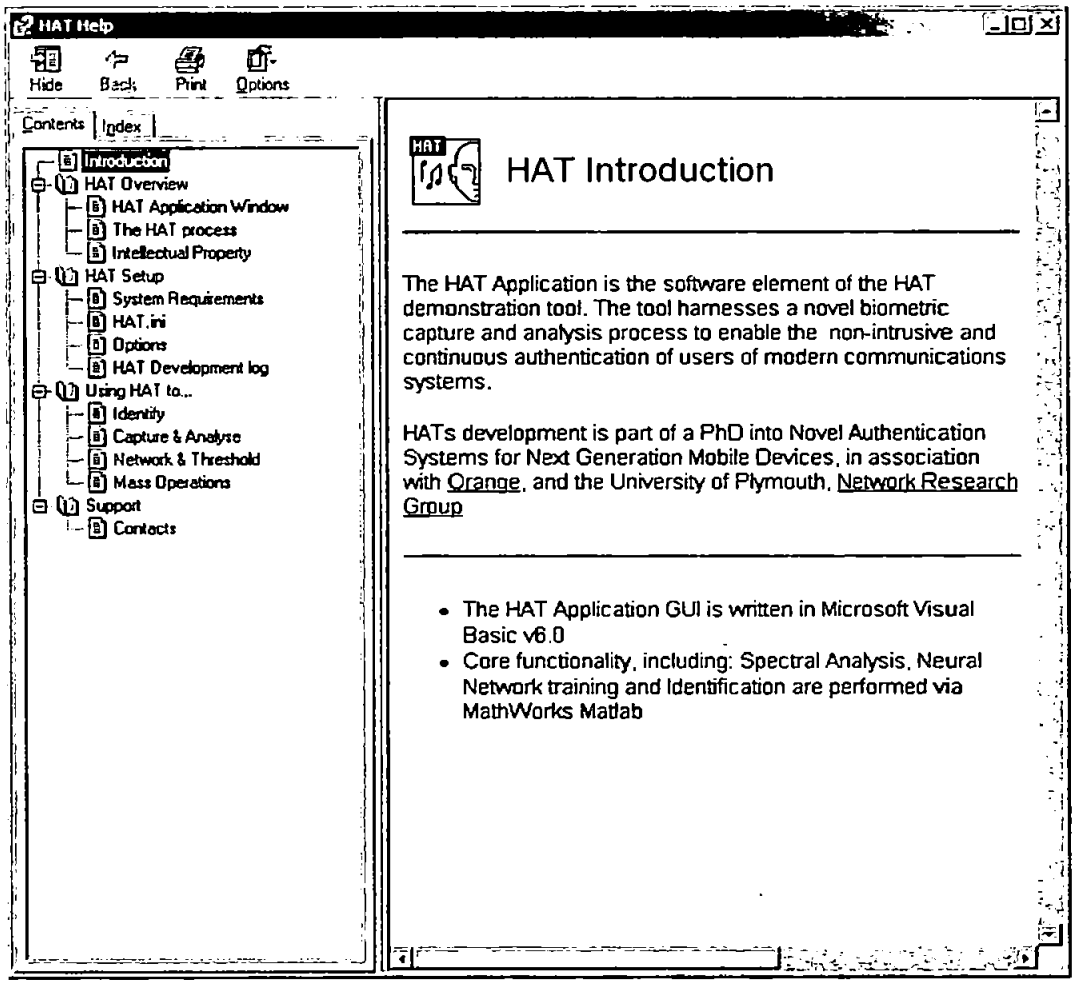


Figure 7-9 : HAT Help menu example – HAT Introduction

The HAT Application includes various resources files, designed to minimise the need for recompiling the source code every time settings are changed. The options include:

- **HAT.ini**: Primary HAT start-up settings (see Appendix F).
- **HAT_Spoken.txt**: Textual prompts for HAT Stage-1 Capture cycle.
- **HAT_CnFq.txt**: Pre-selected filter spot-frequencies (Section 6.2.1.3).
- **Users.txt**: HAT Trial participant's names (see Section 7.3).

7.2.2.3 Registering a New User

In order to be authenticated by the HAT demonstration tool, a user must first register with the system. The registration process involves capturing a selection of phonetically diverse sounds which, for user convenience, are selected from the familiar set of alphanumeric characters[1]. The HAT Application then performs the HAT process (Section 6.2) to realise the user's unique biometric template and neural-network map.

What follows is an explanation of the HAT Application registration process for use by a new user, with reference to the application window in Figure 7-7:

Step 1: Set the HAT Path

Open the HAT Application and select the main HAT directory, containing the HAT executable and resources, in the drive selection window Ⓦ.

Step 2: Select the Capture Mode

Enter the Tools>Capture Mode menu and select the type of capture mode required; the default setting is 'Capture and Analyse'. The default setting is also conveniently available via the shortcut CTRL+K, prompting 'Capture Mode - FULL' in the activity bar Ⓐ.

Step 3: Identify a New User

To identify a new user to the system, enter a username within the field Ⓤ and complete the user demography section Ⓓ. If a user is recognised by the system their *new* capture data is augmented with their previous data to strengthen the existing user profile. If a user is not recognised by the system a new account is setup (a new 'Output' directory created).

[1] Although HAT prompts users for alphanumeric characters during registration, recall that the HAT process is not dependent on 'what is said', but 'how it is said' and 'how it is affected' by the head.

Step 4: Review Settings (Optional)

Select the Review icon in the HAT Application toolbar and conveniently review the complete applications settings.

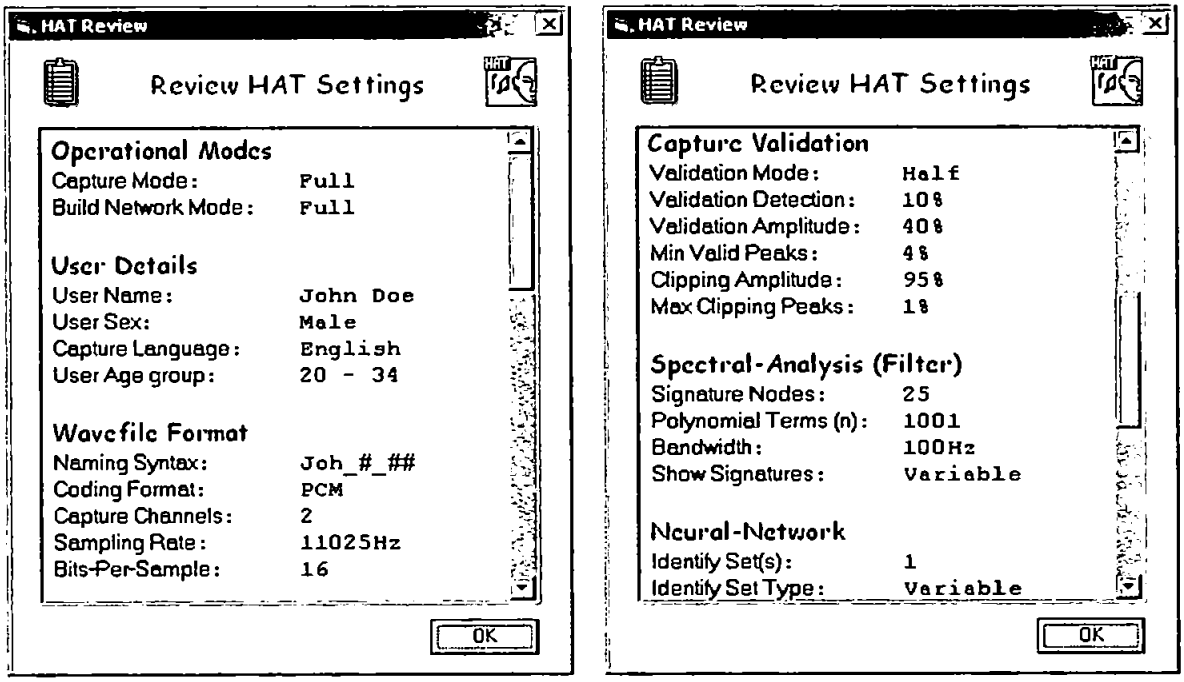


Figure 7-10 : HAT Application settings review frame (two views)

Step 4: Try a Simulation (Optional)

It is recommended that new users try the user simulation within the Help>Simulation menu option. The process will help familiarise a new user with the HAT capture process, minimising bodily tension due to psychological apprehension during a genuine capture cycle. The simulation precisely mimics a genuine capture cycle, responding appropriately to the relevant settings within the options screens.

Step 5a: Check the HAT Headset Hardware

Check that the HAT headset hardware is correctly connected (Figure 7-3) and that there are two good power cells[1] in the microphones jack-plugs.

[1] Each microphone jack-plug requires a single LR44 power cell.

Step5b: Position the HAT Headset

Position the HAT Headset comfortably on the head ensuring that the ear microphone is positioned centrally over the pinna of the outer ear (Figure 5-2), in line with the ear canal, and with the mouth microphone positioned vertically central and horizontally offset from the centre of the mouth, to minimise breathing pickup.

Step 6: Capture

Press the 'Capture' button  on the HAT toolbar ❶ and follow the comprehensive onscreen instructions: the HAT Application will prompt the user to speak up to twenty pseudo-random alphanumeric characters. Having performed a simulation (Step 4) the process should be familiar to the user, minimising any unnecessary body or voice tension.

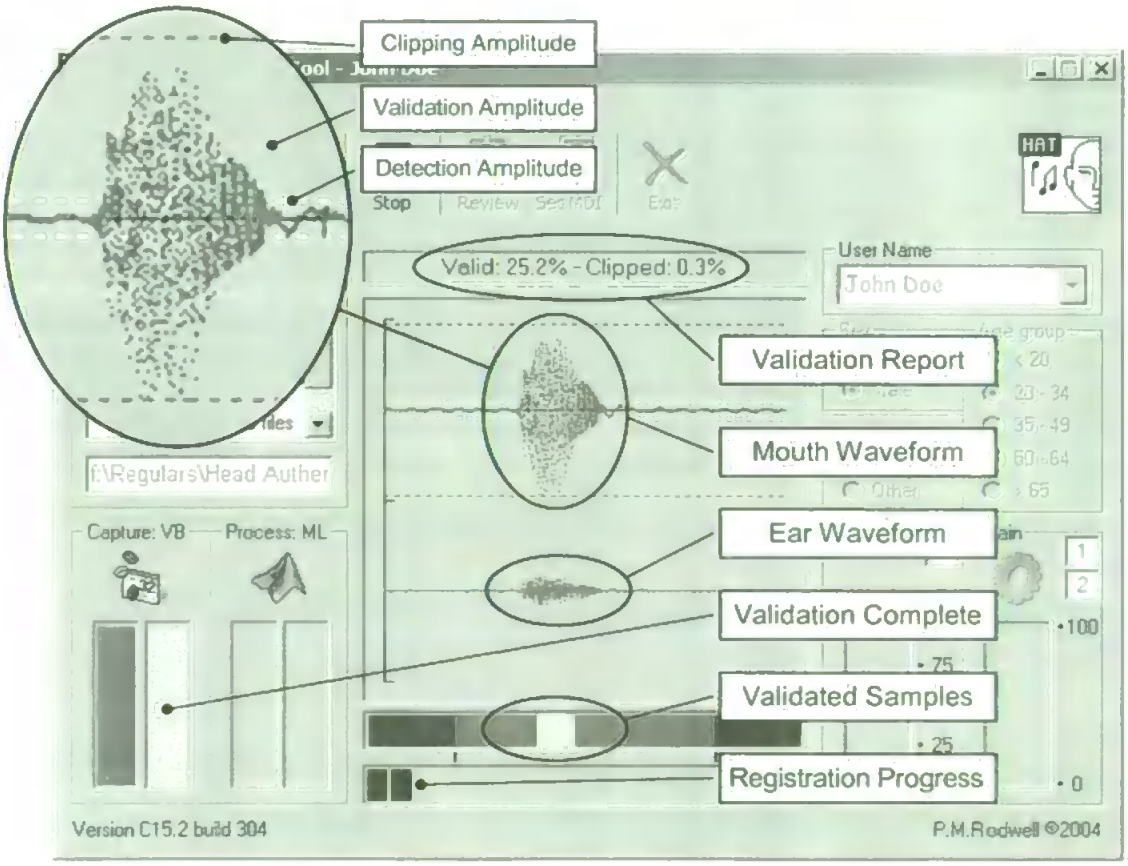


Figure 7-11 : HAT Application - Stage-1 Capture and validation plot

After each individual capture, the application will validate the samples according to the settings in the validation options tab (Figure 7-8) to guarantee their suitability for use by the HAT Application before entering the time-consuming HAT analysis stages. This is also a useful feedback mechanism, indicating to the (new) user 'when' and 'how loud' to speak for optimum tool performance. Upon completion of the waveform validation cycle the application presents the user with a graphical output similar to the one shown in Figure 7-11. By inspection of the figure, it can be seen that for the example shown:

- All of the spoken samples exceed the detection value (see the breakout box).
- 25.2% of the samples are validated within tolerance (the requirement was 4%).
- 0.3% of the samples experienced clipped (the requirement was <1%).

Upon completion of the HAT Stage-1 Capture process, the tool will automatically enter the HAT Stage-2 Filter (Section 6.2.2), HAT Stage-3 Absorption (Section 6.2.3) processing loop F, and calculate the unique HAT absorption template for the data set.

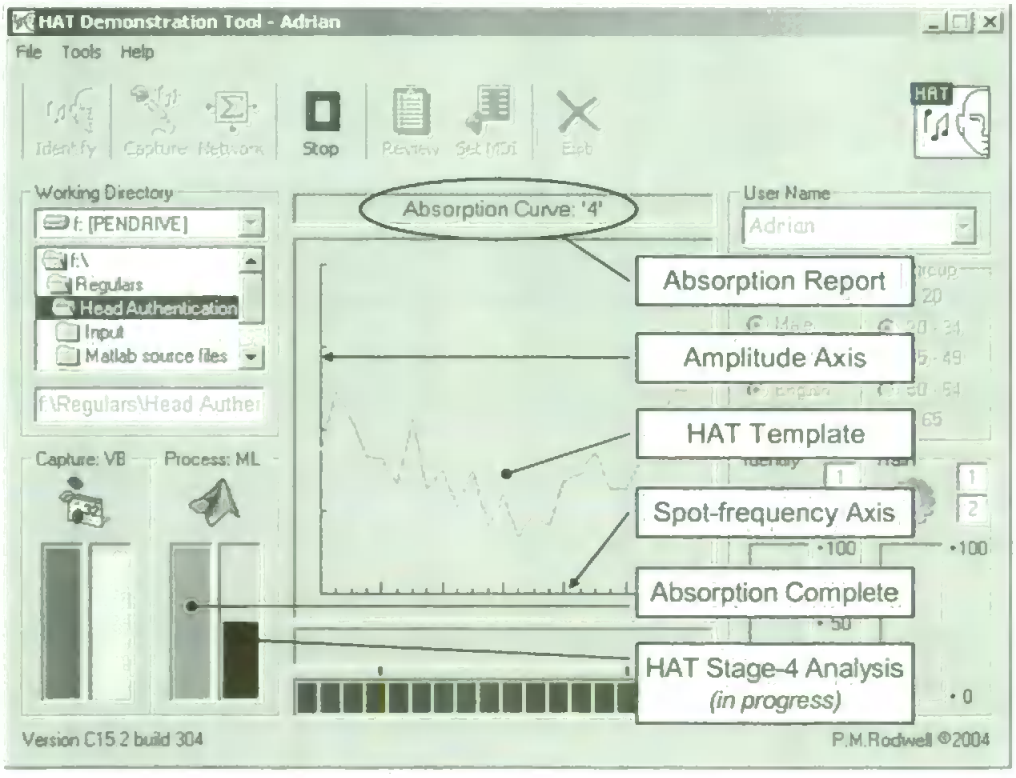


Figure 7-12 : HAT Application - Stage-3 Absorption plot of a user's waveform pair

The HAT absorption template is then briefly displayed within the HAT Application main window[1], as illustrated in Figure 7-12[2]. The HAT template visual was not designed for analytical purposes but solely as a useful real time indicator, for the user, that the capture and analysis hardware and software are functioning correctly (up to and including HAT Stage-3).

The HAT Application will then enter Stage-4 Analysis mode Ⓝ and feed the biometric absorption spectrum matrix into the HAT neural-network (Section 6.2.4.1), along with all of the other registered system users' templates: the new user is identified to the network as 'Good' and everyone else is identified as 'Bad'.[3]

Finally the new user neural-network map will be used along with additional user data sets[4] to determine the network owner's authentication threshold for use in Section 7.2.2.4. In an ideal scenario the authentication threshold of the neural-network would be '1' (one), whereby the network owner always realises a perfect template match and impostors always producing '0' (zero). The reality is somewhat different however. Recall the previous discussion on biometric markers in Section 4.2.2 'Factors Affecting Biometric Systems' and in order to minimise the FMR and FNMR (Section 4.2.3), the authentication threshold will actually exist somewhere in the range: 0 < Threshold 1.

The HAT registration process takes approximately 3 minutes for the capture and another 5 minutes for the analysis (within a user base of twenty users).

[1] The visibility of the HAT template display can be set within the HAT options 'View' tab.
[2] The displayed HAT template is for illustration purposes only: each HAT template is actually unique.
[3] HAT Stage-4 Analysis is ported to Matlab, acknowledged by the inclusion of the Matlab icon.
[4] The HAT demonstration tool requires a minimum of two data sets (or capture runs) for authentication.

7.2.2.4 Authenticating an Existing User

Once a user has been registered with the demonstration tool it is possible for HAT to provide a means of continuous identity verification for that user in the future.

What follows is an explanation of the HAT Application authentication process for use by a registered user, with reference to the application window in Figure 7-7:

Step 1: Set the HAT Path

Open the HAT Application and select the working directory, containing the application executable and resources, in the drive selection window W.

Step 2: Identify Yourself

The HAT demonstration tool currently operates as an authentication system (Section 4.2.4), in contrast to an identification system. The user must therefore first provide a claimed identity for the demonstration tool to verify. Identifying oneself to the HAT Application is a straightforward case of entering the same username as was originally used for registration, within the field U and completing the user demography section D.

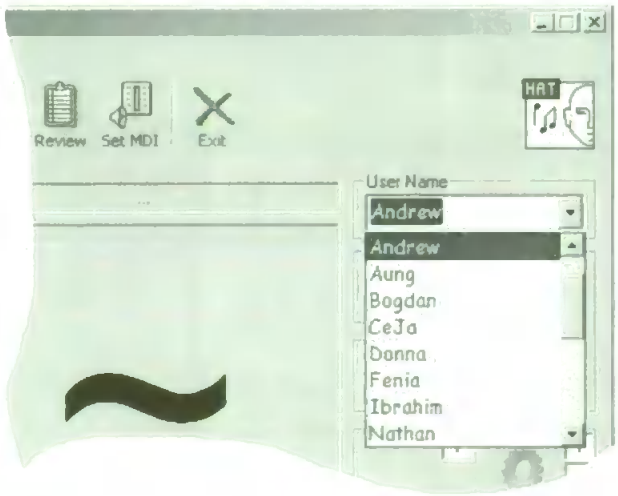


Figure 7-13 : HAT Application - Registered HAT trial user's pull-down list

If the registered user was part of the trials to be discussed in Section 7.3, then their name will already be contained within the convenient pull down list contained under the down-arrow in the username field Ⓤ, illustrated in Figure 7-13.

Step 3: Review Settings (Optional)

Select the Review icon in the HAT Application toolbar Ⓣ and conveniently review the complete applications settings as illustrated in the example in Figure 7-10.

Step 4: Try a Simulation (Optional)

New users may wish to try the authentication simulation under the Help>Simulation menu option. In a similar way to the capture simulation, the identify[1] simulation precisely mimics a genuine authentication cycle, responding appropriately to the relevant settings within the options screens.

Step 5a: Check the HAT Headset Hardware

Check that the HAT headset hardware is correctly connected (Figure 7-3) and that there are two good power cells[2] in the microphones jack-plugs.

Step5b: Position the HAT Headset

Position the HAT Headset comfortably on the head ensuring that the ear microphone is positioned centrally over the pinna of the outer ear (Figure 5-2), in line with the ear canal, and with the mouth microphone positioned vertically central and horizontally offset from the centre of the mouth; to minimise breathing pickup.

[1] The naming of the authentication process 'identify' does not imply the process is identification. The identify process remains strictly identity verification; the authentication of a claimed identity.
[2] Each microphone jack-plug requires a single LR44 power cell.

Step 6: Identify

Press the 'Capture' button on the HAT toolbar Ⓣ and follow the comprehensive onscreen instructions: the HAT Application will prompt the user to speak up a random alphanumeric character. Having already registered with the system (and performed a simulation) the process will be familiar to the user.

After each individual capture, the application will validate the samples according to the settings in the validation options tab (Figure 7-8), following the same process that is used for registration, producing a similar output to the one illustrated in Figure 7-11.

The application will then cycle through the HAT Stage-2 Filter (Section 6.2.2), Stage-3 Absorption (Section 6.2.3) process loop Ⓕ, generating the HAT template (Figure 7-12).

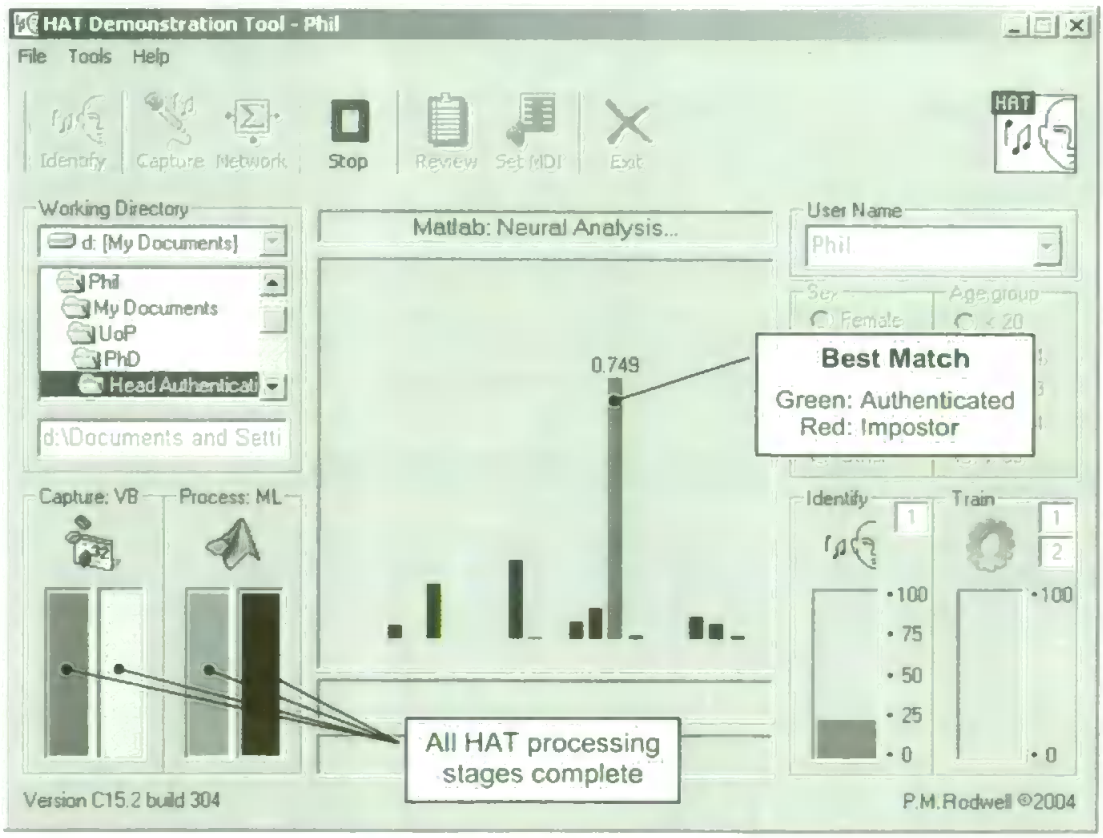


Figure 7-14 : HAT Application – Stage-4 (neural-network) Analysis plot

The HAT template is presented to the stored neural-network of the *claimed* user and the output compared with the authentication threshold associated with their private network, producing the graphical output shown in Figure 7-14. The plot shows the result of feeding the current user's template into each registered user's neural-network (from the HAT trials); the tallest bar indicating the best match. In this example, the tallest bar is coloured green, indicating that the current user was also the best match and passed threshold authentication (with the value indicated). As authentication was successful, the HAT 'Identify' confidence-bar **I** is incremented by 25%. If the value had been less than the authentication threshold, then the identify confidence-bar would have decreased by 25%.

7.2.2.4a The HAT 'Identify' Confidence-bar

The 'Identify' **I** confidence-bar, illustrated in Figure 7-15, was included into the HAT Application as a *soft* authentication response mechanism. It is acknowledged that when performing biometric authentication, there is always an element of inherent uncertainty associated with every biometric sample; the confidence-bar was implemented to reduce the effects on the system FMR and FNMR. In essence, a single authentication failure within a continuous authentication system is of minor consequence and the confidence-bar reflects this, buffering such singular errors. As the confidence-bar is initialised at 50%, or *mildly* confident, it would take two initial authentication failures for the system to flag a warning, as would be expected when in practice authentication successes of a correctly configured system should outnumber authentication failures.

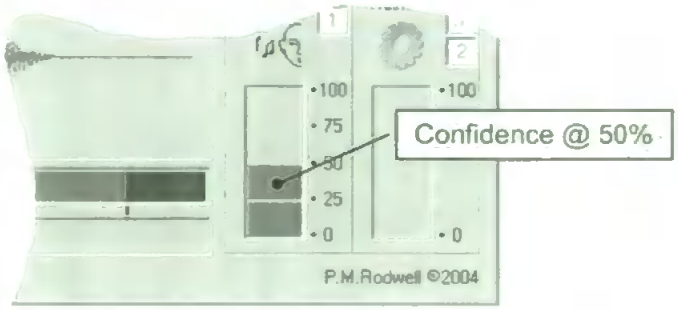


Figure 7-15 : HAT Application - Identity confidence-bar

7.3 The HAT Trials

The development of the HAT process, including the initial proof-of-concept and early experimental work evaluating the absorption and correlation analysis methods, were based on various biometric templates captured from a small sample group of five volunteers. Once the viability of HAT had been established within this control group, a set of trials were proposed involving a set of twenty volunteers (four times the original sample group) to investigate the techniques potential within a wider population; these were called the HAT trials.

The HAT trials can be broken down into four distinct stages of operation, which are identified below and discussed in the following sub-sections:

- **Preparation:** Preparation for the trials, including establishing the trials format and readying the HAT demonstration tool for general use.
- **Selection:** Selection of the trial volunteers.
- **Conduct:** Conduct the trials.
- **Analysis:** Analysis of the HAT trials results.

7.3.1 Preparation for the Trials

Preparation for the trials involved first establishing their format. It was decided to select a sample group of twenty volunteers: a number large enough to pose a suitable challenge to the HAT process and realise a useful set of qualitative results beyond the small developmental control group, and yet not too large as to require a long period of time or overload the design of the current HAT demonstration tool (including practical issues such as the robustness of the only modified HAT Headset and the inherent technical capacity of the HAT Application[1] not originally designed for large scale use).

[1] The HAT Application (v.15) compares ALL registered users during HAT Stage-4 Analysis. Although this is acceptable for twenty users, it would eventually become impractical as the user base increased.

Modifications to the HAT demonstration tool included both the hardware headset and the software application. The headset required strengthening for extended use, including lacing of microphone cables and the purchase of robust signal cables and plugs for the 40+ trial sessions without fear of compromising the trial process due to faulty hardware.

The HAT Application is covered in depth in the previous section (Section 7.2.2), including the extensive redesign and modifications the HAT Application underwent for use in the trials; accounting for around 3 months additional development time on top of the applications 6 month development cycle.

7.3.2 Selection of the Trial Volunteers

The HAT trial group was selected to represent as diverse a group of people as could realistically be represented by twenty volunteers, and included diversity of:

- **Sex:** in Chapter 5 Figure 5-12 it is illustrated how the male and female vocal ranges can differ by up to 100Hz.
- **Age:** ranging from 24 to 64 years; in Chapter 5 Figure 5-1 it is illustrated how the human auditory range varies with age.
- **Nationality:** predominantly English speakers, though including some foreign nationals to demonstrate how the HAT process is language independent, utilising variations in sound, not comprehension, for its biometric markers.

The volunteers were pooled from a variety of disciplines from within the hosting University (including students and lecturers), and external to the University (including: professional and non-professional workers) to represent a fair cross section of society. All non-English trial participants spoke English as a second language, and for consistency all participant registration was conducted in English for the two primary sessions; and in a native tongue for a third session. For a complete list of participant and trial session statistics, see the HAT trials timetable in Appendix G.

7.3.3 Conducting the Trials

The trials were conducted over two sessions: the first session being used to register the user's HAT Stage-4 neural-networks, and the second session to test the neural-networks and calculate the HAT Stage-5 (authentication) Thresholds. The sessions were separated by a period of at least 24 hours, to accommodate any short term aging of the biometric template. Like all biometric authentication systems HAT is susceptible to the variability's of the host's daily life: their age, mood, diet etc. can all have an effect on the composition of the bio-matter in the user's head (Section 4.2.2)[1].

The individual trial sessions were passively supervised within a controlled environment, where participants were insulated from excessive extraneous noise (Section 6.2.1.3) and unwarranted interruptions. After a brief introduction to the HAT Headset and Application, including a simulated registration run (Section 7.2.2.3: Step-4), participants commenced the user-managed HAT registration process, taking approximately 3 minutes to complete. As the HAT Applications default Stage-4 Analysis is configured to use all twenty trial participant's biometric templates to construct the individual user's neural-networks, the trial sessions were conducted with the application in Capture Only[2] mode: HAT Stage-4 Analysis was performed *en-mass*[3] upon completion of trial session 1, and Stage-5 Thresholds calculated *en-mass* upon completion of trial session 2.

7.3.4 HAT Trials Results

A selection of the trial results are presented graphically in the following sub-sections, from two distinct stages of the HAT process: Stage-3 Absorption (Section 6.2.3) producing the HAT template(s); Stage-4 Analysis (Section 6.2.4) producing the neural-network(s).

[1] The long term management of the HAT templates is the responsibility of a biometric security framework.
[2] HAT demonstration tool: Tools>Capture Mode>Capture Only.
[3] HAT demonstration tool 'Mass Operations' function, see Appendix F.

7.3.4.1 HAT Stage-3 Absorption templates

The HAT Stage-3 Absorption template is the product of the mean calculation of ten audio waveforms (the numbers 0 to 9), captured during registration, at the twenty-five discrete HAT Stage-2 Filter spot-frequencies (Section 6.2.1.3).

From the volunteer group of twenty participants, a selection of six HAT templates are shown in Figure 7-16 to Figure 7-21 inclusive; captured directly from the embedded 'Absorption Curve Analysis' tool within the HAT Application[1]. With reference to the thesis section covering the composition of the HAT template (Section 6.2.6), it can be seen that the trial participants' individual response curves showed a clear collective pattern match or correlation with each other; Figure 7-17 is a good example of this exhibiting very little variance between curves. Even when observing a relatively poor example by comparison (Figure 7-20), the consistent shape of the participant's curves are still clearly visible; it is only the variance which has changed, not the unique collective shape. By further comparing the graphs between individual trial participants, it can be seen that each user's collective set of curves follows a unique shape, emphasized indicated by the *mean* curve (the HAT template) shown in red[2].

In comparison to a generic authentication model, the graphs in Figure 7-16 to Figure 7-21 demonstrate HATs ability to fulfil the following fundamental authentication principles:

- Biometric samples captured from an individual user are consistent in nature;
  - HAT Absorption patterns of curves from the <u>same</u> user follow a <u>common</u> shape.
- Biometric samples captured from multiple users are inconsistent in nature;
  - HAT Absorption patterns of curves <u>between</u> users follow a <u>different</u> shape.

[1] The 'Absorption Curve Analysis' tool is activated by entering a registered user into the 'User name' field or selecting a trial participant from the 'User name' pull down menu, and pressing the blue cog ⚙.
[2] Standard deviation curves option has been omitted from the graphs to emphasize the HAT template.

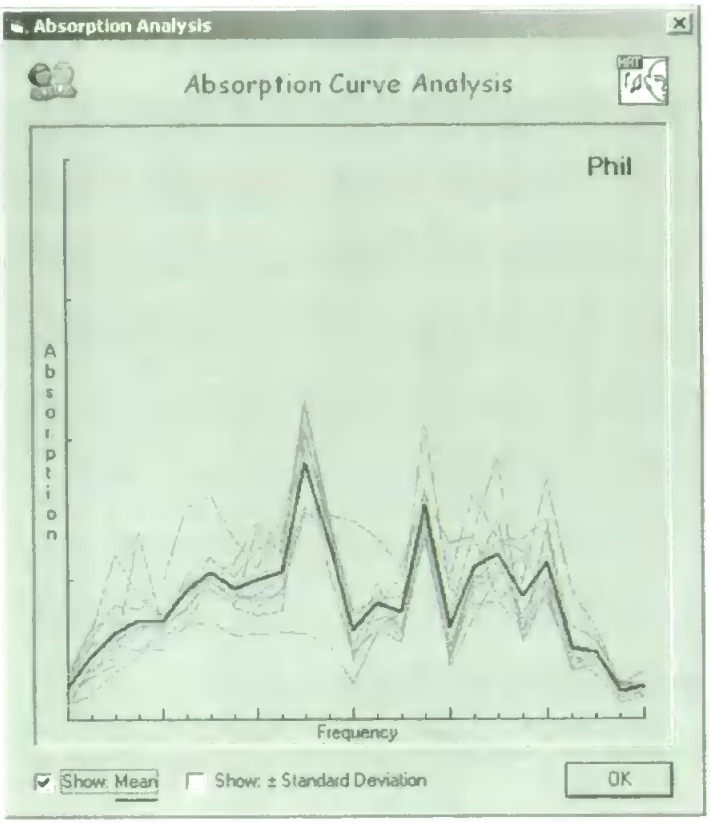


Figure 7-16 : HAT Template of trial participant - u01_Phi

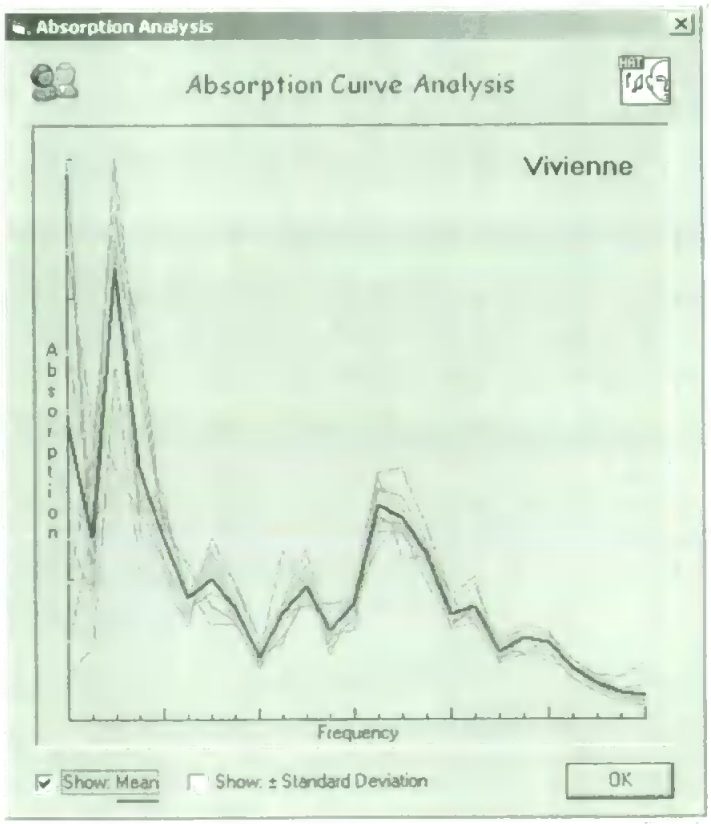


Figure 7-17 : HAT Template of trial participant - u03_Viv

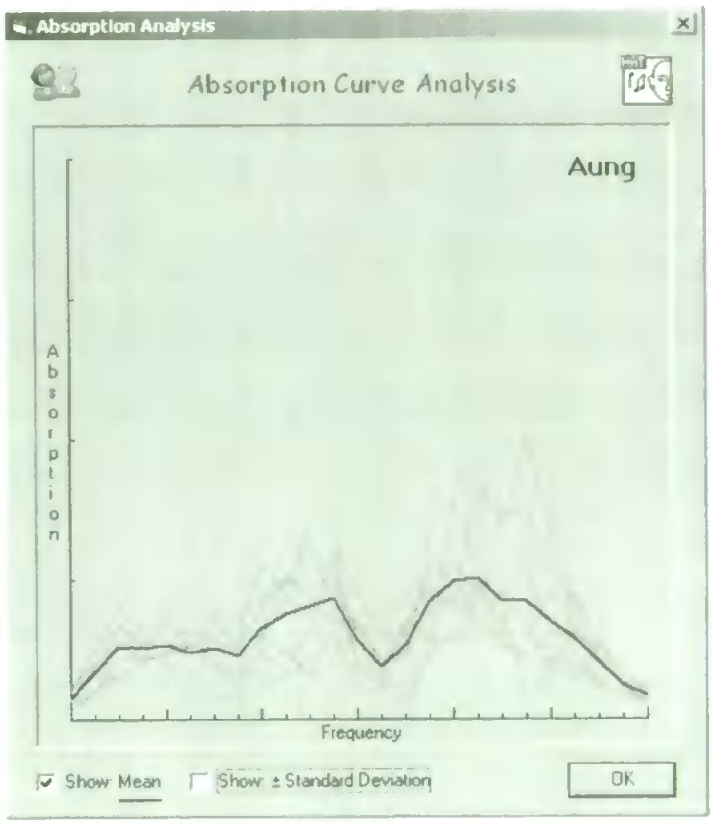


Figure 7-18 : HAT Template of trial participant - u04_Ang

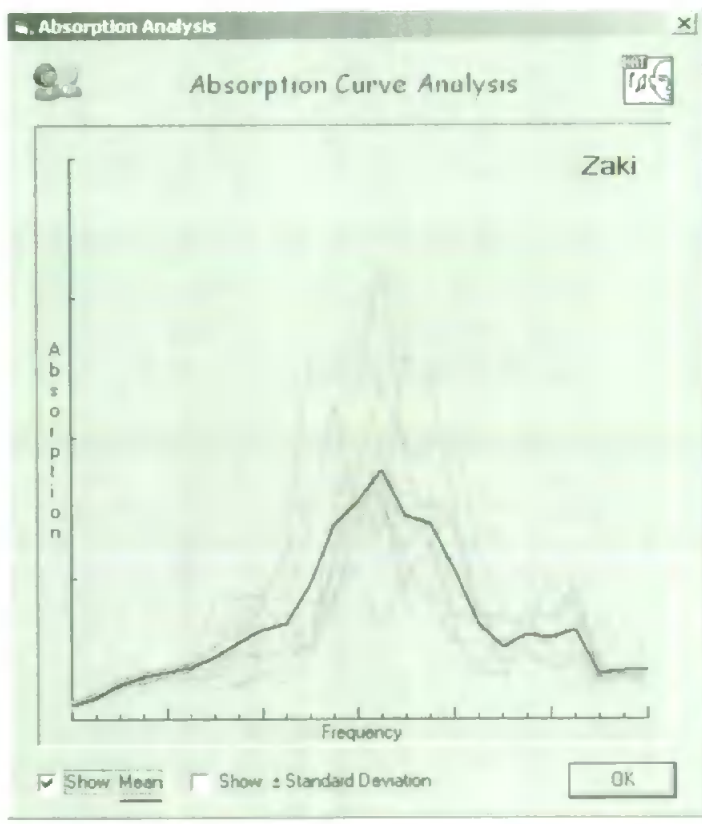


Figure 7-19 : HAT Template of trial participant - u06_Zak

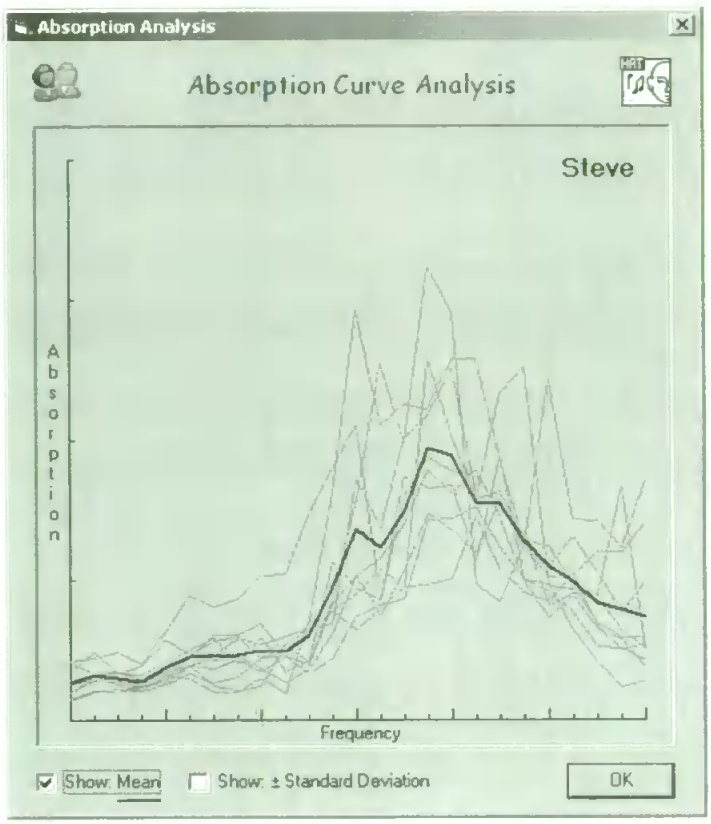


Figure 7-20 : HAT Template of trial participant - u09_Stv

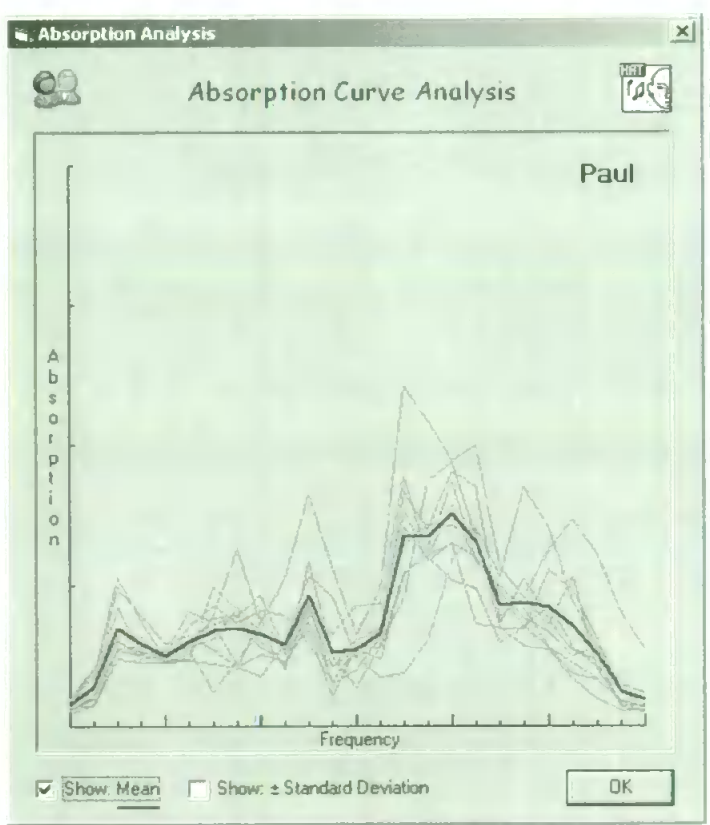


Figure 7-21 : HAT Template of trial participant - u10_Pau

7.3.4.2 HAT Stage-4 (Neural-network) Analysis

To evaluate HATs performance as an authentication system, a user's neural-network was chosen from the trial participants' user base, and subjected to interrogation by a random selection of HAT templates from four other participants of the trials. The neural-networks under investigation were generated using Session 1 data sets, with the data set owner being identified as 'good' and ALL other trial participant's data sets (x20) as 'bad'. The HAT templates used to interrogate the chosen neural-network were generated using Session 2 data from the trials.

The authentication tests were performed in Matlab, using the proprietary neural-network toolbox, and the graphical results are presented as stem plots in Figure 7-23 to Figure 7-32 inclusive. The plots are presented in vertical pairs, where:

- The upper plot is the neural-network response to feeding the original network Session 1 training data back into the network it was used to train. This gives an indication as to the training performance and authentication potential of the network. This plot wants to be as close to the ideal response, shown in Figure 7-22, as possible. Any significant deviation from the ideal response indicates inadequate training, and conversely could be improved with additional training data. In relation to a biometrics system, biometric templates are normally refined over time and not usually dependent on just one sample set; The HAT trials can therefore be considered as representative of a worse case scenario.
- The lower plot represents the neural-network response to interrogation by a random selection of HAT templates from four other participants of the HAT trials. This plot also wants to be as near to the ideal response as possible (in reality, as near to the training response as possible).

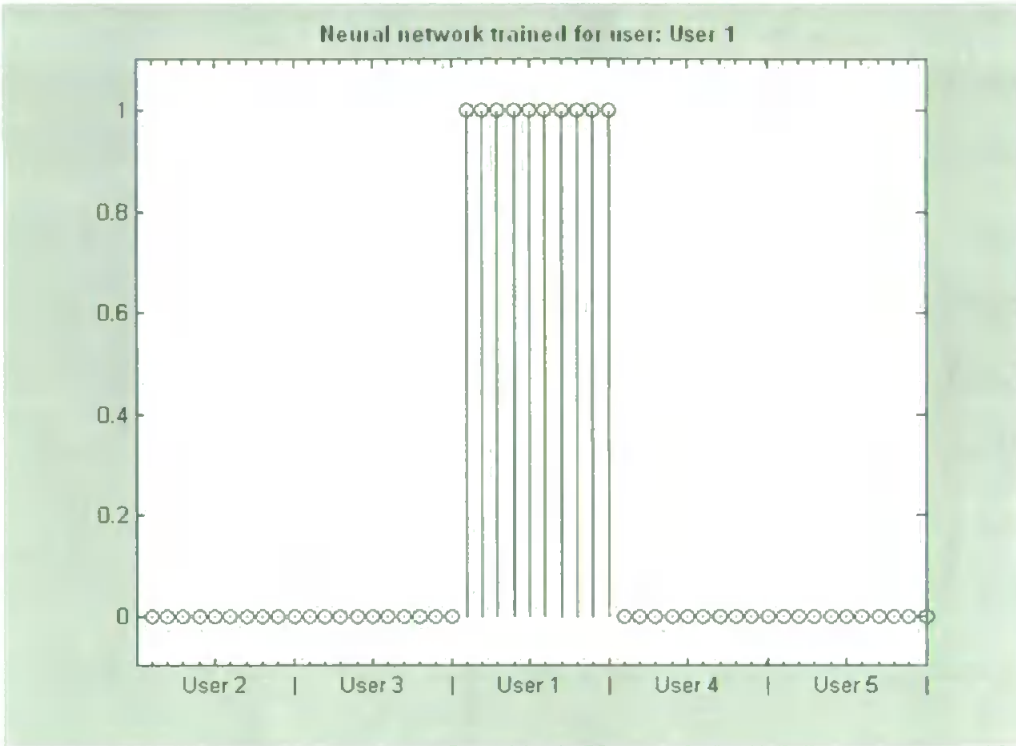


Figure 7-22 : Neural-network testing: Ideal response

Figure 7-22 shows the ideal analysis response plot, composed of the responses of four simulated masquerading users' HAT templates[1] (Users: 2, 3, 4, 5) of the network under test[2], enclosing the responses of the templates[1] of the network owner (User 1) positioned centrally. In the ideal scenario illustrated, the network owner receives 100% recognition of their templates (y-axis = 1), and all other users receive 0% recognition (y-axis = 0).

The five trial participant's neural-network examples under analysis were specifically selected to represent a cross-section of threshold performance, ranging from excellent (users with highly distinctive HAT templates exhibiting low FMR and FNMR error rates) to below average (users with less distinctive templates and potentially unacceptable FMR and FNMR error rates). The final example includes two sets of data from trial session 3 (non-English participant native language), in Arabic and Malay.

[1] Generated using HAT trials Session 2 data sets, for the numbers 1 through 10.
[2] Generated using HAT trials Session 1 data sets, for the numbers 1 through 10.

7.3.4.2a Example 1: User u18_And (Threshold > 0.9)

The example in Figure 7-23 and Figure 7-24 are for HAT trial user 'u18_And'. By inspection of the training data responses in Figure 7-23, the example initially appears to require further training. However, the HAT Identify plot shown in Figure 7-24 produces an excellent response, offering an authentication threshold well in excess of 0.9 for 100% (FNMR=0%) of the owners challenge samples, with none of the opposition users' HAT templates approaching this figure (FMR=0%).

7.3.4.2b Example 2: User u09_Stv (Threshold > 0.7)

The example in Figure 7-25 and Figure 7-24 are for HAT trial user 'u09_Stv'. Although in the training responses in Figure 7-25, one training sample notably drops to a value of 0.8, the remaining training samples maintain an average in excess of 0.9. The HAT identify plot shown in Figure 7-24 produces a result with 90% of the owners challenge samples offering an authentication threshold in excess of 0.7 (FNMR=10%), with only one sample form user 'u10_Pau' presenting a potential problem for the network (FMR = 0.025%).

7.3.4.2c Example 3: User u10_Pau (Threshold ≈ 0.4)

The example in Figure 7-27 and Figure 7-27 are for HAT trial user 'u10_Pau'. User 'U10_Pau's neural-network presented one of the best sets of training response data, with all training samples well in excess of 0.8 and an average of 0.9. However, this performance was not maintained during HAT Identification, where 90% of the owners challenge samples offered an authentication threshold of only 0.4 (FNMR=10%). In the systems defence however, even at this reduced threshold only one of the opposition trial users' HAT templates, from user 'u08_Adr', challenged this threshold (FMR=0.025%).

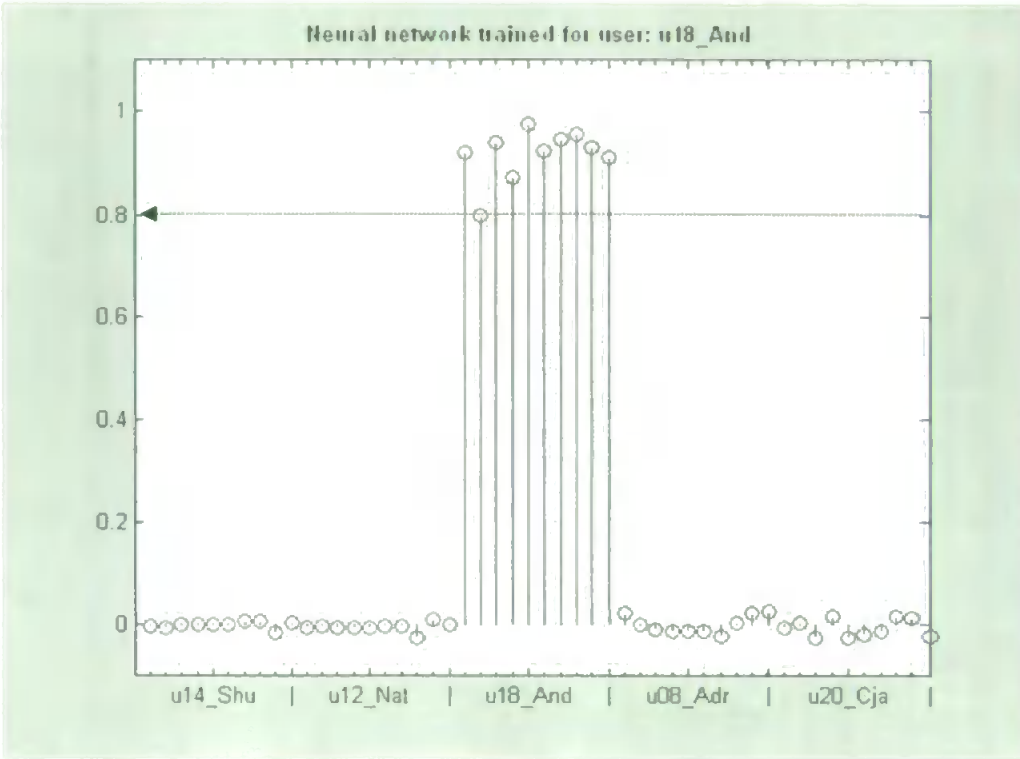


Figure 7-23 : Neural-network testing of user: u18_And (Training Session 1)

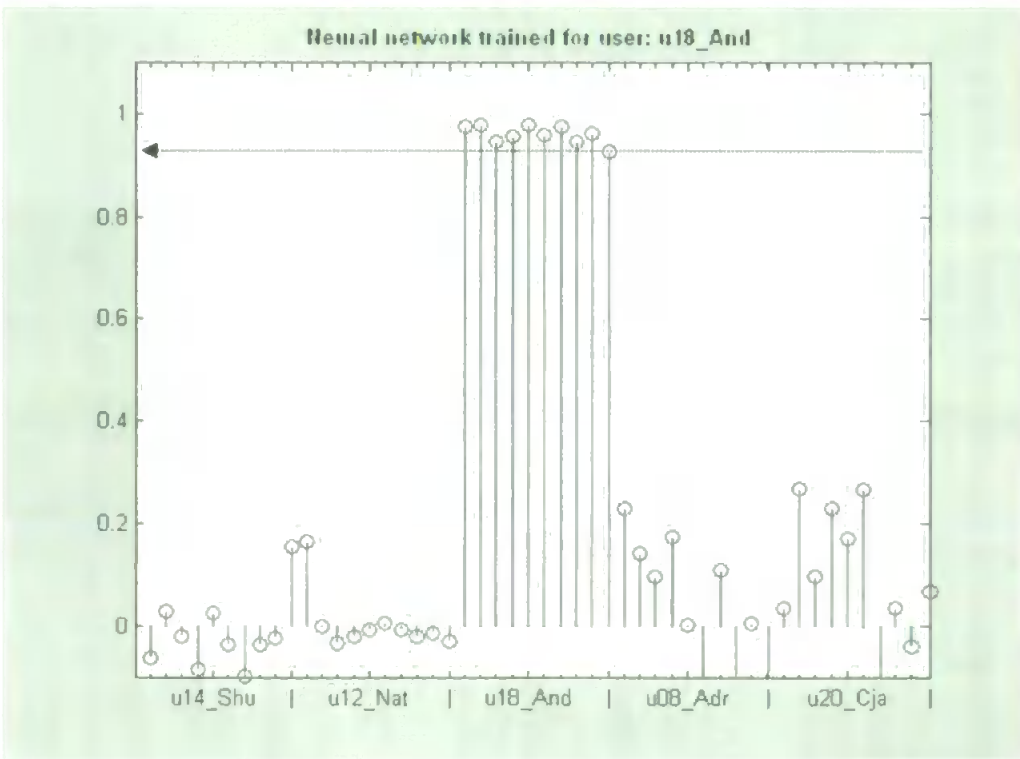


Figure 7-24 : Neural-network testing of user: u18_And (Identify Session 2)

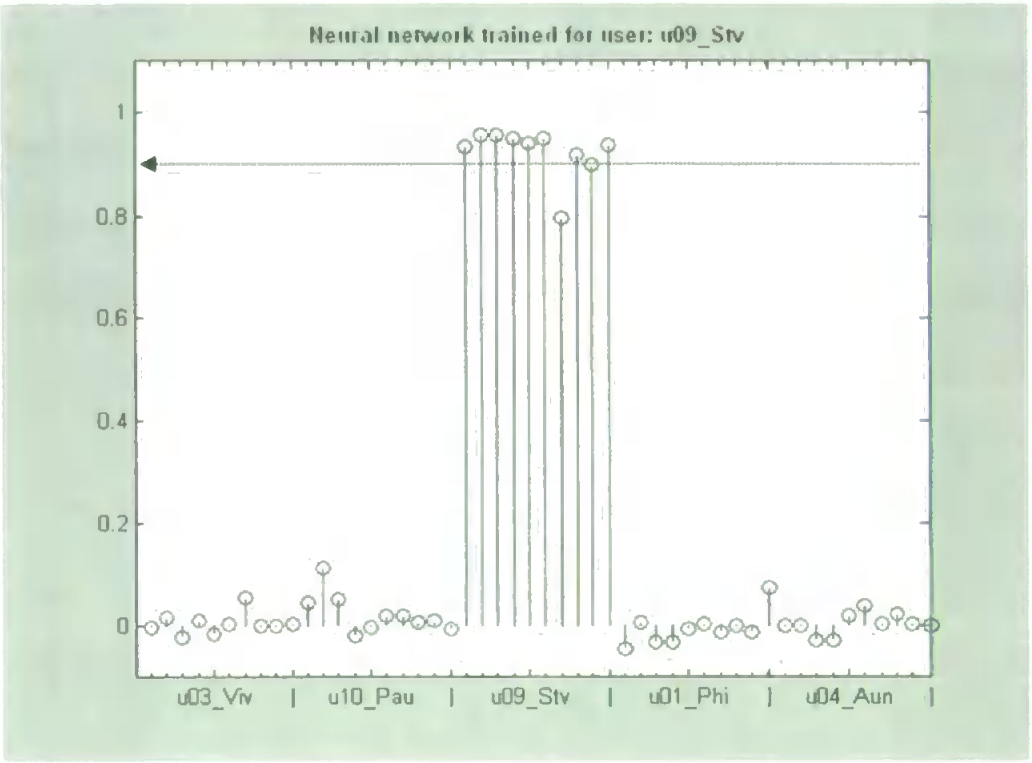


Figure 7-25 : Neural-network testing of user: u09_Stv (Training Session 1)

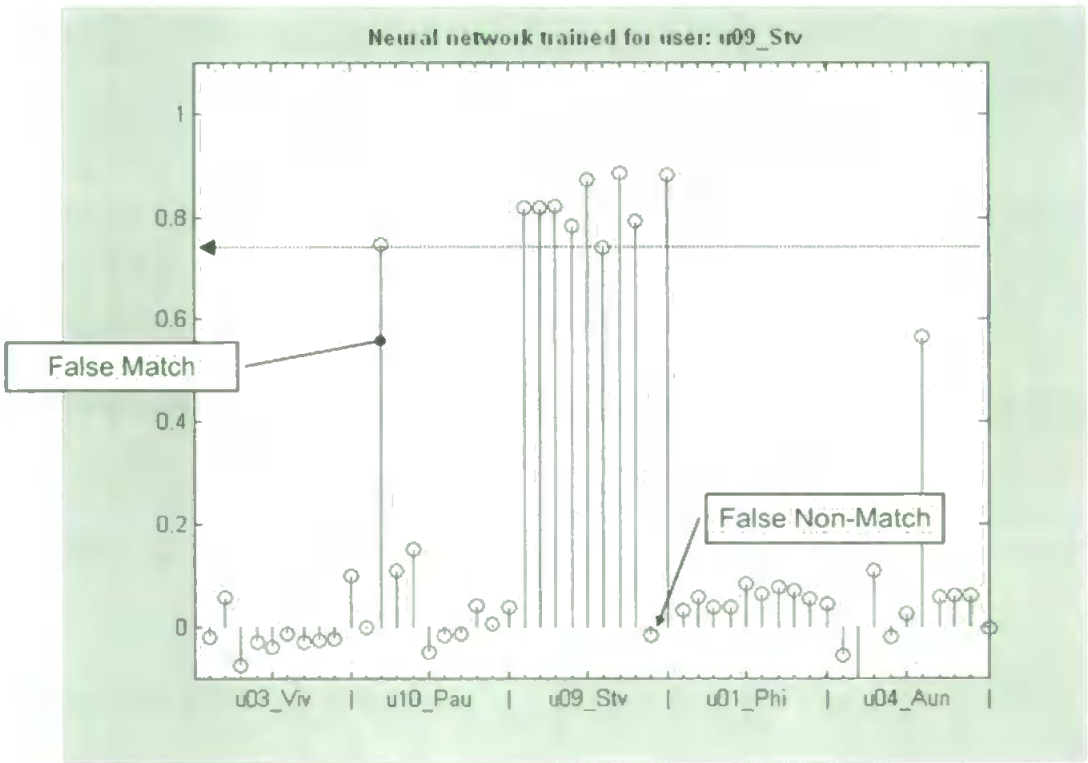


Figure 7-26 : Neural-network testing of user: u09_Stv (Identify Session 2)

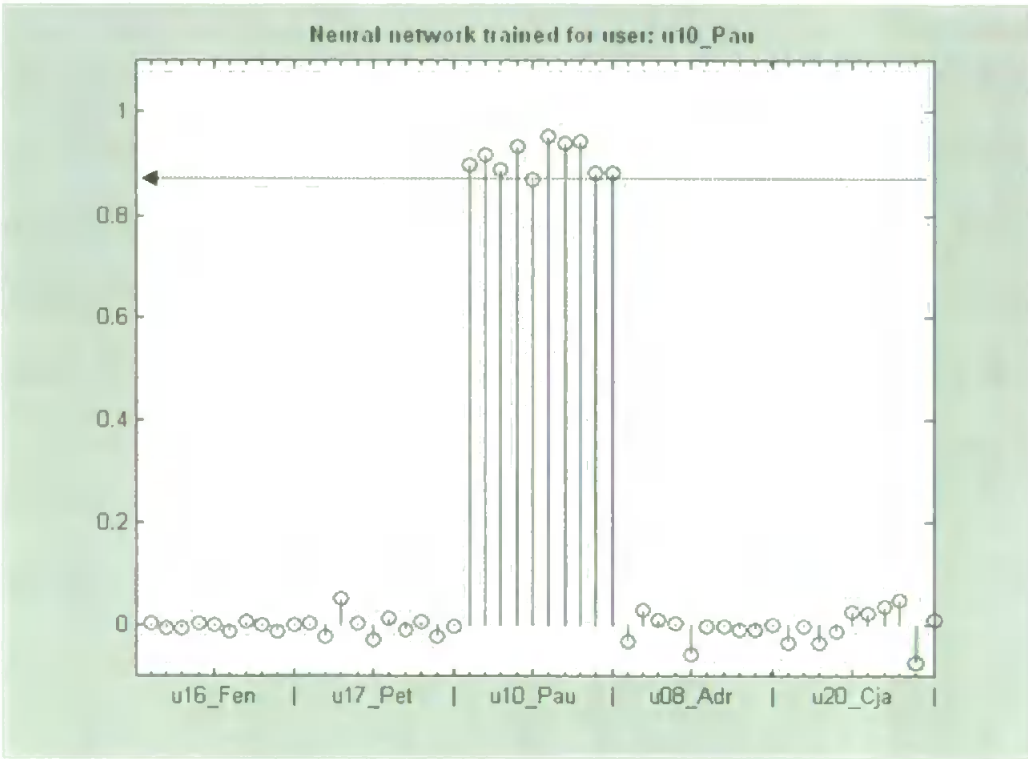


Figure 7-27 : Neural-network testing of user: u10_Pau (Training Session 1)

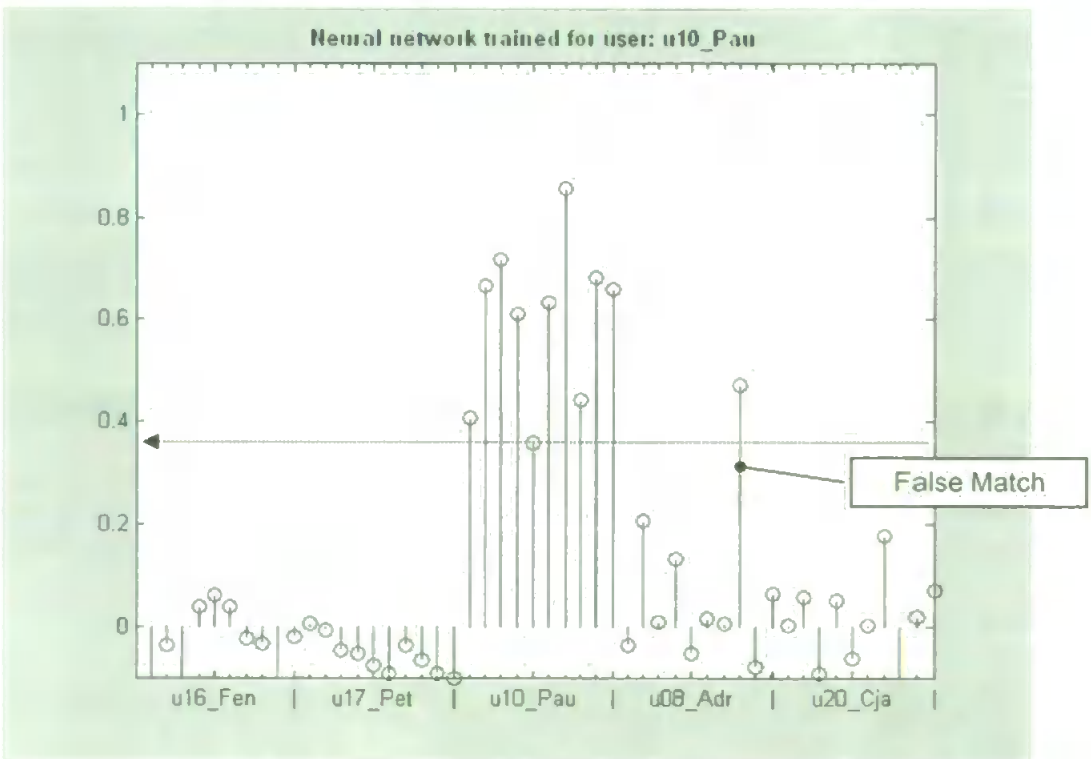


Figure 7-28 : Neural-network testing of user: u10_Pau (Identify Session 2)

7.3.4.2d Example 4: User u01_Phi (Threshold ≈ 0.2)

The example in Figure 7-29 and Figure 7-30 are for HAT trial user 'u01_Phi'. User 'u01_Phi' appeared at first inspection to offer a potentially robust neural-network, with all training samples exceeding a value of 0.8, illustrated in Figure 7-29. However, during HAT Identify testing, the network produced a below average performance, offering an authentication threshold of only 0.2 for 90% of the network owners challenge samples (FNMR=10%, FMR=0.075%). With only 60% of the owners challenge samples exceeding a threshold value of 0.7 (FNMR=40%, FMR=0%), this network presents a clear case for retraining (Figure 7-30) as neither of these scenarios is acceptable in the long term.

7.3.4.2e Example 5: User u17_Pet (Foreign Language, Threshold ≈ 0.5)

The example in Figure 7-31 and Figure 7-32 are for HAT trial user 'u17_Pet'. In this example it was decided to introduce some foreign language data into the tests to demonstrate the HAT processes transparency to language; the HAT process is not dependent on 'what you say', but 'how you say it'. In the examples, user 'u11_Abd' presented his training and challenge data in Arabic, and user 'u04_Aun' in Malay: two languages which sound distinctively different to English. The plot showing the results of neural-network training is shown in Figure 7-31, illustrating a good training session with 100% of the training samples exceeding a threshold value of 0.8. The HAT Identify challenge plot, shown in Figure 7-32, shows a good response to both the owners and the opposition users' HAT templates, with 80% of the network owners challenge data exceeding a threshold of 0.7 and 90% exceeding 0.5 (FNMR=10%): none of the opposition users' challenge samples present any threat to the owners network (FMR=0%), and this example offers the second best authentication response from the tests.

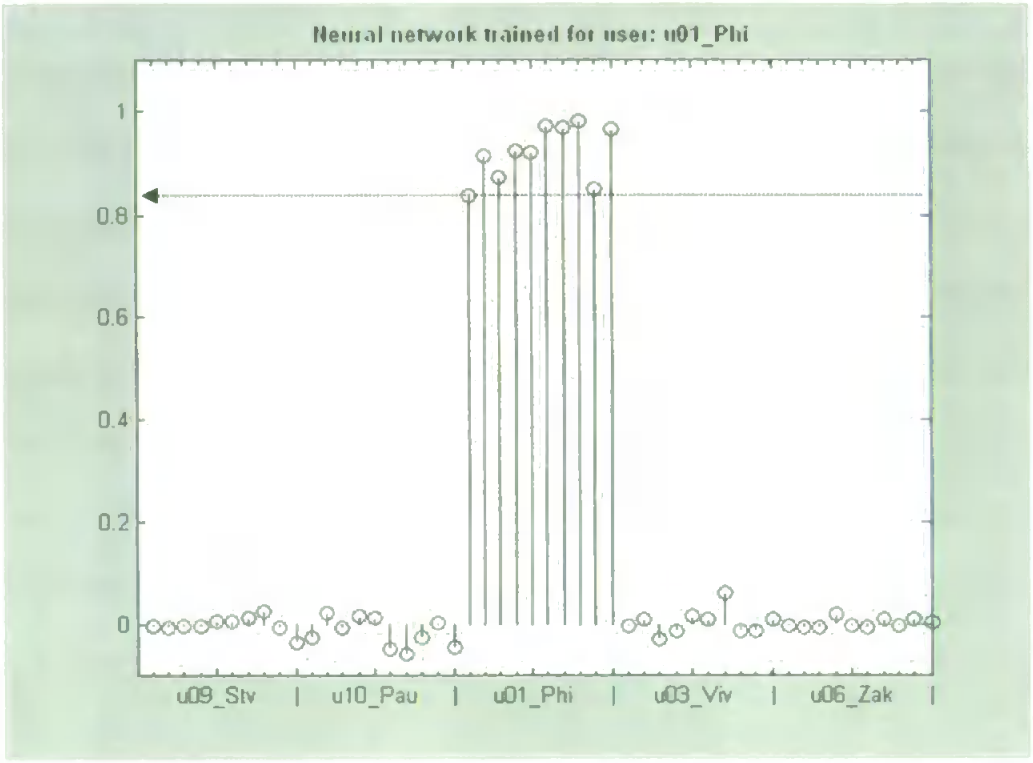


Figure 7-29 : Neural-network testing of user: u01_Phi (Training Session 1)

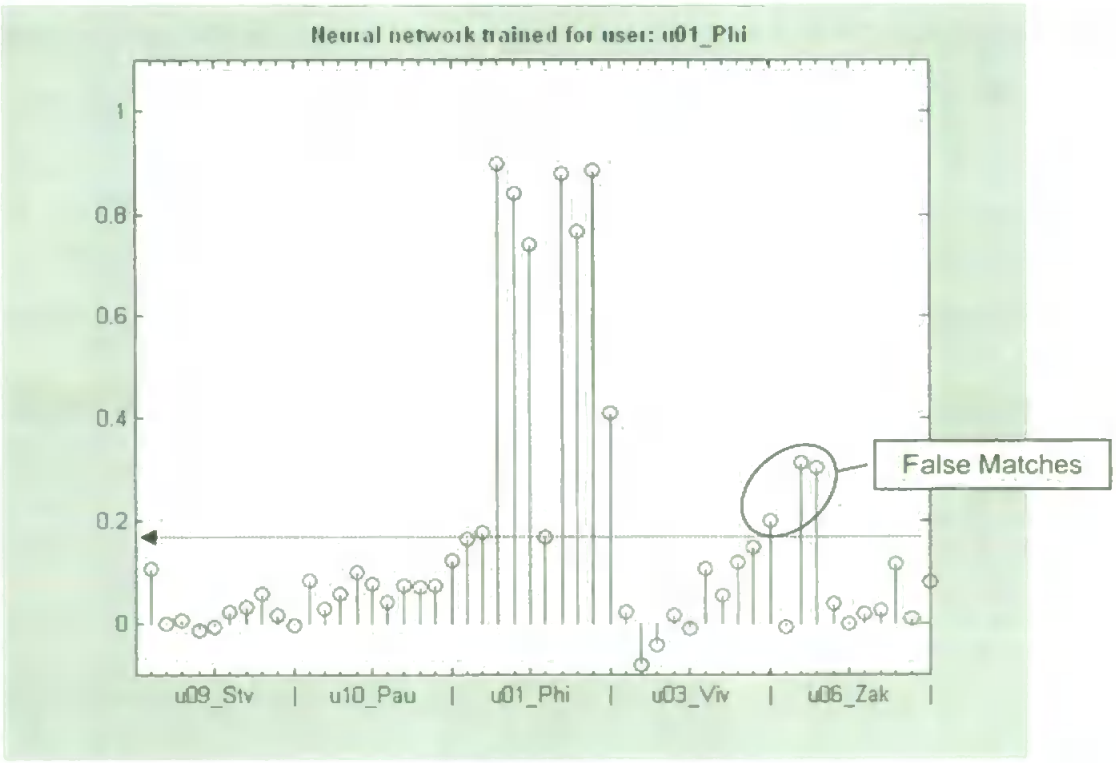


Figure 7-30 : Neural-network testing of user: u01_Phi (Identify Session 2)

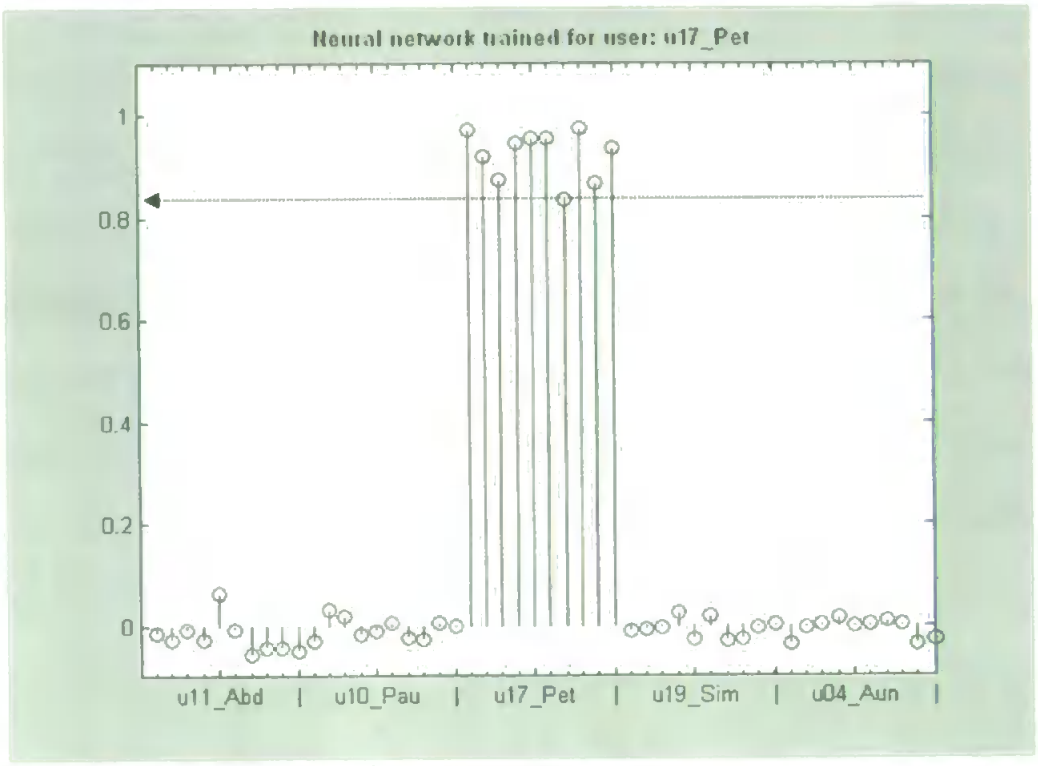


Figure 7-31 : Neural-network testing of user: u17_Pet (Training Session 1 - Foreign)

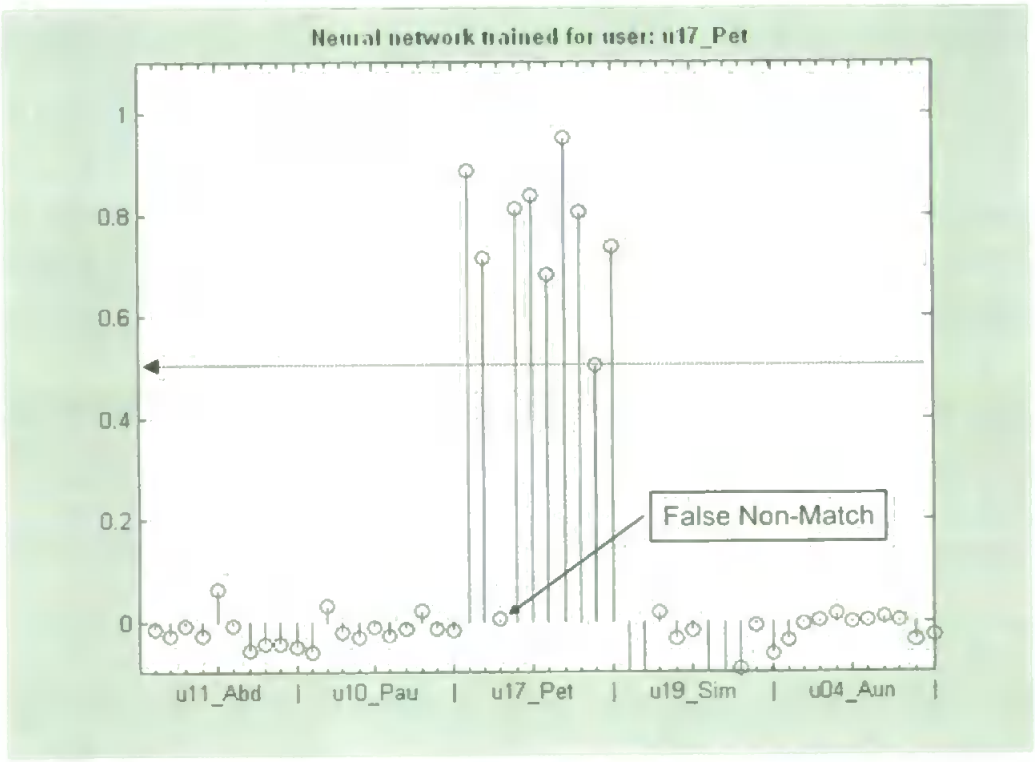


Figure 7-32 : Neural-network testing of user: u17_Pet (Identify Session 2 - Foreign)

7.3.4.3 System Authentication Thresholds and Error Rates

Owing to HATs potential for continuous non-intrusive authentication, individual authentication successes and failures within a HAT protected system are less important than in traditional PoE security systems. It is a user's authentication history or *trend* which will now be used to determine an appropriate system response to deviations in the approved authentication response profile.

By combining the error rates generated in the examples 7.3.4.2a to7.3.4.2e, it is possible to produce *preliminary* error rates for the current HAT system as a whole of FNMR = 6% and FMR = 0.025%, where preliminary draws attention to the following key points:

- The error rates are for the current demonstration tool NOT for the HAT process.
- The user's neural-network was trained using only ONE registration data set.
- The user's authentication threshold was calculated using only ONE set of user registration challenge data.
- The HAT Application does not intelligently manage its thresholds.

The HAT demonstration tool (v15.2) calculates its HAT Stage-5 Thresholds based on a preset FNMR of 10% (1 in 10 samples); when trial user's session-2 data is fed into their session-1 network. The HAT Application has NOT been programmed to intelligently manage or dynamically refine its user thresholds, as would be expected in a commercial system. Although a basic thresholds calculation algorithm was required within the HAT Application to facilitate authentication, this task would traditionally fall under the jurisdiction of an overall security management framework.

System thresholds management is included in the section on Future work (Section 8.3).

7.4 Conclusion

Having defined the five discrete stages of the HAT authentication process in Chapter 6, it was necessary to evaluate the technique in a broader context. To realise this goal, a set of HAT trials were conceived involving volunteers including: both sexes, a cross section of age groups, and multiple nationalities. To enable the trials, the HAT demonstration tool was developed out of the research test bed used to prove the original concepts of head authentication in Chapter 5.

Through a series of examples, the individuality of trial participants' biometric template(s) generated at Stage-3 of the HAT process was proven, where:

- HAT Absorption patterns of curves from the <u>same</u> user follow a <u>common</u> shape.
- HAT Absorption patterns of curves <u>between</u> users follow a <u>different</u> shape.

Through a series of further examples, a selection of the user templates, generated in HAT Stage-3, were fed into a selection of five HAT Stage-4 authentication networks realising a series of stem plots giving an indication as to the systems authentication capabilities. The results were presented in order of performance from excellent to poor, realising error rates (for the examples shown) of FNMR = 6% and FMR = 0.025%. These error rates are highly dependent on the authentication thresholds set in HAT Stage-5, and it is expected that a biometric network management framework would ultimately manage these values in order to maintain optimum system performance: the development of such a framework was beyond the scope of this research.

The next chapter discusses the conclusions of the research into non-intrusive authentication in greater detail, addressing the key areas of research limitation and future work for the novel HAT process.

Chapter 8

Conclusion

8 Conclusion

It was established in Chapter 2 that security provisions within the current mobile telecommunications networks, are primarily aimed at secure communications through data encryption and *terminal* authentication via use of a SIM card. It was discussed how the advanced services enabled by post 2nd generation wideband mobile networks have developed services far in advance of the security systems originally conceived to protect their forebears. There now exists a requirement for a more secure *subscriber*-based authentication system enabling protection commensurate with the risks and consequences associated with the more sensitive information that these new service networks access.

Having clearly identified the problem the research was conceived to address, a survey was conducted to assess public opinion on current mobile security and their awareness of the security issues raised by the advanced data services of wideband mobile networks. The survey was divided into two sections covering present and future mobile authentication respectively. Chapter 3 covered the first part of this survey and proposed the hypothesis:

> *The majority of mobile subscribers either do not understand or are lacking well founded opinion on mobile security issues. They are also generally ignorant of the security implications of the advanced services being offered through the next generation of wideband networks known as 3G.*

The survey results presented a contradiction. Although the majority of survey users are happily willing to signup for the advanced services on offer by the wideband network operators, with 85% claiming to be aware of the security risks involved, 70% are still unwilling or unable to activate the most rudimentary security setting on their current mobile devices; the PIN. The survey concluded broadly in support of the hypothesis, but with the added finding that it is not the principals of authentication which users are rejecting, but the current application of those principals; the authentication mechanism(s).

One of the requirements of the research was for an authentication mechanism, either novel or adapted, which could be realised non-intrusively within a mobile context: the discipline of biometrics naturally lent itself to this requirement. A full review of current biometric authentication techniques was conducted in Chapter 4, including the second part of the consumer survey addressing users' attitudes towards future authentication issues; including biometrics. The survey found that 96% of respondents had no objection to their biometric markers being used as part of a mobile authentication system; this is an excellent result when compared to the 70% of respondents who are essentially unhappy with using the PIN, suggesting users would use a suitable system if it existed. When asked about their views on continuous authentication, 83% of respondents had no objection to the idea. The groundwork was essentially laid for the development of a continuous, non-intrusive, biometric authentication system.

Through a novel process of reinvention of selected existing biometric techniques combined with principles drawn from the discipline of Audio Evoked Responses, Chapter 5 discusses the conception of the Head Authentication Technique. The chapter includes a series of trials performed by the ENT department of the local hospital designed to experience AER (specifically otoacoustic emission) analysis techniques in their native environment as an intellectual grounding for the techniques development.

HAT is a novel, inherently multi-modal, biometric authentication technique where the natural symbiotic relationship of the 'behavioural characteristics' of the human voice stimulate the 'physiological anatomy' of the head. The HAT research process discussed in Chapter 6 realised two subtly different versions of the head authentication principles: the absorption method and the correlation method. After extensive testing on and between the two methods, the absorption method was selected as the more appropriate method for final development due to its consistently better performance and simpler analysis stages, requiring less processing time.

The HAT authentication process was rationalised into a five stage operation, defined as:

- **Capture** of biometric audio waveform pairs from a user.
- **Filter** of audio waveform pairs at discrete spot-frequencies.
- **Absorption** comparison of discrete waveform spectra defining a HAT template.
- **Analysis** of the HAT absorption template within a neural-network.
- **Classification** of the neural-network output through threshold comparison.

Having established the principles and stages of the HAT process, the tool was evaluated through a series of trials, discussed in Chapter 7, involving a group of twenty volunteers representing a cross section of sexes, ages and nationalities. To enable the trials, a comprehensive HAT demonstration tool was developed to manage system registration and authentication for the novice user. Analysis of the trials results using a series of group examples realised system error rates of FNMR = 6% and FMR = 0.025%, and confirmed the individuality of HAT templates generated by the HAT process, where:

- HAT Absorption patterns of curves from the <u>same</u> user follow a <u>common</u> shape.
- HAT Absorption patterns of curves <u>between</u> users follow a <u>different</u> shape.

The research has met all of the objectives originally outlined in Chapter 1 and has resulted in the design and development of an advanced authentication technique capable of continuous non-intrusive application in a vocalised services environment. A number of papers relating to the research have been presented at national and international conferences, and the research has realised an international patent, in association with Orange PCS, in the area of 'determining identity of a user' on an electronic communication system (#GB2375205, 2001). The novel aspects of the patent include:

- The head authentication method(s) of biometric capture.
- The head authentication method(s) of biometric analysis.

Copies of these materials are included in the appendices.

8.1 Achievements of the Research

This section provides a list of the key research achievements made during the course of the PhD, culminating in the Head Authentication Technique. In order the research has:

1. Performed a review of mobile network technologies, from the 1st generation analogue telephony systems to the latest 3rd generation wideband digital networks, identifying user authentication security issues relating to post 2G developments.
2. Assessed mobile subscriber's awareness of the risks of masquerade attack on current mobile devices, specifically relating to the effectiveness of the PoE PIN, and their receptiveness to a range of possible alternative advanced authentication principles.
3. Performed an analysis of current biometric principles and techniques, identifying those techniques which could be applied in a mobile context.
4. Conceived a number of novel non-intrusive biometric authentication approaches applicable to the mobile environment, leading to the selection of a single approach and its realisation in a proof-of-concept prototype. The chosen approach was named the Head Authentication Technique (HAT).
5. Developed the HAT authentication biometric into a five stage process and realised the registration and authentication aspects of the technique within a user accessible demonstration tool. The composite prototype tool included construction of a hardware biometric collector and programming in Win32 of a software management application.
6. Evaluated HAT in a series of trials using a representative user community, providing proof of viability of the technique in practice. The trials demonstrated the unique nature of the biometric templates produced by the HAT process: how biometric templates from the <u>same</u> user exhibit a <u>common</u> pattern, yet templates <u>between</u> users exhibit a <u>different</u> pattern. The trials were also used to demonstrate the authentication performance of the process through a series of masquerade challenge examples: basic error rates for the HAT demonstration tool were: FNMR = 6% and FMR = 0.025%.

8.2 Limitations of the Research

Although all of the original objectives for the research set out in Chapter 1 have been met, time constraints and the operational envelope of the HAT demonstration tool imposed certain limitations upon the work, which are summarised below:

- HAT authentication can only be performed when a user is verbally interacting with their mobile device. As such, HAT would most usefully form part of an *arsenal* of authentication techniques, covering the full range of mobile interaction scenarios.
- During the development of the HAT process, a small core group of five volunteers was used to develop the initial proof of concept up to peer approval for the HAT trials. The trials were conceived to extend the proof of concept to a wider audience; however, owing to the completely novel aspect of the technique the trial group was deliberately restricted to twenty volunteers. It is accepted that this number is representative of only a restricted cross-section of society.
- Although the HAT process was primarily developed for mobile use, it has not been installed or demonstrated within a mobile device. The HAT demonstration tool is however capable of operation within a laptop computer.
- Development of the HAT process included two methods of template analysis, absorption and correlation: due to time constraints only the absorption method was developed to proof of concept and incorporated into the HAT process (and subsequent demonstration tool). Further development of the correlation analysis method could yield additional multi-modal system performance benefits.
- Although not a limitation of the HAT process, the HAT demonstration tool was developed for use in trial groups of twenty users (the HAT trials); larger trials would require recoding of certain aspects of the tool: e.g. HAT Stage-4 Analysis.

Despite these limitations, the research programme has made valid contributions to knowledge and provided sufficient proof of concept for the ideas proposed.

8.3 Future Research Work

The HAT research has introduced a novel hybrid multimodal biometric to the field of electronic user authentication. Although the technique was originally developed for use within the field of *mobile* communications, future work could extend the techniques scope to include many additional electronic communications devices, such as the PC.

During the development of the HAT process, certain decisions had to be made to ensure that the research reached completion within a reasonable time. A number of these decisions left areas for future work, which are summarised below:

- Basic HAT Stage-1 Capture collects audio samples from two points on the user's head. Once the HAT technique was proven, the possibility existed of raising the number of capture points to three; including both ears.
- The resolution of the HAT Stage-3 Absorption template (dependent on the number of Stage-2 spot-frequencies), was partly based on the available processing resources available during HAT development. Integration within a custom designed chipset would allow for optimised code and the potential for higher resolution templates without impacting upon authentication cycle times.
- HAT Stage-3 currently only utilises the absorption method to realise the HAT template. The correlation method of difference analysis was not fully developed owing to the existence of a working alternative; they both could exist in unison.
- HAT Stage-5 Thresholds algorithm used during the HAT trials was passive, and based on the network owners' samples simple numerical advantage over impostors. Future work could dynamically set the threshold level, based on a more precise statistical analysis of authentication successes and failures over time.
- A second round of HAT trials involving a more comprehensive assessment of the technique, involving a larger sample group (50 to 100 users), more registration session data (>2), a more natural 'noisy' mobile environment.

8.4 Authentication in Next Generation Mobile Systems

The last ten years have bared witness to a revolution in communications technology not seen since Antonio Meucci original invention of the 'teletrofono' (telephone) in 1849 (Link: Meucci), and the first live trans-Atlantic television transmission in 1962. Up until the mid 1980s, mobile communications for the majority of the general population was a large static box at the side of the road containing a coin operated bakelite telephone. With the introduction of the first analogue mobile handsets in 1983, users' perceptions of mobile communications changed forever. Running parallel with similar growth in the computer market, the introduction of 2nd generation digital technology in 1992 saw the boundaries between mobile handsets and mobile computers merge, with handsets offering traditional computer facilities, and computers becoming ever more mobile. The 3rd generation of mobile communications technology, introduced in 2004, has brought a wealth of new service possibilities to network operators and their subscribers, including: rich-internet, online-banking and m-commerce: to offer these latest personal services, network operators must be able to safely handle the highly sensitive and personal data on which these services depend. Unfortunately, the security in place to protect this personal data from masquerade attack has remained essentially unchanged since the introduction of the first mobile handsets in 1983, in essence 3rd generation data (banking details, medical details) under the protection of a 1st generation authentication system designed to prevent somebody making a voice call on your analogue handset.

The successful deployment of next generation mobile networks and their services will become increasingly dependent on the basic authentication assurance of the networks subscribers. HAT was conceived and developed to address this need offering a viable authentication solution capable of continuously and non-intrusively verifying the identity of any user accessing your data at any time. A biometric solution dependent on 'who you are', not on 'what you know' (or have overheard), or 'what you have' (or have stolen).

References

References

3GPP, 1999. *3G Security: Security Threats and Requirements*. Technical Specification Group Services and System Aspects. 3G TS 21.133 v3.1.0. (Link: 3GPP)

3GPP, 2005. *HSDPA; UTRAN Description* (TS 25.855). *HSDPA Layer 2 and 3 Aspects* (TS 25.856). *Multiple-Input Multiple-Output Antenna Processing for HSDPA* (TS 25.876). *HSDPA - Iub/Iur Protocol Aspects* (TS 25.877). *HSDPA; User Equipment (UE) radio transmission and reception (FDD)* (TS 25.890). Available from: <http://www.3gpp.org> [Accessed Dec. 2005].

911, 2001. *Islamic terrorists destroy the twin-towers of the World Trade Centre in New York* [online]. BBC News, 11th Sept. 2001. Available from: <http://news.bbc.co.uk /hi/english/static/in_depth/americas/2001/day_of_ terror> [Accessed Dec. 2002].

AMD, 2005. *The AMD Geode LX 800@0.9W processor operates at 500MHz*. Anandtech (Hardware analysis and news). Available from: <http://www.anandtech.com/ talkarticle.aspx?frmResourceID=24365&frmWhere=1> [Accessed Dec. 2005].

Baken, R. J. and Orlikoff, R.F., 1999. Clinical Measurement of Speech and Voice. 2nd ed. Singular Press. ISBN: 1565938690

BBC News, 1998. *UK: Ear Print Catches Murderer* [online]. BBC News, 15th Dec. 1998. Available from: <http://news.bbc.co.uk/1/hi/uk/235721.stm> [Accessed Mar. 2004].

BBC News, 1999. *Sci/Tech: Police Play it by Ear* [online]. BBC News, 2nd Jan. 1999. Available: <http://news.bbc.co.uk/1/hi/sci/tech/246713.stm> [Accessed Mar. 2004].

BBC News, 2003. *3G goes live in the UK* (Hutchison) [online]. BBC News, 3rd Mar. 2003. Available from: <http://news.bbc.co.uk/1/hi/technology/2808761.stm> [Accessed Feb. 2005].

BBC News, 2004. *Barcelona clubbers get chipped* (VIP Baja Beach Club) [online]. BBC News, 29th Sept. 2004. Available from: <http://news.bbc.co.uk/2/hi/ technology/3697940.stm> [Accessed Dec. 2005].

BBC News, 2005. *Mobile phone cancer link rejected* [online]. BBC News, 30th Aug 2005. Available from: <http://news.bbc.co.uk/1/hi/health/4196762.stm> [Accessed Nov. 2005].

Bisgaard-Bohr, M. 2002. *Purchase Behaviour Profiling* (White Paper) [online]. Teradata (Europe), Dec. 2002. Available from: <http://www.teradata.com/t/pdf. aspx?a=83673&b=86842> [Accessed Jan. 2004].

Brown, P., McCaig, I., Short, M., Eggleston, A., 2001. *Did the £22 billion auction cripple the Mobile Industry?* [online]. PITCOM meeting, 30th Apr. 2001. Available from: <http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi 2g.com/cgi/mi2g/press/300401.php> [Accessed Feb. 2006].

Bush, G.W., 2002. *Specifics of Secure and Smart Border Action Plan*, 7th Jan. 2002 and *Enhanced Border Security and Visa Entry Reform Act*, 14th May 2002. Signed by G.W.Bush for The Office of Homeland Security, U.S.Government.

Cala, L.A., Thickbrown, G.W., Black, J.L., Collins, D.W., Mastaglia, F.L., 1981. Brain density and cerebrospinal fluid space size: CT of normal volunteers. *American Journal of Neuroradiology*, Vol 2, Issue 1, pp.41-47.

Carreira-Perpiñán, M.A. and Sánchez-Calle, A., 1995. *A Connectionist Approach To Using Outer-ear Images For Human Recognition and Identification* [online]. Depto. de Lenguajes, Sistemas de Información e Ingeniería de Software, Facultad de Informática, Technical University of Madrid. Available from: <http://www.dcs .shef.ac.uk/~miguel/papers/ps/ear-abstract.pdf> [Accessed Sept. 2005].

CellularOnline, 2003. *Latest Handset & Base Station Mobile Statistics* [online]. CellularOnline, 3Q 2003. Available from: < http://www.cellular.co.za/stats/stats-handsets.htm> [Accessed Nov. 2003].

CellularOnline, 2004. *Mobile content shows revenue promise says Nokia report* [online]. CellularOnline, 1st May 2004. Available from: <http://www.cellular.co.za/news_20 04/may/050104-mobile_content_shows_revenue_pro.htm> [Accessed Jan. 2004].

CellularOnline, 2006a. *The History Of GSM: 1982 to 2001* [online]. CellularOnline. Available from: <http://www.cellular.co.za/gsmhistory.htm> [Accessed Feb. 2006].

CellularOnline, 2006b. *Latest Mobile, GSM, Global, Handset, Base Station, & Regional Cellular Statistics* [online]. CellularOnline. Available from: <http://www.cellular. co.za/stats/stats-main.htm> [Accessed Jan. 2006].

CellularOnline, 2006c. *Secure GSM & CDMA Mobile Phones* [online]. CellularOnline. Available from: < http://www.cellular.co.za/phones/secure/secure-phones.htm> [Accessed Jan. 2006].

Chopra, G., 2002. *£4M Mobile Phone Theft* [online]. UK, BBC News. Available from: <http://news.bbc.co.uk/1/hi/england/2482091.stm> [accessed 15th Nov. 2002].

Clarke, A.C., 1945. *Extra-terrestrial Relays*. Wireless World, Oct.1945, pp.305-308. Available from: <http://www.clarkefoundation.org> [Accessed Mar.2005]

Clarke, N., Furnell, S., Lines, B. and Reynolds, P., 2003. Using Keystroke Analysis as a mechanism for Subscriber Authentication on Mobile Handsets. *18th International Conference on Information Security (SEC2003), 26-28 May, 2003, Athens, Greece.* IFIP Conference Proceedings 250 Kluwer 2003, ISBN 1-4020-7449-2, pp.97-108.

CNN, 2001. *HK mobile carriers seek to split 3G tab* [online]. CNN (Business), Dec. 2001. Available from: < http://archives.cnn.com/2001/BUSINESS/asia/12/03/hk. 3g.network.share/> [Accessed Feb. 2006].

CoA, 1999. *State of Washington vs David Wayne Kunze*. Court of Appeal Division II, State of Washinton. Available from: FindLaw, 10th Nov. 1999. <http://caselaw.lp.findlaw. com/scripts/getcase.pl?court=wa&vol=223384&invol=o01> [Accessed Nov. 2005].

Competition Commission, 2003. *Vodafone, O2, Orange and T-Mobile: Reports on references under section 13 of the Telecommunications Act 1984 on the charges made by Vodafone, O2, Orange and T-Mobile for terminating calls from fixed and mobile networks* [online]. Competition Commission Reports, 2003. Available from: <http://www.competition-commission.org.uk/rep_pub/reports/2003/475 mobilephones.htm> [Accessed Feb. 2005].

Cope, B.J.B., 1990. Biometric Systems of Access Control. *Electrotechnology*, April/ May, pp.71-74.

Cox, A., 1997. New Services for UMTS. *UMTS - The Next Generation of Mobile, 27-29 Oct. 1997, London, UK.*

CSI, 2001. Issues and Trends: 2001 CSI/FBI Computer Crime and Security Survey. *Computer Security Issues & Trends* (Computer Security Institute), Spring 2001, Vol.7(1), pp.1-18.

Das, R., 2005. EyeDentification System 7.5 by Eyedentify. In: *An Application of Biometric Technology: Retinal Recognition Series - Part 2* [online]. Technology Executives Club. Available from: <http://www.technologyexecutivesclub.com/ Articles/security/artRetinalRecognition2.php> [Accessed Jun. 2005].

Daugman, J., 1998. *How Iris Recognition Works*. Cambridge: University of Cambridge Press. Extract: IEEE Trans. CSVT 14(1), 2004, pp.21 - 30. Available from: <http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf> [Accessed Jul. 2005].

ETSI, 1999. *Proposed agreement on new requirements on the IMEI*, ETSI TC SMG#30 Plenary meeting, Brighton, 9-11 Nov. 1999. Tdoc SMG P-99-776. Available from: <http://www.3gpp.org/ftp/tsg_t/WG2_Capability/TSGT2_07/Docs/T2-991020%20(IMEI%20agreement).pdf> [Accessed May 2005].

ETSI, 2003. *New form factor for smart cards introduced* [online]. ETSI, Dec. 2003. Available from: <http://www.etsi.org/pressroom/previous/2003/2003%5F12% 5Fff3%5Fsim.htm> [Accessed Apr. 2005].

Fellbaum, K., 2005. *Human Speech Production Based on a Linear Predictive Vocoder* [online]. Brandenburg Technical University of Cottbus, Germany. Available from <http://www.kt.tu-cottbus.de/speech-analysis/> [Accessed Jan. 2006].

Fulton, S.M., 2005. *Fujitsu launches palm vein authentication system* [online]. TGDaily, 30th Jun. 2005. Available from: <http://www.tgdaily.com/2005/06/30/fujitsu_ launches_palm_vein_authentication_system/index.html> [Accessed Nov. 2005].

Furnell, S.M., Green, M., Hope, S., Morrissey, J.P. and Reynolds, P.L., 1996. Non-Intrusive Security Arrangements to support Terminal and Personal Mobility. *Euromedia 96, 19-21 Dec. 1996, London.* pp.167-171.

Geodsoft, 2005. *Good and Bad Passwords How-To* (An Example List of Common and Especially Bad Passwords) [online]. Geodsoft. Available from: <http://geodsoft. com/howto/password/common.htm> [Accessed Dec. 2005].

Geissler, P., 2000. *Vodacom Group Executive Risk Management*, GSM Association Fraud Forum, Feb. 2000.

Gold, S., 2004. *Ninety per Cent of Mobile Devices have no IT Security* [online]. SecureSynergy. Available from: <www.securesynergy.com/securitynews/newsitems/2004/apr-04/020404-08.htm> [Accessed Jan. 2006].

Granger, S., 2001. *Social Engineering Fundamentals, Part 1: Hacker Tactics* [online]. Security Focus. Available from: <http://www.securityfocus.com/infocus/1527> [Accessed Jan. 2006].

Grason-Stadler, ca.2000. *A Complete Guide to Otoacoustic Emissions*. Grason-Stadler Inc. Part No. 1760-0112 - Rev.4.

GSM Association, 2002. *CEIR Back in the Spotlight* [online]. GSM World. Available: <http://www.gsmworld.com/using/security/index.shtml> [Accessed Apr. 2005].

GSM Association, 2005. *GSM Facts and Figures* [online]. GSM World. Available from: <http://www.gsmworld.com/news/statistics/index.shtml> [Accessed Feb. 2005].

GSM 02.09 Version 7.1.1, 1998. *Digital cellular telecommunications system (Phase 2+); Security aspects*. ETSI EN 300 920 V7.1.1 (2000-08)

GSM 03.20 Version 8.0.0, 1999. *Digital cellular telecommunications system (Phase 2+) (GSM); Security related network functions*. ETSI TS 100 929.

Hall, J.W., 2000. *Handbook of Otoacoustic Emissions*. San Diego, CA: Singular Thomson Learning. ISBN: 1565938739

Harrington, V., Mayhew, P., 2001. *Mobile Phone Theft* [online]. Home Office Research Study 235, Development and Statistics Directorate. Available from: <http://www.homeoffice.gov.uk/rds/pdfs/hors235.pdf> [Accessed Dec. 2005].

Herschel, W., 1858. In: The Remains of Tomorrows Past: Speculations on the Antiquity of New Media Practice in South Asia. *ISEA2004: 12th international symposium on electronic art. 14-22 Aug. 2004. Helsinki, Finland.* ISBN 9529943903. Available from: <http://www.isea2004.net/content/allpres.php> [Accessed Nov. 2005].

Herzberg, A., Krawczyk, H. and Tsudik, G., 1994. On Travelling Incognito. *IEEE Workshop on Mobile Computing Systems and Applications, 8-9 Dec. 1994. Santa Cruz, CA*. pp.205-211.

Home Office, 2006. *Identity theft, don't become a victim* [online]. Home Office Identity Fraud Steering Committee. Available from: <http://www.identity-theft.org.uk/> [Accessed Jan. 2006].

Hoogstrate, A.J., van den Heuvel, H., Huyben, E., 2001. Ear Identification based on Surveillance Camera Images. *Science & Justice - journal of the Forensic Science Society*, pISSN: 1355-0306, Jul-Sept 2001. Vol.41(3), pp.167-172.

Hornak, J.P., 2006. *The Basics of MRI* [online]. Rochester Institute of Technology (Chemistry and Imaging Science). Available from: <http://www.cis.rit.edu/htbooks/mri/index.html> [Accessed Oct. 2005].

Iannarelli, A.V., 1964. *The Iannarelli system of Ear Identification*. 1st ed. New York: Brooklyn Foundation Press. Reprinted 1989: *Ear Identification*. Freemont, CA: Paramont Publishing Company. ISBN: 0962317802.

IBG, 2004. *Biometrics Market and Industry Report 2004-2008*. International Biometrics Group, 4th Mar. 2004. Available: <http://www.biometricgroup.com/press_releases/pr_2004_%20Biometrics%20MIR.html> [Accessed Jan. 2005]. Update: *Biometrics Market and Industry Report 2006-2010*. Available from: <http://www.biometric group.com/press_releases/pr_2006_BMIR _2010.htm> [Accessed Jan. 2006].

IEE IP, 2005a. Public trust in Internet at lowest level. *Information Professional* (Journal of the IEE), April/May, pp.10.

IEE IP, 2005b. Report calls ID card system into question. *Information Professional* (Journal of the IEE), April/May, pp.3.

ISO/IEC JTC1/SC37, 2004. *Biometric Vocabulary Corpus*. International Biometrics Standards Sub-Committee: SC37. (ISO/IEC JTC1/SC37/WG1 N0456).

ITU, 2001. *Enhanced IMT-2000 specifications for improved data performance approved and technical framework for global circulation of terminals agreed in Tokyo* [online]. ITU Press, 25th Oct. 2001. Available from: <http://www.itu.int/newsarchive/press_releases/2001/20.html> [Accessed Oct. 2002].

Jobusch, D.L. and Oldehoeft, A.E., 1989. Survey of Password Mechanisms: Weaknesses and Potential Improvements. *Computers & Security*, Vol. 8, No. 7, pp.587-604.

Joyce, R. and Gupta, G., 1990. Identity Authentication Based on Keystroke Latencies. *Communications of the ACM*, Feb. 1990. Volume 33(2), pp.168-176.

Juniper Research, 2002. MMS revenues to reach US$8.3 billion by 2004 (Juniper Research). *The Mobile Internet*, Dec. 2002. Available from: <http://www.find articles.com/p/articles/mi_m0NZB/is_12_4/ai_97731235> [Accessed Feb. 2004].

Kaspersky, E., 2006. *Kaspersky boss explodes security myths* [online]. silicon.com. Available from: <http://software.silicon.com/malware/0,3800003100,39155837,00.htm> [Accessed Jan. 2006].

Konstantinos, N.Y., 1997. *Applications of Biometrics & Implications for Security and Ethics* (Shearson-Hamill, Wall Street, 1968), University of Illinois at Urbana-Champaign, 13th Nov. 1997. Available from: <http://www.staff.uiuc.edu/~efantis/biometrics/sld001.htm> [Accessed Jan. 2005].

Legget, J. and Williams, G., 1988. Verifying identity via keystroke characteristics. *International Journal of Man-Machine Studies*, No.28, pp.67-76.

Lemos, R., 2003. *Cracking Windows passwords in seconds* [online]. CNET News, Jul. 2003. Available from: < http://news.zdnet.com/2100-1009_22-5053063.html> [Accessed May 2005].

Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S., 2003. *Handbook of Fingerprint Recognition*. New York: Springer. ISBN: 0387954317. Available from: <http://bias.csr.unibo.it/maltoni/handbook/> [Accessed Jan. 2006].

MET, 1901. *Fingerprint Bureau* [online]. Metropolitan Police Service - Historical Timeline. Available from: <http://www.met.police.uk/history/fingerprints.htm> [Accessed Oct. 2005].

Miller, S., 2001. *Mobile sales soar, driven by teenage market* [online]. MediaGuardian, 23rd May 2001. Available from: <http://media.guardian.co.uk/newmedia/story/0,7496,495263,00.html> [Accessed May 2002].

MIT Tech, 2003. *10 Emerging Technologies That Will Change the World* [online]. Technology Review - An MIT Enterprise, Feb. 2003. Available from: <http://www.gapoptic.unige.ch/HomeExtras/MIT/10%20Emerging%20Technologies%20That%20Will%20Change%20the%20World.htm> [Accessed Nov. 2005].

Modisette, L., 1999. State-of-the-Art in Preventative Fraud Systems. *The 1999 GSM World Congress (Day 2), 23-25 Feb. 1999, Cannes, France.*

Moenssens, A., 1971. *Fingerprint Techniques* (Inbau law enforcement series). Chilton Book Co. ISBN: 0801955270.

Morgan, J., 1999. *Court Holds Ear-print Identification Not Generally Accepted In The Scientific Community* [online]. Forensic-Evidence.com. In: STATE v. David Wayne KUNZE, Court of Appeals of Washington, Division 2. 97 Wash.App. 832, 988 P.2d 977 (1999). Available from: <http://www.forensic-evidence.com/site/ID/ID_Kunze.html> [Accessed Feb. 2005].

Nanavati, S., Thieme, M., Nanavati, R., 2002. *Biometrics - Identity Verification in a Networked World.* New York: John Wiley & Sons. ISBN: 0471099457.

National Mobile Phone Crime Unit (NMPCU), 2003. A new weapon to combat phone theft, *The Job* [online], Vol.36. Available from: <http://www.met.police.uk/job/job919/live_files/2.htm> [Accessed Dec. 2003].

Newmann, J., 1997. *Improved measurement techniques for otoacoustic emissions.* Thesis (PhD). Universität Oldenburg. Available from: <http://www.bis.uni-oldenburg.de/bisverlag/neurec97/inhalt.html> [Accessed Nov. 2005].

Nortel, 2005. *HSDPA Trials Pick Up Speed* [online]. Wireless Week, Feb. 2005. Available from: <http://www.wirelessweek.com/article/CA503596.html?space desc =Departments> [Accessed May 2005].

Norton, R.E., 2002. *The Implications and Challenges of Integrating Biometric Technology into Day-to-Day Immigration and Security Policy* [online]. The International Biometric Industry Association, 7th May, 2004. Available from: <http://www.ibia.org/aboutibia/newsletter_detail.asp?id=28> [Accessed Jan. 2005].

NTT DoCoMo, 2004. *DoCoMo's Newest 505i Handset Features Fingerprint Authentication* [online]. NTT DoCoMo, 9th Jul. 2003. Available from: <http://www.nttdocomo.com/presscenter/pressreleases/press/pressrelease.html?param%5Bno%5D=257> [Accessed Dec. 2004].

Open Mobile Alliance (WAP Forum), 2005. *Material from Affiliates – Wireless Application Protocol* [online]. OMA. Available from: <http://www.openmobile alliance.org/tech/affiliates/wap/wapindex.html#wap20> [Accessed Dec. 2005].

Philips, 1985. *The predecessor of the CD* [online]. Philips Research. Available from: <http://www.research.philips.com> [Accessed May 2005].

Polemi, D., 1997. *Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Most Applicable Areas*. European Commission DG XIII-C.4 on the Information Society Technologies (IST) (Key action 2: New Methods of Work and Electronic Commerce). Available from: <www.cordis.lu/infosec/src/stud5fr.html> [Accessed Jan. 2005].

Porras, P.A. and Neumann, P.G., 1997. EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances. *20th National Information Systems Security Conference, 7-10 Oct. 1997, Baltimore, Maryland, USA.*

Ratha, N.K., Connell, J.H., Bolle, R.M., 2001a. Enhancing security and privacy in biometrics-based authentication systems [online]. *IBM Systems Journal*, Vol.40, No.3. Available from: <http://www.research.ibm.com/journal/sj/403/ratha.pdf> [Accessed Apr. 2003].

Ratha, N.K., Connell, J.H., Bolle, R.M., 2001b. An analysis of minutiae matching strength. *Third International Conference on Audio- and Video-Based Biometric Person Authentication, 6-8 Jun. 2001, Halmstad, Sweden, pp. 223-228*. Available: <http://www.research.ibm.com/ecvg/pubs/ratha-strength.pdf> [Accessed Jun. 2002]

Richardson, K., 2000. UMTS Overview. *Electronics Communications Engineering Journal*, Vol.12, No.3, pp.100.

Rodwell, P., 2001. *Determining Identity of a User*. UK Patent Application GB 2375205 A 06.11.2002. US Patent Application 10/476,588 31.10.2003.

Rodwell, P. and Clarke, N., 2002. *Assessing Subscribers' Attitudes towards Mobile Services and Security* [online]. Network Research Group, University of Plymouth. Available from: <http://www.network-research-group.org> [Accessed Dec. 2003].

Rogers, J., 2001. *Data Mining Fights Fraud* [online]. Computer Weekly, 8th Feb. 2001. Available from: <http://www.computerweekly.com/Articles/2001/02/08/178302/ Dataminingfightsfraud.htm#ContentContinues> [Accessed Apr. 2003].

Rosenblatt, F., 1958. The Perceptron: A Probabilistic Model for Information Storage & Organisation in the Brain. *Psychological Review*. Vol. 65(6), pp.386-408.

Sagan C., 1978. The Quest for Extraterrestrial Intelligence. *Smithsonian*, May 1978. Available from: <http://www.bigear.org/vol1no2/sagan.htm> [Accessed Mar. 2005]

Sagem, 2000. *SAGEM points a finger at GSM* [online]. SAGEM, 24th Jan. 2000. Available from: < http://www.sagem.com/en/communiques-en/cp-1sem2000-en.htm - mc 959 id empreinte> [Accessed Feb. 2001].

Sharma, D.C., 2005. *PC sales growth to slow in 2006* [online]. CNET News, Dec. 2005. Available from: <http://news.zdnet.co.uk/hardware/mobile/0,39020360,39243156, 00.htm> [Accessed Dec. 2005].

Smith, R.E., 2002. *Authentication - From Passwords to Public Keys*. Addison-Wesley Professional. ISBN: 0201615991.

Squires, M., 2001. Interview. In: *The Mobile* [Documentary]. TV, Channel 5. Transmitted: 27th May 2001.

UMTS Forum, 2003. *Mobile Evolution - Shaping the Future*. UMTS Forum, Aug. 2003. Available from: <http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/ umts/Resources_Papers_index> [Accessed Mar. 2005].

UMTS Forum, 2005. *3G/UMTS subscribers hit 16 million, confirms UMTS Forum* [online]. UMTS Forum, Jan. 2005. Available from: < http://www.umts-forum.org/ servlet/dycon/ztumts/umts/Live/en/umts/News_PR_Article050105> [Accessed Jan. 2006].

VisionGain, 2005. *3G and Wireless Data Services: Market Analysis and Forecasts 2005-2010* [online]. MarketResearch, Jan. 2005. Available from: <http://www.market research.com/product/display.asp?productid=1118851&g=1> [Accessed Jan. 2006].

vnunet, 2000. *How to sell mobile computing - part 4* [online]. vnunet, Aug. 2000. Available from: < http://www.vnunet.com/vnunet/features/2129789/sell-mobile-computing-part> [Accessed Mar. 2005].

W2F, 2004. *UK Wireless Statistics, 2004-2006* [online]. W2Forum, Apr. 2004. Available from: <http://www.hottelecom.com/w2f-uk-mobile-statistics.html> [Accessed Feb.2005].

Washington Technology, 1996. *High-Tech Security Firms Have Summer Games Covered* [online]. Washington Technology, Vol.11(7), 7th Nov. 1996. Available from: < http://www.washingtontechnology.com/news/11_7/news/10086-1.html> [Accessed Oct. 2005].

Watson, A., 2001. *Standardise This* [online]. In: Goldman, J., TheFeature, Jul. 2001. Available from: < http://www.thefeaturearchives.com/12040.html> [Accessed Feb. 2005].

Woodward, J.D. Jr., Orlans, N.M., Higgins, P.T., 2003. *Biometrics – Identity Assurance in the Information Age*, UK: McGraw-Hill Osborne.

Zakaria, T., 2003. *CIA to capture iris recognition at a distance* [online]. (Reuters) News in Science, 5th Nov. 2003. Available from: <http://www.abc.net.au/cgi-bin/ common/printfriendly.pl?/science/news/tech/InnovationRepublish_982770.htm> [Accessed Feb. 2005].

Internet Links

Internet Links

3GPP
- Name: Third Generation Partnership Project.
- Function: Catalyst of telecommunications Standards Bodies.
- Web: http://www.3gpp.org

A4Vision
- Name: A4Vision.
- Function: Provider of 'Vision, Access, Enrolment and Identification' systems.
- Web: http://www.a4vision.com

APWG
- Name: Anti-Phishing Working Group.
- Function: Committed to wiping out Internet scams and fraud.
- Web: http://www.antiphishing.org

BBC Mobile Services
- Name: British Broadcasting Corporation (BBC) Mobile services.
- Function: The BBC on your mobile.
- Web: http://www.bbc.co.uk/mobile

Biomark
- Name: Biomark.
- Function: Specialists in electronic animal identification (tagging).
- Web: http://www.biomark.com

Biometric Consortium
- Name: The Biometric Consortium.
- Function: R&D, evaluation and application of biometric identification technology
- Web: http://www.biometrics.org

BioPassword
- Name: BioPassword Inc. (Issaquah, Washington).
- Function: Biometric password enforcement software.
- Web: http://www.biopassword.com

Bluetooth
- Name: Bluetooth
- Function: The official Bluetooth website.
- Web: http://www.bluetooth.com

CCCN
- Name: Centre for Cognitive and Computational Neuroscience, Department of Computing and Mathematics, University of Stirling.
- Function: Overview of neural-networks.
- Web: http://nevis.stir.ac.uk

CompTIA
Name: Computing Technology Industry Association.
Function: Dedicated to advancing the growth of the IT industry.
Web: http://www.comptia.org

Disney
Name: The Walt Disney Company.
Function: Entertainment specialists in studios, parks and media, since 1923.
Web: http://www.disney.com

DuPont Authentication Systems
Name: Dupont Authentication Systems.
Function: Provider of authentication security solutions: IZON™ technology.
Web: http://www.dupontauthentication.com

ETSI
Name: The European Telecommunications Standards Institute (France).
Function: Information and Communication Technology (ICT) standards in Europe.
Web: http://www.etsi.org

GSM Association
Name: GSM Association.
Function: Annual Reports
Web: http://www.gsmworld.com

Home Office (Identity Fraud)
Name: The Home Office.
Function: Home Office Identity Fraud Steering Committee.
Web: http://www.identity-theft.org.uk

iAfB/ICSA
Name: International Association for Biometrics (iAfB)
International Computer Security Association (ICSA).
Function: Glossary of Biometric Terms (1999).
Web: http://www.iafb.org.uk/docs/glossary.htm

IBG
Name: International Biometrics Group.
Function: Biometrics leading consulting and technology services, since 1996.
Web: http://www.biometricgroup.com

ISIS(a)
Name: Image Speech and Intelligent Systems Research Group.
Function: Automatic Gait Recognition @ University of Southampton.
Web: http://www.gait.ecs.soton.ac.uk

ISIS(b)
Name: Image, Speech and Intelligent Systems Research Group.
Function: Automatic Ear Recognition @ University of Southampton.
Web: http://www.isis.ecs.soton.ac.uk

ISO

Name: International Organization for Standardization.
Function: Network of the national standards institutes of 151 countries.
Web: http://www.iso.org

ITU

Name: International Telecommunications Union.
Function: Telecommunications standards and harmonisation union, since 1865.
Web: http://www.itu.int

Juniper Research

Name: Juniper Research.
Function: Providers of analytical reports and consultancy to the telecoms industry.
Web: http://www.juniperresearch.com

Lavater (German)

Name: Johann Casper Lavater
Function: 19th Century theologian and physiognomist.
Web: http://www.kunsthaus.ch/ausstellungen/2001/lavater

Meucci

Name: Antonio Meucci
Function: 19th Century inventor.
Web: http://www.italianhistorical.org/MeucciStory.htm

MDA

Name: Mobile Data Association
Function: Global association for vendors and users of mobile data.
Web: http://www.mda-mobiledata.org/mda

National Statistics

Name: National Statistics and the Office for National Statistics (ONS).
Function: Home of official UK statistics.
Web: http://www.statistics.gov.uk

NTC

Name: National Training Centre for Scientific Support to Crime Investigation
Function: British police force crime scene investigation unit.
Web: NTC - http://www.forensic-training.police.uk
NTCSSI - http://centrex.police.uk/forensic-training/scientific.html

Nuance Communications Inc.

Name: Nuance Communications Inc.
Function: Providers of voice automation technology, since 1994.
Web: http://www.nuance.com

Orange

Name: Orange™ PCS Ltd.
Function: The principle UK mobile network operator (2003)(Section 3.3.1).
Web: http://www.orange.co.uk

Otoacoustics Emissions
Name: The Otoacoustic Emissions (OAE) Portal Zone.
Function: Information, News and Forum on OAEs.
Web: http://www.otoemissions.org

Persay Inc.
Name: Persay Inc. (Woodbridge NJ), a subsidiary of Converse Technology.
Function: Providers of voice verification technology: FreeSpeech™.
Web: http://persay.com

Recognition Systems Inc.
Name: Recognition Systems Inc. (Ingersoll-Rand Inc.)
Function: Principal supplier of hand geometry products: HandPunch/Handkey®.
Web: http://www.recogsys.com / http://www.handreader.com

Sagan, C.
Name: The Carl Sagan Foundation.
Function: Dedicated to the "planet-wide campaign of public science".
Web: http://www.carlsagan.com

Statistics
Name: Statistics Glossary
Function: Explanation of statistical analyses terms.
Web: http://www.stats.gla.ac.uk/steps/glossary

VeriVoice Inc.
Name: VeriVoice Inc. (Princeton NJ)
Function: Providers of biometric voice verification solutions.
Web: http://www.verivoice.com

Veid Ltd.
Name: Veid Pte. Ltd. (Singapore)
Function: Hand Vascular Pattern Person Identification system: the VP-II.
Web: http://www.veid.net

Vocalist
Name: Vocalist
Function: Dedicated to the world of singers, vocalists and students of the voice.
Web: http://www.vocalist.org.uk

W2F
Name: Wireless World Forum
Function: Online community of 4000 senior professionals in the wireless industry.
Web: http://www.w2forum.com

Wikipedia
Name: Wikipedia
Function: Web-based free-content reference encyclopaedia.
Web: http://en.wikipedia.org/wiki/Wikipedia

Bibliography

Bibliography

Ashbourn, Julian
"Biometrics - Advanced Identity Verification", © Springer, 2000.
ISBN 1-85233-243-3

Baken, R.J.; Orlikoff, R.F.
"Clinical Measurement of Speech and Voice (Speech Science)"
© Singular Publishing, 2nd Edition, 22nd Dec. 1999.
ISBN: 1565938690

Everest, F. Alton
"Master Handbook of Acoustics - Fourth Edition", © McGraw-Hill, 2001.
ISBN 0-07-136097-2

Hagan, Martin T.; Demuth, Howard B.; Beale, Mark
"Neural Network Design", © PWS Publishing, 1996.
ISBN 0-53-494332-2

Hall, James W. III
"Handbook of Auditory Evoked Responses", © Allyn and Bacon, 1992.
ISBN 0-205-13566-8

James, Glyn
"Advanced Modern Engineering Mathematics", © Addison-Wesley, 1993.
ISBN 0-201-56519-6

Maltoni, Davide; Maio, Dario; Jain, Anil K.
"Handbook of Fingerprint Recognition", © Springer, 2003.
ISBN 0-387-95431-7

Smith, Richard E.
"Authentication - From Passwords to Public Keys", © Addison-Wesley, 2002.
ISBN 0-201-61599-1

Nanavati, Samir; Thieme, Michael; Nanavati, Raj
"Biometrics – Identity Verification in a Networked World", © John Wiley & Sons 2002.
ISBN 0-471-09945-7

Woodward, John D. Jr., Orlans, Nicholas M., Higgins, Peter T.
"Biometrics – Identity Assurance in the Information Age", © McGraw-Hill/Osborne, 2003.
ISBN 0-07-222227-1

Appendices

Appendices

Appendix A

Anatomy of the Subscriber Identity Module (SIM)

The anatomy of a typical mobile SIM card (Section 2.3.1)

Appendix A Anatomy of the Subscriber Identity Module (SIM)

The micro controller on a SIM is effectively a complete, albeit very small, computer on a single *potted* chip (Figure A-1), containing all the basic integrated hardware features normally found in a larger desktop or laptop system. It is this fully integrated package that gives a SIM its inherent security.

A SIMs' features include:

- An operating system which can respond to external or internal commands.
- Data storage that can be accessed via the operating system.
- Applications called to perform simple or complex tasks when requested.

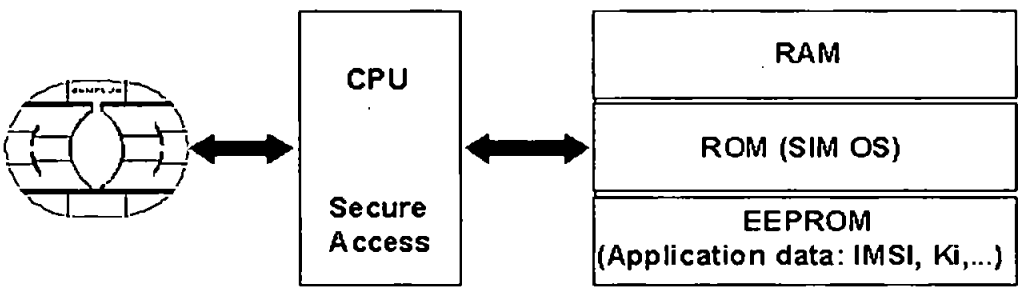


Figure A-1 : Block diagram of a typical SIM

CPU (Typically 8-Bit) – The Central Processing Unit (CPU) is the processing heart of the SIM. Similar to the CPU found in a typical desktop computer, a SIM's CPU performs all required software and data processing. In stark contrast to a desktop computer system however, the CPU is typically only an 8-Bit[1], low performance, low power drain device.

[1] Desktop computer CPUs circa 2004/5 were predominantly 32-bit, with 64-bit available for power users.

RAM (Typically 256Bytes) - Unlike a conventional computer, the RAM is extremely limited in a smart card, usually amounting to only a few hundred bytes. This memory is used for functions, such as program variables, stack values and pointers, and in particular, the input/output buffer memory.

ROM (Typically 16K) - The ROM section contains the SIM card operating system. This is Masked ROM, which unlike conventional ROM that is programmed electrically with the operating system, is programmed during the wafer manufacture. This means that the code is processed into the silicon forming an integral part of the device itself. This mask process means that the code can never be altered, erased or replaced.

EEPROM (Typically 4-16K) - The EEPROM stores data on the card which needs to be permanent, it is analogous to the hard disk on a computer, except considerably smaller.

Input/Output function - The I/O is the system by which the SIM communicates with the ME. The operating system uses a serial simplex protocol called T=0, which is an international standard specified by ISO.

Control Logic - The control logic implements of functions associated with the low layer systems, such as memory management and security. Some of the SIM's security measures are hardware implemented, such as clock and voltage tamper detectors. These stop an attack on the device by shutting down the SIM if monitored values stray outside tolerances i.e. additional CPU clock cycle detection due to unexpected coding instructions or additional battery loading due to hardware modification.

Data Stored on the SIM

The data stored on the SIM is stored in 'elementary files', which are arranged in 'directory files' much like the DOS file system found on a standard PC. The operating system can select an elementary file, and then perform commands upon that file. For each individual file, access conditions can be set when the card is personalised. These access conditions determine if an action can be performed.

GSM Data

The GSM data stored on the SIM card is used by the network operator to check the identity of the subscriber and where they within the network. The SIM contains: an International Mobile Subscriber Identity (IMSI); a Temporary Mobile Subscriber Identifier (TMSI), used to identify the subscriber to the system; secret keys for authentication and encryption. The IMSI & TMSI are completely independent to the IMEI. Using these keys, the network can authenticate who you are, or at least who the SIM is registered to. If authentication fails, then the subscriber is denied access to the network (Section 2.3.4). For security, the SIM also stores the current mobile cell identifier each time it is activated.

User Data

The SIM is able to store information for the user, such as phonebook data, short message data (SMS). In fact, the bulk of the EEPROM is used to store datafields required for user data. The network operator does however have some control over the size of the available user data. With flexible partitioning it is possible, for example, to limit the available phonebook to 100 entries in order to utilise some of the SIMs memory space to add operator specific customisation.

Appendix B

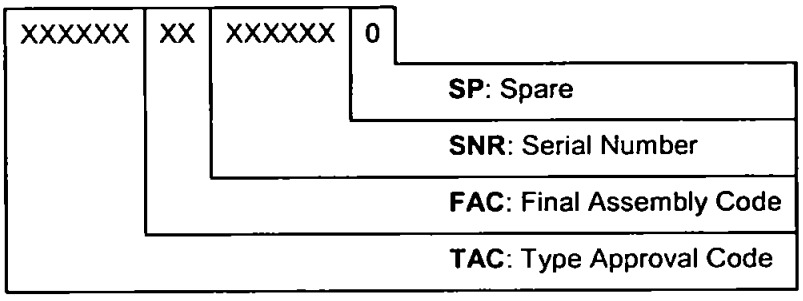
A Breakdown of the IMEI Code

A breakdown of the mobile handset IMEI code (Section 2.3.2)

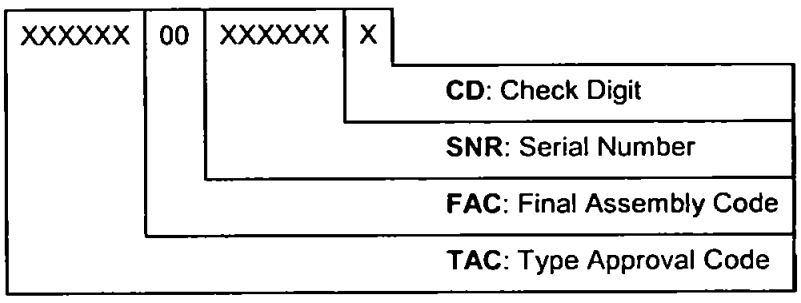
Appendix B A Breakdown of the IMEI Code

The IMEI has undergone some evolutionary changes since its introduction in 1992; the three figures below represent the three possible variations of the IMEI, dependant on the manufacturing date of the mobile handset (Figure A-2).

Prior to 01.01.2003 (phase 1)



Between 01.01.2003 and 01.04.2004 (Phase 2)



After 01.04.2004 (Phase 2+)

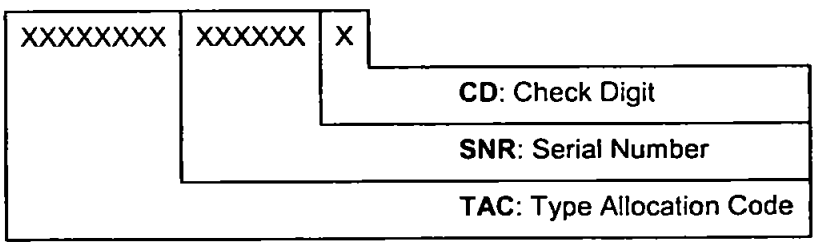


Figure A-2: The code variations of the IMEI

- **TAC** - Type Approval/Allocation Code

  The first two-digits (all phases) identify the IMEI reporting body and the remaining digits, are the Type Identifier defined by the reporting body

- **FAC - Final Assembly Code**

  Up until 31.12.2002, the FAC identified the manufacturing facility where the handset was assembled, as shown in Table A-1.

07, 40	Motorola
10, 20	Nokia
30	Ericsson
40, 41, 44	Siemens
50	Bosch
51	Sony Ericsson
60	Alcatel
70	Sagem
80	Philips
85	Panasonic

Table A-1 : IMEI Final Assembly Codes (FAC)

- **SNR – Serial Number**

  A unique product serial number

- **SP – Spare**

  The SP is an additional spare digit, usually set to zero.

- **CD – Check Digit**

  The CD is a single digit dependent on the value of the preceding 14 digits.

Appendix C

Mobile Phone Security Survey

A copy of the questions asked as part of the security survey covered in Chapter 3

Appendix C Mobile Phone Security Survey

Section 1 of 4 - About You!

Q1. What Gender are you?

Male	☐
Female	☐

Q2. To which age group do you belong?

Under 16	☐
17 - 24	☐
25 - 34	☐
35 - 44	☐
45 - 54	☐
55 - 64	☐
Over 65	☐

Q3. Are you an employee/student at the university of Plymouth?

Yes	☐
No	☐

Section 2 of 4 - Services

Q1. To which network provider do you subscribe?

O^2 (BT Cellnet)	☐
Orange	☐
T-Mobile (One2one)	☐
Virgin	☐
Vodafone	☐
Other	☐

Q2. How do you pay for your phone calls?

Contract	☐
Pre-pay	☐

Q3. Who is the manufacturer of your current mobile phone?

Bosche	☐
Ericsson	☐
Motorola	☐
Nokia	☐
Samsung	☐
Siemens	☐
Sony	☐

Q4. When choosing your network operator, please rank the considerations below in order of importance to you.

	Low	Medium	High
Choice of handset	☐	☐	☐
Network coverage	☐	☐	☐
Operator loyalty	☐	☐	☐
Prices, deals etc.	☐	☐	☐
Reliability	☐	☐	☐
Security features	☐	☐	☐

Q5. When selecting your handset, please rank the considerations below in order of importance to you.

	Low	Medium	High
Accessories	☐	☐	☐
Battery life	☐	☐	☐
Brand loyalty	☐	☐	☐
Games	☐	☐	☐
Connectivity	☐	☐	☐
Security features	☐	☐	☐
Swappable facias	☐	☐	☐

Q6. Approximately, how many hours a day is your phone switched on?

< 1	☐
2 - 5	☐
6 – 10	☐
> 10	☐

Q7. Approximately, how many times in a typical day is your phone used?

	0 - 1	2 - 5	6 - 10	> 10
Voice calls	☐	☐	☐	☐
Data services (SMS, etc)	☐	☐	☐	☐
Features (Games, etc.)	☐	☐	☐	☐

Q8. Please indicate which services you use on your mobile phone.

	Yes	No	Not Available
Voice	☐	☐	☐
Text messages (SMS)	☐	☐	☐
Information services	☐	☐	☐
WAP	☐	☐	☐
Email	☐	☐	☐
International roaming	☐	☐	☐

Q9. Please indicate any additional services you would like to see on a mobile phone in the future.

	Yes	No
Video conferencing	☐	☐
Ecommerce	☐	☐
Personal organiser	☐	☐
Music download	☐	☐
Video on demand	☐	☐
Multimedia message (MMS)	☐	☐
GPS location services	☐	☐
Other		

Section 3 of 4 - Security

Q1. Please indicate which of these following statements applies to you?

Note: The use of the term 'calls' in the following question includes all forms of communications; voice, text, WAP etc.

My mobile phone has:	Yes	No
- been borrowed and tampered with.	☐	☐
- been borrowed and calls made.	☐	☐
- been stolen and NO calls made.	☐	☐
- never been stolen or abused.	☐	☐

Q2. Are you aware of the existence of the international mobile equipment identifier (IMEI) of your handset?

Yes	☐
No	☐

Q3. Do you use any of the personal identification number (PIN) authentication facilities on your mobile phone?

Yes	☐
No	☐
What is a PIN	☐

If yes, please indicate which facilities you use.

	Yes	No	Not Available	Not Applicable
PIN @ switch-on	☐	☐	☐	☐
PIN keypad lock	☐	☐	☐	☐
Other PIN options	☐	☐	☐	☐

Q4. How often do you change ANY of your mobile phone PIN's?

Not applicable	☐
Never	☐
Initially at purchase	☐
Monthly	☐
Yearly	☐

Q5. How do you consider PIN authentication?

Convenient	☐
Inconvenient	☐

Q6. How do you feel generally about the protection the PIN provides against mobile phone misuse?

Very confident	☐
Confident	☐
Adequate	☐
Inadequate	☐
Indifferent	☐

Q7. Have you ever had to use the pin unlock code (PUK) on your mobile phone, because you have forgot your PIN?

Yes	☐
No	☐

Q8. Do you use the same PIN for multiple services, such as your mobile phone, bank cards, PC Access etc?

Yes	☐
No	☐

Q9. Do you think, in principle, additional mobile phone security is:

A good idea	☐
A bad idea	☐
Indifferent	☐

Note: Biometrics is the measurement of unique personal characteristics (e.g. Fingerprints, Voice Recognition & Hand Geometry)

Q10. How do you feel about biometric authentication in general?

A good idea	☐
A bad idea	☐
Indifferent	☐

Q11. Please indicate in the table below which of the following methods of security authentication are you aware of & which you would consider using on a mobile phone?

Security Technique	Aware of?		Would use?	
	Yes	No	Yes	No
Finger Print	☐	☐	☐	☐
Voice Print	☐	☐	☐	☐
Hand Geometry	☐	☐	☐	☐
Facial Recognition	☐	☐	☐	☐
Iris Scanning	☐	☐	☐	☐
Typing Style	☐	☐	☐	☐

Q12. How would you feel about your mobile phone continuously and transparently authenticating who is using it?

A good idea	☐
A bad idea	☐
Indifferent	☐

Q13. For any authentication technique to work, a security profile or signature about you has to exist somewhere; where would you prefer this security profile to reside?

A good idea	☐
A bad idea	☐
Indifferent	☐

Section 4 of 4 - General Knowledge

Q1. Which of the following is NOT a UK Network Operator?

Don't know	☐
Nokia	☐
T-Mobile	☐
Orange	☐
Vodafone	☐

Q2. Which of the following is NOT a mobile phone buzzword?

Don't know	☐
3G	☐
ADSL	☐
WAP	☐

Q3. What is the data rate of a standard GSM connection?

Don't know	☐
9.6 Kbps	☐
14.4 Kbps	☐
56 Kbps	☐
64 Kbps	☐

Appendix D

The Resource Interchange File Format (RIFF)

An explanation of the structure and usage of the WAV and RIFF file formats (Section 7.2)

Appendix D The Resource Interchange File Format (RIFF)

The WAVE file format is a subset of the Microsoft RIFF file specification, which can include many different types of data. Although it was originally intended for multimedia files, the specification is open enough to allow almost any form of data to be stored within the file format, and used or ignored as required by programs that can read the format correctly.

RIFF Format

RIFF is a file format for storing many kinds of data, primarily multimedia data like audio and video. It is based on *chunks* and *sub-chunks*. Each chunk has a type, represented by a four-character tag. This chunk type comes first in the file, followed by the size of the chunk, then the contents of the chunk.

The entire RIFF file is a big chunk that contains all the other chunks. The first thing in the contents of the RIFF chunk is the "form type," which describes the overall type of the file's contents. So the structure of a RIFF file looks like this:

Offset	Length	Contents	Note
0000	4 bytes	'R' 'I' 'F' 'F'	
0004	4 bytes	<file length>	32-bit unsigned integer[1]
0008	4 bytes	Form type	4 characters
000C	4 bytes	chunk type	4 characters
0010	4 bytes	chunk length	32-bit unsigned integer[1]
0014		chunk data	
...	...		

[1] All integers are stored in the Intel low-high byte ordering (referred to as "little-endian").

A more detailed description of the RIFF format can be found in the Microsoft Win32 Multimedia API documentation, which is supplied as a Windows Help file with many Windows programming tools such as C++ compilers.

WAVE (wav) File Format

The WAVE file format is a subset of RIFF used for storing digital audio. Its form type is "WAVE", and it requires two kinds of chunks:

- the **fmt** chunk, which describes the sample rate, sample width, etc., and
- the **data** chunk, which contains the actual samples.

WAVE can also contain any other chunk type allowed by RIFF, including LIST chunks, which are used to contain optional kinds of data such as the copyright date, author's name, etc. Chunks can appear in any order.

The WAVE specification supports a number of different compression algorithms. The **format tag** entry in the **fmt** chunk indicates the type of compression used. A value of 1 indicates Pulse Code Modulation (PCM), which is a "straight," or uncompressed encoding of the samples. Values other than 1 indicate some form of compression.

The WAVE format starts with the RIFF header:

Offset	Length	Contents	Note
0000	4 bytes	'R' 'I' 'F' 'F'	RIFF file identifier
0004	4 bytes	<file length>	
0008	4 bytes	'W' 'A' 'V' 'E'	Wave file identifier
...	...		

The **fmt** chunk describes the sample format:

Offset	Length	Contents	Note
0012	4 bytes	'f' 'm' 't'	
0016	4 bytes	0x00000010	Length of fmt data
0020	2 bytes	0x0001	Format tag: 1 = PCM
0022	2 bytes	<channels>	1 = mono, 2 = stereo
0024	4 bytes	<sample rate>	Samples per second
0028	4 bytes	<bytes/second>	sample_rate*block_align
0032	2 bytes	<block align>	channel*bits_per_sample/8
0034	2 bytes	<bits/sample>	8-bit or 16-bit

Finally, the **data** chunk contains the sample data:

Offset	Length	Contents	Note
0036	4 bytes	'd' 'a' 't' 'a'	data chunk
0040	4 bytes	<length of data block>	
0044	? bytes	<sample data>	

Additional Notes

- Sample data must end on an even byte boundary.
- All numeric data fields are in the Intel format of low-high byte ordering.
- 8-bit samples are stored as unsigned bytes (0 to 255).
- 16-bit samples are stored as 2's-complement signed integers (-32768 to 32767).
- For multi-channel data, samples are interleaved between channels, like this:

```
sample 0 - channel 0 (Left)
sample 0 - channel 1 (Right)
sample 1 - channel 0 (Left)
sample 1 - channel 1 (Right)
...
```

Source: The Canonical WAVE File Format (www.timothyweber.org)

Appendix E

An Introduction to Neural Networks

Neural-networks are an integral part of the HAT process discussed in Section 6.2.4

Appendix E An Introduction to Neural Networks

Neural-networks are based on the parallel architecture of animal brains and represent a different paradigm to traditional linear computing. They are particularly suited to the task of pattern recognition within large sets of data, and are therefore particularly suited to analysing the sets of biometric markers produced by HAT. They consist of:

- multiple simple processing elements referred to as neurons[1].
- a high degree of interconnection between neurons.
- adaptive interaction between neurons.
- simple scalar messaging.

Although biological neurons in real brains can have as many as 10,000 inputs, computer-based neural-networks traditionally have many orders of magnitude less than this. The structure for a simple neural-network is shown in the example in Figure A-3, showing a single layer five neuron-network design. HAT utilises a single layer twenty-five input neuron arrangement (Figure 6-15), one neuron for each of the spot-frequencies.

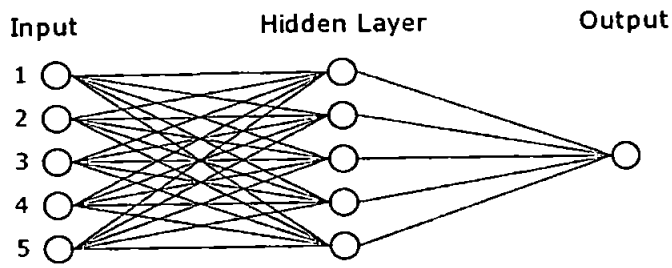


Figure A-3 : A single layer five neuron neural-network

Single Input Neuron

The neuron is the basic building block of a neural-network, and it is in mutual quantity and arrangement that neural-networks gain their processing power. A representation of a single input neuron (aka perceptron, Rosenblatt 1958) is shown in Figure A-4.

[1] The simple processing elements within a neural-network are named after their biological counterparts.

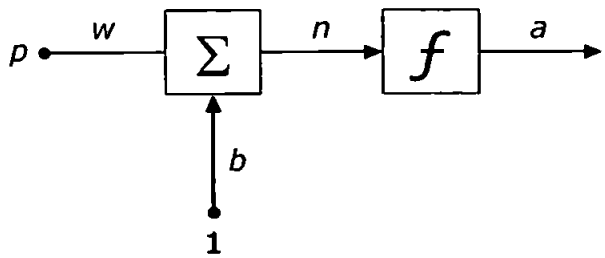


Figure A-4 : A single input neuron

In reference to Figure A-4, the scalar *input* p is multiplied by the scalar *weight* w to form wp; the first input to the summer. The second input, 1 , is multiplied by a *bias*[1] b , forming the second input to the summer. The two input values are summed and outputted as the *net input* n , and passed into the *transfer fuction*[2] f ; which produces the scalar neuron output a. In summary, the neuron output is defined by the equation:

$$a = f(wp + b)$$

Transfer Function(s)

The transfer function (f in Figure A-4) is used to shape the operational envelope of a neurons output and can be either linear ($a = n$) or non-linear ($a = f(n)$) depending on the specific requirements of the neural-network. The three most common transfer functions and their input/output relationships are defined in Table A-2 (non-symmetrical format).

Hard Limit	$a = 0 \quad n < 0$ $a = +1 \quad n \quad 0$	
Saturating Linear	$a = 0 \quad n < 0$ $a = n \quad 0 \quad n \quad 1$ $a = +1 \quad n > 1$	
Log-Sigmoid	$a = \dfrac{1}{1 + e^{-n}}$	

Table A-2 : Table of common neural-network transfer function

[1] The input 'bias' is also sometimes known as the input 'offset'.
[2] The 'transfer function' is also sometimes known as the 'activation function'.

Appendix F

The HAT Demonstration Tool Manual

A complete list of the HAT help files is included as part of the HAT demonstration tool

Appendix F The HAT Demonstration Tool Manual

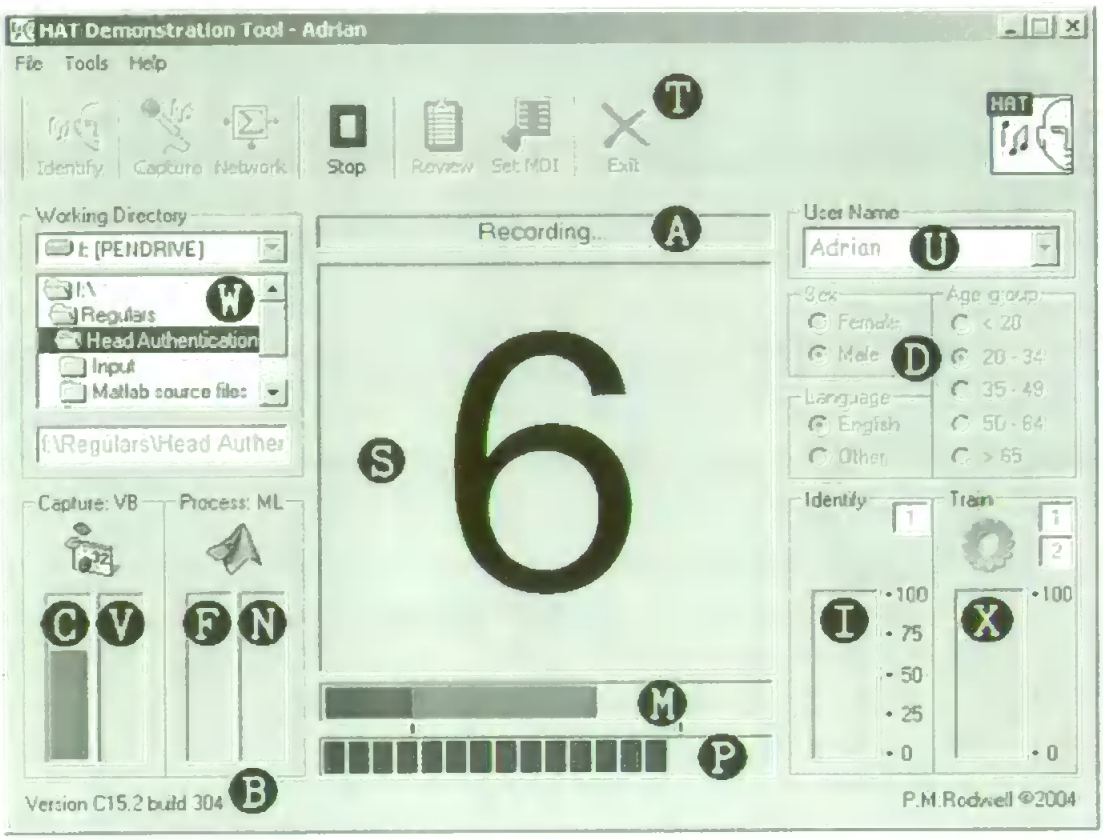
HAT Introduction

The HAT Application is the software element of the HAT demonstration tool. The tool harnesses a novel biometric capture and analysis process to enable the non-intrusive and continuous authentication of users of modern communications systems.

HATs development is part of a PhD into Novel Authentication Systems for Next Generation Mobile Devices, in association with Orange, and the University of Plymouth, Network Research Group

- The Head Authentication Tool GUI is written in Microsoft Visual Basic
- Core functionality, including: Spectral Analysis, Neural Network training and Identification are performed via MathWorks Matlab

The HAT Application Window



T The live main window toolbar provides easy access to all of HATs primary functions; without the need to enter the menus.

W The path to the HAT working directory containing the HAT Application executable and additional HAT resources: HAT.ini etc.

A The HAT activity indicator constantly reports the operational state of the tool.

U A user can either manually enter a new user name for registration, or conveniently select their name from the static pull down list of included HAT trial participants..

D A small selection of the active user's demographic data; also saved as 'user_id.txt' for each user. The 'language' option is the captured language not the user nationality.

Ⓢ The tools central display window is used to prompt the user with example text to speak during a capture cycle, or random text during an authentication cycle.

Ⓒ The HAT capture progress-bar (green) indicates the progress of a HAT Stage-1 Capture, working in tandem with the timing-bar Ⓜ.

Ⓥ The HAT waveform validation progress-bar (yellow) indicates the progress of the amplitude validation cycle performed on each new waveform.

Ⓕ The HAT filter progress-bar (light-blue) indicates the timing of the HAT Stage-2 Filter, HAT Stage-3 Absorption processing loop.

Ⓝ The HAT analysis progress-bar (dark blue) indicates the progress of the HAT Stage-4 Analysis using the HAT neural-network.

Ⓜ The timing-bar is used to prompt the user when to speak during Capture or Identify cycles: 'green' indicates when to speak and 'red' when to wait.

Ⓟ The current operation progress-bar indicates the progress of the complete active operation: for example, the five stages of an authentication cycle.

Ⓘ The identity confidence-bar is used to indicate HATs confidence in the claimed identity of the active user in four steps: 0, 25%, 50, 75% & 100%. Each step increment indicates either a passed or failed authentication cycle.

Ⓧ The auxiliary progress-bar is used to indicate the progress of *en-mass* operations; for example, HAT Stage-4 Analysis of ALL the HAT trial participants

Ⓑ The current HAT Application software build information.

The HAT Processes

Note: For HAT data processing to be performed Matlab must be installed on the system, else an error will occur.

Capture

Capture a new set of wavefiles for an existing user, or a new user.

- The captured wavefiles are based on the contents of the Spoken-text file, in the HAT 'Input' directory.
- HAT will automatically name the wavefiles based on their contents and repetition.
- A completed user directory will contain the following files:

Filename	Purpose
HAT_Spoken.txt	A copy of the spoken-text file used at time of capture
???_id.txt	User Id data & wavefile specifications at time of capture • ??? are the first 3 characters taken from the users name
???_C_##.wav	Captured wavefiles • ??? are the first 3 characters taken from the users name • C is the individual spoken character • ## is the spoken character repetition count
MEa_?.txt	Analysis results • ? is either F'ixed or V'ariable data
MEa_?.mat	Neural-networks (Matlab) • ? is either F'ixed or V'ariable data
Threshold.txt	Neural-network thresholds results

Analysis

Analyse the captured wavefiles according to the HAT rule-set and produce the appropriate MEa analysis data files.

- The analysed wavefiles MEa results are dependent on the frequencies defined in the frequencies resource file, within the HAT 'Input' directory.

Network

Build and Train a Neural-network based on the MEa analysis data files.

- The selected user MEa analysis data is presented to the neural-network as **Good** data, and all other users MEa analysis data is presented as **Bad** data.

Threshold

Calculate the Authentication Threshold, by feeding a second data set into the Neural-network.

- A second data set is presented to the neural-network created using the first data set, and the relevant threshold calculated.

Identify

Authenticate a user against their profile.

- Authentication is based on a result exceeding their own network threshold.
- It may be possible for users to occasionally exceed thresholds other than their own. However, statistically their own threshold will sustain the best results in the long term. The confidence-bar attempts to iron out these anomalies.

HAT Patent

The Head Authentication Tool core functionality is protected under UK Patent

Patent No. GB2375205, 2001 "Determining identity of a user"

- **First Author**
  Philip Rodwell
  Network Research Group
  University of Plymouth UK.

- **Second Author**
  Paul Reynolds
  Orange PCS
  Bristol, UK.

System Requirements

Before installing the Head Authentication Tool, please ensure you have the following:

Hardware

- x86 processor clocking at least:
  - 500MHz for wavefile Capture only
  - 1GHz for Analysis and Networking, including Authentication
- 64 MB of system RAM or more
- Free hard-disk space:
  - 1Mb for HAT application and resources
  - 1.4MB for **each** registered user set
- A soundcard with line-in facility, via 3.5mm jack plug
- The HAT headset (2xLR44 batteries), Pre-amp and 9v Power transformer

Software

- Microsoft Windows 98/Me/NT 4.0/2K/XP
- Mathsoft Matlab v6.1 or later
- Latest version of HAT

Resource files (contained in either the HAT directory or Windows SYSTEM directory)

- MSVBVM60.DLL

  - Microsoft Visual Basic generic controls
- MSCOMCTL.OCX

  - Microsoft Visual Basic custom controls (Toolbar, Tabbed options window)
- RICHTX32.OCX

  - Microsoft Visual Basic Rich-Text Control (Review window)

HAT.ini File

The HAT initialisation file is used to set HATs user definable options at startup.

If the file exists in the HAT application directory, it is loaded at run-time by default, else internal settings will be assumed.

- The file is in fact a plain-text file and can be edited as such.
- HAT.ini is NOT automatically updated with changes made between sessions.

File Syntax

[Working Dir]
working_dir_path = *filepath* (*filepath* = 'HAT Application' directory)

[Operational Modes]
capture_mode = capture_only | capture_analyse | analyse_only
network_mode = network_only | network_threshold | threshold_only

[User]
user_name = *name* (4 chars *name* 15 chars)
user_sex = female | male
user_language = english | other
user_age = *age* (0 < *age* 120)

[Wavefile Format]
wavefile_samplingrate = 11025 | 22050 | 44100
wavefile_bitspersample = 8 | 16

[Wavefile Validation]
validation_mode = full | half | off
validation_amplitude = *amplitude* (0 amplitude 100)
validation_tolerance = *tolerance* (0 *tolerance* 100)
clipping_amplitude = *amplitude* (0 amplitude 100)
clipping_tolerance = *tolerance* (0 *tolerance* 100)

[Spectral Analysis]
filter_ncount = *count* (101 count(odd) 5001)
filter_bandwidth = *bandwidth* (50 *bandwidth* 1000)

[Neural-Network]
network_perfgoal = *goal* (0.001 *goal* 1)
network_epochs = *epochs* (1 *epochs* 10000)

[View Output]
view_waveform = yes | no
view_waveform_axis = yes | no
view_signature = yes | no
view_signature_axis = yes | no
view_bargraph = yes | no
view_bargraph_axis = yes | no

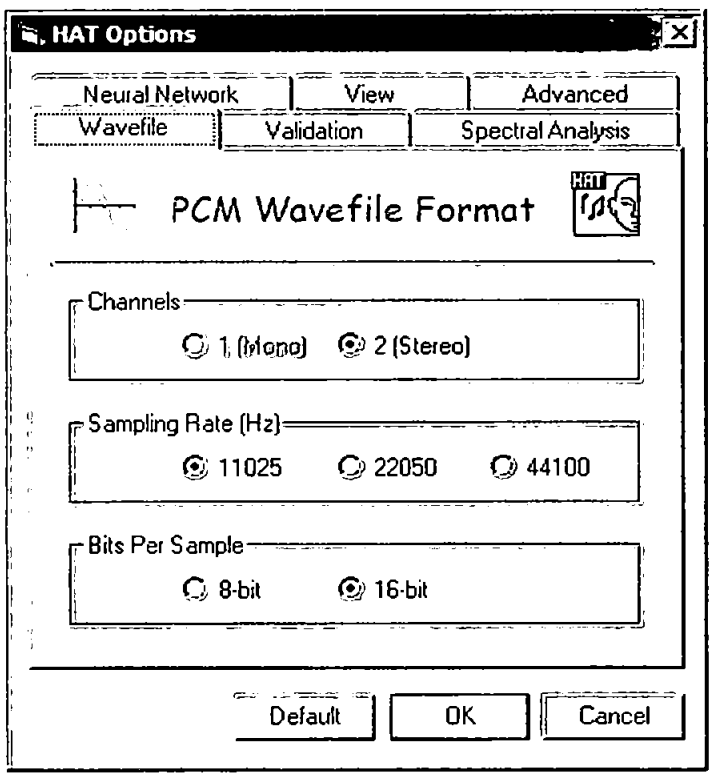
[Advanced Settings]
onscreen_prompts = on | off
process_pauses = short | normal | long

Options

PCM Wavefile Format

The 'Wavefile' tab is used to the set the HAT Stage-1 Capture wavefile parameters.

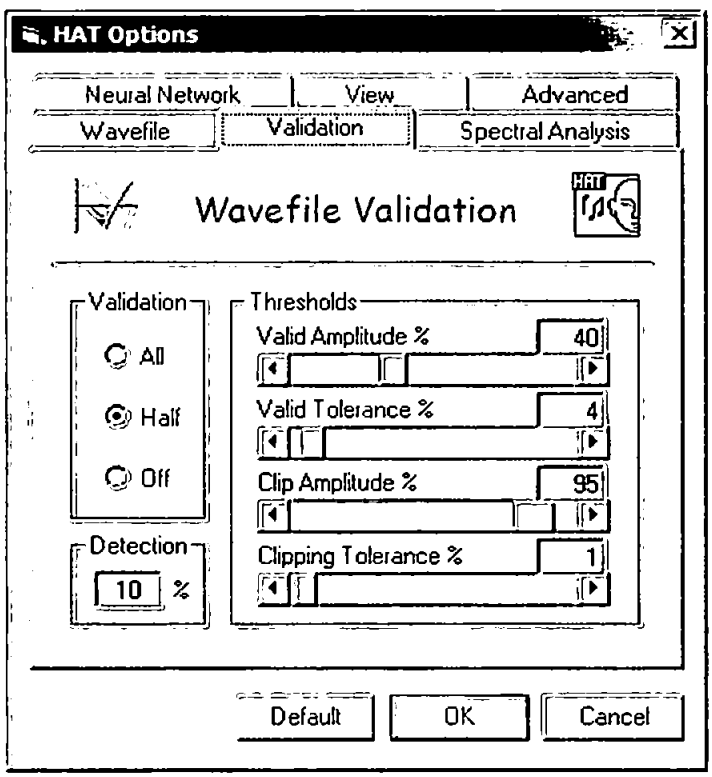
- **Channels**: Number of capture channels (basic HAT locked on 2)
- **Sampling rate**: Wavefile sampling rate
- **Bits-per-sample**: Bit-size of each capture sample



Wavefile Validation

The 'Validation' tab is used to the set the HAT Stage-1 Capture wavefile validation parameters.

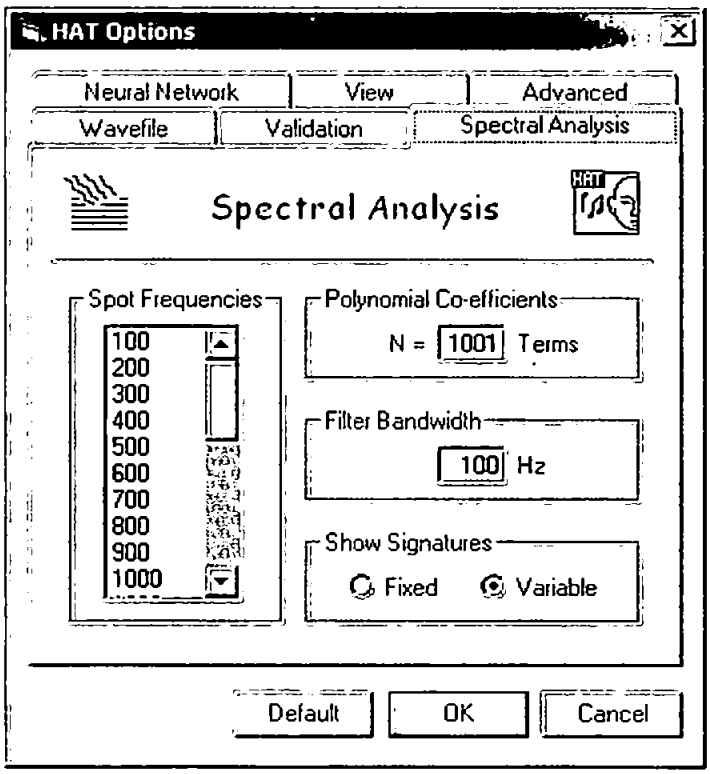
- **Validation**: Number of samples to validate (All | Half | Off) (default = Half)
- **Detection**: Minimum validation detection amplitude (0 → 100%)
- **Valid Amplitude**: Minimum validation amplitude (Detection → Clip Amplitude)
- **Valid Tolerance**: Minimum validation samples (0 → 100%)
- **Clip Amplitude**: Maximum validation amplitude (Valid Amplitude → 100%)
- **Clip Tolerance**: Maximum validation samples (0 → 100%)



Spectral Analysis

The 'Spectral Analysis' tab is used to the set the HAT Stage-2 Filter parameters.

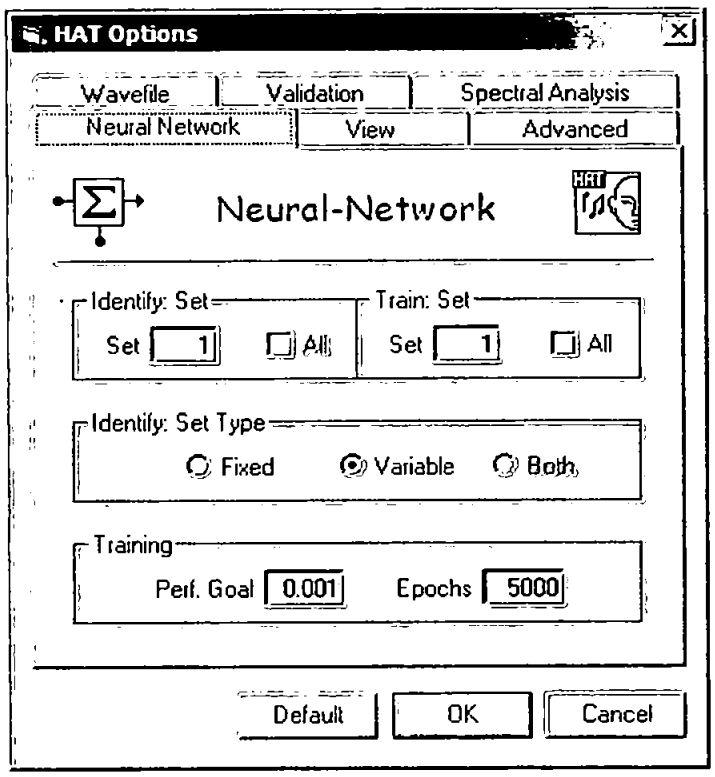
- **Spot Frequencies**: Preset spot-frequency values in Hertz
- **Polynomial Coefficients**: Coefficient count of the filter polynomial (1 → 10001)
- **Filter Bandwidth**: Bandwidth of the filter in Hertz (10 → 1000)Hz
- **Show Signatures**: Select the default capture set format (fixed | variable)



Neural-Network

The 'Neural-Network' tab is primarily used to set the HAT Stage-4 Analysis neural-network training parameters.

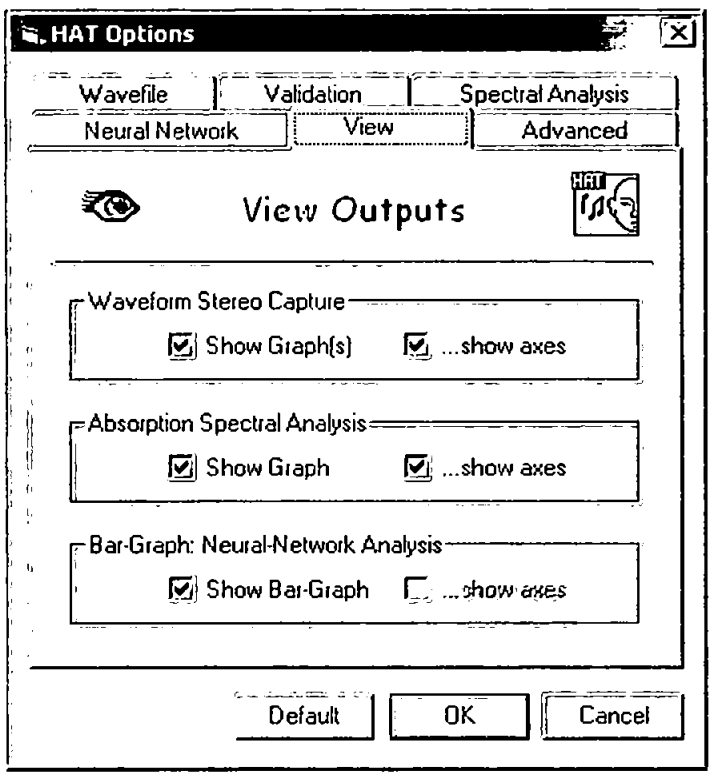
- **Identify-Set**: Default data set to be used for HAT authentication
- **Train-Set**: Default data set to be used for neural network training
- **Set Type**: There are two different captures (Fixed | Variable)
- **Training-Perf. Goal**: Target error-rate whilst training (0.1 → 0.0001)
- **Training-Epochs**: Maximum number of training epochs (1 → 10000)



View Outputs

The 'View' tab is used to set the visibility state of mid-process graphical outputs.

- **Waveform Stereo Capture**: Time-domain plot of the captured waveforms (upon completion of HAT Stage-1 capture)
- **Absorption Spectral Analysis**: HAT absorption template view (upon completion of HAT Stage-2 Filtering / Stage-3 Absorption loop)
- **Neural Network Analysis:** Threshold comparison with all trial participants (upon completion of HAT Stage-4 Analysis)



HAT Development Log (Extracts)

HAT_C15.2 (12.12.2005)

Minor cosmetic changes to reflect the renaming of the tool from the 'Head Authentication Tool' to the 'HAT demonstration tool', including renaming of HAT frames headers: Splash frame, About frame, Patent frame, HAT Properties description

Rename Options > Spectral Analysis – 'Frequency nodes' to 'Spot-frequencies'

Updated, extended and completed HAT Help.

Corrected some minor bugs

HAT_C15.1 (26.10.2004)

Change user-name text box to a combo-box containing HAT registered users names in a pull down list

- entering a registered users name will update the users recorded demography settings from the users ???_id file

Add function headers to all functions

Reverse Development.log layout, with latest updates first

Convert a selection of in-program Help to HTML Help. Initial conversions include:

- HAT.ini Help link
- Capture & Analysis form
- Development Log
- Patent form

(27.10.2004)

Compile the HAT help file using VisualCHM

Add 'Contents...' to the Help menu

Add VB Help API, and implement HTML Help (CHM) for the first time

- Remove form: frmHAT_TrainHelp
- Remove form: frmHAT_IdentifyHelp
- Remove HAT.ini reference from the Help menu and from the code

Remove all Toolbar references to the removed toolbar Help link

Add 'Index...' to the Help menu

(29.10.2004)

Correct inaccurate error reporting in frmHAT_Analysis for error 'File not found' & 'Path not found'

Add crude legend (coloured underlining) to Mean and Standard-Deviation display option

Edit help files, adding: Identify, Network & Threshold, Contacts topics

(01.11.2004)
Block illegal Mode selections when performing en mass operations
Correct visibility timing issue of Network button to match Identify button
Add HAT Process sheet to Help file
(08.11.2004)
VisualCHM v4.3 (currently latest) is proving too unstable and bug ridden, so switching CHM creation to Microsoft HTML Help
Modify capture simulation to mirror current Capture operational Modes
Modify capture simulation output curve to better simulate a real HAT analysis curve, via a simple smoothing algorithm
Code the captured waveform time-domain output graph, set via Tools>Options>View, as part of the wavefile Validation cycle
Change colour allocation to indirect method; ie set operational colours in the header file and not directly in the code
(10.11.2004)
Recode Cmb_UserName_LostFocus to trap empty username field
Delete Cmb_UserName_DblClick function (no longer required), single click auto-selection
Add function: Cmb_UserName_Click, to catch username list selection

HAT_C15.0 (19.10.2004-25.10.2004)
Change tool from identification to authentication at the request of the PhD Director of Studies
Changes include massive reworking of tool, hence new major version number:
- split capture function into four separate functions: Capture, Analyse, Network & Threshold (~30 hours)
- the last user capture set is now performed by a separate function, fnLastSet
- remove Help button from toolbar...will ultimately write separate HTML Help resource
- remove Pause option and all related links...added unecessary complication to the tool whilst offering non-essential functionality
- Add Tools>Build Networks Mode to menus with associated code; works in a similar way to Tools>Capture Mode
- Add operational modes to Review panel
- Add 'ALL' codewords to Review panel
- Add [Operational Modes] to ini file
- Reorder visibility objects in fnSetEnable; create associated Excel spreadsheet to aid development

(26.10.2004)
rework Identify function to work with the NEW thresholds file; for authentication (~6 hours)
- add dblThreshold variable to contain threshold file values (fixed and variable)

rework fnTrainButtonOK to handle user name entry for identification in addition to capture entry, button enable status
- and rename fnTrainButtonOK to fnIdentifyCaptureEnable, to reflect its NEW dual purpose

HAT_C14.8 (09.10.2004)

Planning on making a number of major changes, (4 pages of A4) after a long paper brain storming session one evening

Changes focus on, speeding up the processing time of the tool and further rationalising the forms

- Half validation: Place an option in Tools>Options>Validation to only validate half the samples. As validations sole purpose is to ensure reliable captures, it is acceptable, that validation analysis does not have to be performed on every single sample
- Add Spectral-Analysis filter Tab to Tools>Options, displaying signature nodes, and editable n-count and bandwidth
- Change HAT_Config file to HAT.ini and relocate from C:\ to the application directory, adjust code accordingly
- Change all 'on-screen message' references to 'screen prompt'
- Change the Tools>Validation Tab from text input to text+scroll-bars, and add DetectAmp option

(11.10.08)

Modify main HAT window title bar to include user name when valid, add kHAT constant to header

Add Review form option to Tools menu

Change setup icon to volume icon, to better reflect MDI call

Update HAT.ini handling to include all editable HAT options, extension of (09.10.2004)(4) above

Rebuild the vbMEta.m Matlab module, with some code optimisation

Run some tests on VB, C & Matlab to determine the speed ratings: C is 4x faster than VB which is 6x faster than Matlab

Experiment with building the routine into C with 'mcc -m vbMEta', but resultant code was bloated and NO faster

(12.10.2004)

Change centre frequencies file to minimise filter overlaps; though retaining 25 frequency points

Change n-count default to 1001 from 1301, as reducing the sampling rate (ages ago) reduced the need for the higher figure

Debug...run...debug...run...HAT

(14.10.2004)

Add facility to display the absorption signatures set of the identified user, by clicking the Train icon

Adjust validation so that it only validates the mouth samples, as these are the loudest

Correct a validation bug, where half validation was not stepping correctly through the samples

(18.10.2004)

Add frmHAT_Analysis form, as the displayed analysis data was too small to be of any use

Add point data to display near cursor, when cursor passes over relevent points

How to: Identify

Note: For HAT authentication to be performed, Matlab must be installed on the system, else an error will occur and the Identify process will exit.

Step 1: Select the HAT directory

Locate and select the 'Head Authentication Tool' directory.

- When capturing a new data-set, a temporary sub-directory will automatically be created within the HAT 'Output' directory.

Step 2: Provide training data

In order to be authenticated by the Head Authentication Tool, you must first register yourself with the system.

- Full Capture and Analysis instructions can be found here.
- The more training data you provide, over time, the more accurate the results will become.

Step 3a: Identify yourself

Input a user name.

- User names of at least 4 characters, and no more than 15 characters are allowed.
- The directory name will take the form of the entered user name, and the appropriate set number.
- If the selected user is already registered with the system, HAT will acknowledge this and assign a new data-set number for the existing user.
- If the selected user is a new user, the data-set number will default to 1.

Step 4: Try a simulation

The simulate option within the Help menu precisely mimics a normal Authentication run, and will familiarise you with the Authentication process.

- The simulation will respond appropriately to the relevant Options settings of HAT. Eg. No OnScreen prompts, show signatures etc.

Step 5: The HAT headset

Position the HAT headset correctly on your head

- Ensure there are batteries in the headset plugs: LR44.
- The headset should be positioned with: the ear-piece sitting comfortably over the centre of the ear, and the mouth microphone should be central to the open mouth, though not too close to pick up breathing.

Step 6: When ready, press 'Identify'

Press Identify, and in a normal speaking voice, recite some text during the capture stage of the process.

- Try to time your responses to correspond with the green portion of the timing-bar, below the display.
- Each response will automatically be validated in real-time. Yellow indicators will appear in the timing-bar indicating the main spoken part of the capture.
- HAT will determine the appropriate authentication response and notify the user accordingly.
- Identification requires a complete set of Neural-Network & Threshold data files to be present.

How to: Capture & Analysis

Note: For HAT data Analysis to be performed, Matlab must be installed on the system, else an error will occur.

Step 1: Select the HAT directory

Locate and select the 'Head Authentication Tool' directory.

- When capturing a new data-set, a unique user sub-directory will automatically be created within the HAT 'Output' directory.

Step 2: Select the Capture & Analysis Mode of operation

Via the Tools>Capture Mode menu, select the Capture & Analysis, mode of operation desired.

Step 3a: Identify yourself

Input a user name.

- User names of at least 4 characters, and no more than 15 characters are allowed.
- The directory name will take the form of the entered user name, and the appropriate set number.
- If the selected user is already registered with the system, HAT will acknowledge this and assign a new data-set number for the existing user.
- If the selected user is a new user, the data-set number will default to 1.

Step 3b: User demography

Select the appropriate demographic options. i.e. Sex, Nationality, Age.

Step 4: Try a simulation

The simulate option within the Help menu precisely mimics a normal Capture & Analyse run, and will familiarise you with the Capture & Analyse process.

- The simulation will respond appropriately to the relevant Options settings of HAT. Eg. No OnScreen prompts, show signatures, etc.

Step 5: The HAT headset

Position the HAT headset correctly on your head

- Ensure there are batteries in the headset plugs: LR44.
- The headset should be positioned with: the ear-piece sitting comfortably over the centre of the ear, and the mouth microphone should be central to the open mouth, though not too close to pick up breathing.

Step 6: When ready, press 'Capture'

Press Capture, and in a normal speaking voice, recite each character which appears in the 'text-to-speak' central display.

- Try to time your responses to correspond with the green portion of the timing-bar, below the display.
- Characters will appear in the order they are presented in the spoken-text file.
- Each response will automatically be validated in real-time. Yellow indicators will appear in the timing-bar indicating the main spoken part of the capture.

How to: Network Analysis & Thresholds

Note: For HAT Network and/or Threshold to be performed, Matlab must be installed on the system, else an error will occur.

Step 1: Select the HAT directory

Locate and select the 'Head Authentication Tool' directory.

- When networking a data-set, the source files are located within the HAT 'Output' directory.

Step 2: Provide Capture & Analysis data

In order to build neural-networks, captured data must first have been analysed, and the MEa data files created.

- Full Capture and Analysis instructions can be found here.

Step 3: Select the Network Mode of operation

Via the Tools>Network Mode menu, select the Networking, mode of operation desired.

- For authentication to be performed Network & Threshold are both required, else an error will occur.

Step 4: When ready, press 'Network'

Press Network, and the tool will attempt to build the selected users Neural-network and/or Threshold resources.

- Neural-network creation requires a complete registered users set of Capture & Analysis MEa data files to be present.
- Threshold creation requires a least two complete data sets to be present, one being fed into the other.

How to: *En-Mass* Operations

HAT has been enabled with the facility to perform the primary Analysis and Networking operations *en mass*.

En mass processing:

- will perform the requested operation on ALL registered used autonomously.
- triggers minimal internal delays, reducing individual user processing time by as much as 40%.
- is triggered by entering a case-sensitive codeword as the username before activating the required process.
- will automatically set the valid Mode of operation, blocking any changes until the codeword is removed.
- must be performed in the order shown, as each stage depends on the previous stages results.

Codeword	**Function**
ANALYSE	**Analyse** ALL captured users wavefiles
NETWORK	Build Neural-**Networks** for ALL users
THRESHOLD	Calculate **Thresholds** for ALL users

Contacts

All comments should first be directed to the projects author:

- Mr. Philip Rodwell
  Network Research Group
  University of Plymouth UK.

The authors PhD Director of Studies and Head of the Network Research Group is:

- Dr. Steven Furnell
  Network Research Group
  University of Plymouth UK.

The projects industrial supervisor is:

- Prof. Paul Reynolds
  Orange PCS
  Bristol, UK.

Appendix G

HAT Trials Timetable

A table documenting HAT trials participant's demography and session data (Section 7.3)

Appendix G HAT Trials Timetable

User	User Alias[1]	Sex	Nationality[2]	Session 1		Session 2		Elapsed	Notes[3]
1	u01_Phi	M	English	09.09.2004	14:30	15.09.2004	21:00	6	Mild cold session 2
2	u02_Nit	F	Mauritian	13.09.2004	20:00	15.09.2004	12:00	2	Session 3 - Creole
3	u03_Viv	F	English	11.09.2004	21:00	16.09.2004	20:30	5	
4	u04_Aun	M	Burmese	09.09.2004	17:00	16.09.2004	14:00	7	Session 3 - Burmese
5	u05_Vas	M	Greek	09.09.2004	15:00	14.09.2004	14:45	5	Session 3 - Greek
6	u06_Zak	M	Indian	09.09.2004	16:30	22.09.2004	15:00	13	Session 3 - Hindi
7	u07_Don	F	English	10.09.2004	12:00	14.09.2004	17:00	4	
8	u08_Adr	M	Romanian	09.09.2004	16:15	22.09.2004	15:30	13	
9	u09_Stv	M	English	09.09.2004	17:15	22.09.2004	16:00	13	
10	u10_Pau	M	English	10.09.2004	17:00	14.09.2004	16:45	4	
11	u11_Abd	M	Arabic	09.09.2004	14:45	16.09.2004	12:30	7	Session 3 - Arabic
12	u12_Nat	M	English	09.09.2004	16:00	14.09.2004	14:00	5	
13	u13_Bog	M	Romanian	09.09.2004	16:45	22.09.2004	17:15	13	
14	u14_Shu	M	Malaysian	09.09.2004	14:45	14.09.2004	14:15	5	Session 3 - Malay
15	u15_Ibr	M	Turkish	14.09.2004	10:00	14.09.2004	15:00	0.5	Session 3 - Turkish
16	u16_Fen	F	Greek	22.09.2004	17:00	23.09.2004	16:30	1	
17	u17_Pet	M	English	15.09.2004	20:00	22.09.2004	21:30	7	
18	u18_And	M	English	22.09.2004	16:30	23.09.2004	14:00	1	
19	u19_Sim	F	English	16.09.2004	16:00	24.09.2004	14:30	8	
20	u20_Cja	M	Indonesian	23.09.2004	14:00	24.09.2004	14:00	1	

[1] The HAT Application allocates user aliases according to the entered user name to preserve trial participant's anonymity.
[2] All sessions were recorded in English unless otherwise stated.
[3] Non-English sessions (session 3) were performed immediately after session 2.

Table A-3 : HAT Trial participants' session data

Appendix H

Published Works

Appendix H Published Works

H1 Conference Invited Speaker (Powerpoint)

Communication Fraud Control Association, Spring 2000

Presentation on behalf of Orange PCS.

2–5 May 2000, Crowne Plaza Hotel, The Royal Mile, Edinburgh, Scotland.

"Non-intrusive Security in 3G – UMTS, Subscriber Authentication"

orange

Non-intrusive Security in 3G - UMTS

Subscriber Authentication - an Operators Perspective

Mr. Philip Rodwell
PhD Research Student
University of Plymouth
United Kingdom

Overview

CFCA Spring 2000

- Introduction
- 2G - Security Issues, specifically GSM
- 3G - Authentication Requirements, UMTS
  - Justification of requirements
- Review potential 3G security solutions
- Summary

Introduction

Security provisions within the current GSM network are primarily aimed at secure communications through data encryption and *terminal* authentication via the SIM card.

The proposed services of UMTS demand a more secure subscriber based authentication system in order to protect personal information in the event of masquerade attacks.

GSM Security (2G)

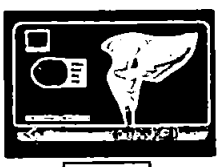
Terminal Authentication

- International Mobile Equipment Identifier (IMEI)
  - In conjunction with the Equipment Identity Register (EIR)
- Subscriber Identity Module (SIM)
  - Subscriber (SIM) authentication (*impersonal*)
    - In conjunction with an Authentication Centre (AuC)
  - Personal Identification Number (PIN) (*Personal*)

GSM Security

The SIM Card

- Subscriber identity module
- Terminal authentication (IMSI)
- Data encryption (cipher key)
- Personal user data
- Unique operator data
- SIM toolkit - e.g. SMS



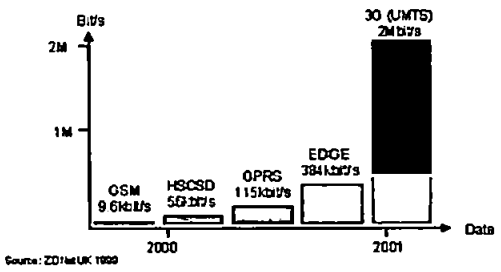
ID-1 SIM

Plug-In SIM

GSM Security
Subscriber Authentication

- ✓ What you have - Token SIM card
- ✓ What you know - Password / PIN
  - ➥ Point-of-entry authentication only
  - ➥ Subscriber intrusive
  - ➥ Relies on transferable knowledge
- ✗ What you are - Physiological signature ?

3G Introduction
The Evolution to 3G

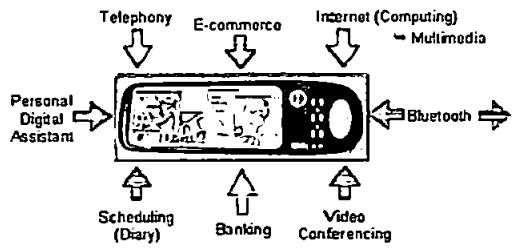


3G Introduction
UMTS

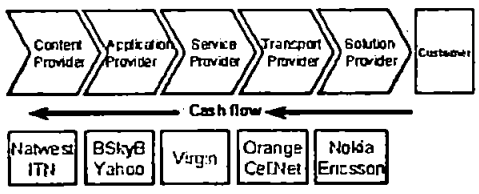
- Universal Mobile Telecommunications System
- Standards Committee: 3G Partnership Projects
  - ➥ UMTS Forum
- A complete global system (Standard)
- Broadband Service - up 2Mbits/s (~400kbit/s)
- 5x 20 year Licences (Total value: £22.47 Billion)*
- Expected introduction date 2001/2

* 27th April 2000

3G = 1G Convergence
UMTS



3G Security Requirements
The Changing Business Model



- Who owns the customer ?
- Each party in the chain needs to know that content is secure

3G Security Requirements
Implications for Operators

- Move from bit-shifter to broker
- Greater responsibility
  - ➥ Content now includes bank details, share portfolios....
- Increased accountability
- Non-repudiation agreements
- Consequential Damages

3G Security Requirements
The Difference is Services

- Mobile Phone → Personal Digital Assistant (PDA)
  - Financial details enabling e-commerce
  - Electronic certificates for digital signatures
  - Full contact details of friends & associates
  - Personal Scheduler (Calendar)
  - Medical details
- A real need for increased access security

3G Security Requirements
Subscriber Authentication

- Preventing against masquerade attacks:
- ✓ What you have - Token SIM card
- ✓ What you know - Password / PIN
- ✓ What you are - Physiological signature
  - Personal (Not Terminal) subscriber authentication
  - Real-time + Point-of-entry authentication
  - Non-Intrusive security techniques
  - Biometric subscriber signaturing

3G Security Requirements
Biometric Authentication Techniques

- Physiological Signaturing
  - ➥ Vision verification *(Facial recognition)* - 2D/3D techniques
  - ➥ Fingerprint / Palmprint
- Behavioural profiling
  - ➥ Voice verification *(Speaker recognition)*
  - ➥ Services profile
  - ➥ System profile

3G Security
A Biometric authentication system

SAGEM MC 959 ID

- Dual-band GSM (900/1800) handset
- Incorporates compact fingerprint reader into the back panel.
- Provides secure authentication for advanced services like e-commerce and mobile banking
- No real need for access PIN

Source : Smart Card 2000 show, London

Authentication Centricity
Terminal-centric

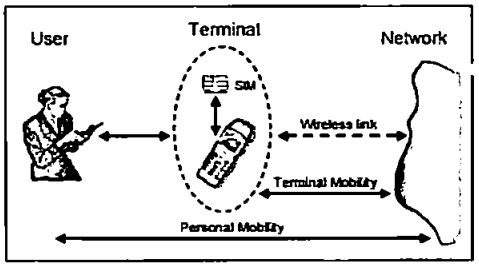
- Inherently insecure ?
  - ➥ Security system held within the terminal SIM
- Signature confidentiality in hands of subscriber
- Potentially fast authentication (better transparency)
  - ➥ Increased Mobile Equipment (ME) CPU usage
  - ➥ Subsequent increase in terminal cost
- Link independent (bandwidth independent)

Authentication Centricity
Network-Centric

- Potential for increased personal mobility
  - ➥ Network holds subscribers personal identifier
  - ➥ Need not carry a network access terminal (subscribers)
- Signature confidentiality in hands of network
- Overhead of increased network traffic
  - ➥ Minimal increase in ME CPU operations
- Link dependent (bandwidth restricted)

2G/3G Authentication

Scope of Mobility



3G Security

Primary Issues for Network Operators

- Dependent on centralisation of solution
- Increased administration
- Increased hardware cost (Mobile Equipment)
  - Larger memory requirements
  - faster CPU's
  - Larger (heavier) batteries
- Biometrics is as much about convenience as security

Summary

UMTS Authentication Requirements

- 2G Authentication Techniques
  - Terminal based (SIM card)
- Need for increased authentication techniques
  - Subscriber rather than terminal authentication
- Based on biometric signaturing and/or profiling
  - Operates in real-time
  - Non-intrusive to the end user
- Network or Terminal based ?

3G Today

Welcome to the 21st Century

- Video Phone
- Internet Access
- e-mail
- e-commerce
- ee-backpain...!

!

the future's bright...
the future's **Orange**

orange

H2 Published Paper

PG-NET 2000

Symposium on the Convergence of Telecommunications, Networking and Broadcasting.

19-20 June, John Moore's University, Liverpool, UK.

"Non-intrusive security requirements for third generation mobile systems"

Non-intrusive security requirements for 3rd generation mobile systems

P.M.Rodwell[†], S.M.Furnell[†] and P.L.Reynolds[‡]

[†] Centre for Communications, Networks and Information Systems, Department of Communication & Electronic Engineering, University of Plymouth, United Kingdom
[‡] Orange Personal Communications Services Ltd, St James Court, Great Park Road, Bradley Stoke, Bristol, United Kingdom

Abstract

The next few years will witness the emergence of third generation mobile technologies, such as the Universal Mobile Telecommunications System (UMTS). The increased bandwidth available will enable the support of significantly wider application scenarios than the voice telephony and basic data services of current networks. This expansion of services will also demand a corresponding increase in the level of protection provided by the devices and network operators. This paper considers the security requirements of UMTS, with particular focus upon subscriber authentication techniques, comparing them against the more basic measures that have been considered satisfactory within second-generation systems such as GSM.

Introduction

The world wide market for mobile telephone technologies has experienced dramatic growth in recent years. Statistics from October 1999 indicated that there were 376.5 million subscribers (with a growth of 52.5% having been experienced in the previous twelve months) and the forecast market by 2003 will exceed one billion (Intekom, 1999). The mobile technologies themselves have already evolved from the voice-only analogue systems of the mid to late 1980s, to the current second generation (2G) systems, introduced in the early 1990s. These systems, based upon digital technology, have enabled mobile data links, albeit at rather limited rates (e.g. 9.6 Kbit/s). Second generation networks are currently being enhanced with a range of data-oriented developments, designed to increase both the capacity of the air interface (e.g. the General Packet Radio Service, GPRS) and the range of mobile data services (e.g. the Wireless Application Protocol, WAP). However, by 2001, it is expected that these technologies will begin to be superseded by third generation (3G) systems such as UMTS, the Universal Mobile Telecommunications System (UMTS Forum, 1998).

UMTS aims to provide a complete, global system and offer a broadband service of up to 2 Mbit/s. This increased capacity will facilitate a fundamental improvement in mobile services, offering the potential for true multimedia capabilities. As such, UMTS is seen as the natural evolutionary path for both subscribers and operators, and a competitive market can already be seen to exist. At the time of writing, the auction of five UMTS licenses in the UK have all attracted bids in excess of £3.5 billion from the network operators (Rushe and Oldfield, 2000).

As service opportunities advance, so to do the requirements to protect subscribers and network operators from the possible effects of fraud and unauthorised use. This paper considers the security requirements for 3G systems, comparing them to the established security practices utilised within 2G networks. Specific requirements are considered from the subscriber perspective, leading to the identification of a requirement for non-intrusive methods that do not impede legitimate activity.

Security in second generation (2G) systems

The most widespread 2G system is the Global System for Mobile Communications (GSM) (Mouly and Pautet, 1992), which, by September 1999, accounted for 344 operational networks across 127 countries (GSM Association, 1999). Security provision in GSM networks is largely geared towards secure communication (i.e. radio interface encryption) and terminal-based authentication. The latter is achieved via the combination of the Subscriber Identity Module (SIM) and the International Mobile Equipment Identifier (IMEI). The SIM holds the subscriber's personal information, such as contact numbers and text messages that have been sent and received. The SIM also contains the International Mobile Subscriber Identity (IMSI), enabling the subscriber to be uniquely identified, irrespective of the handset into which their SIM may be placed. The terminal itself can be uniquely identified via the IMEI number. This can be used in conjunction with the operator's Equipment Identity Register (EIR) database to determine the status of a device. This status will indicate that the terminal is either white-listed (i.e. allowed to access the network), grey-listed (i.e. under observation for possible problems) or black-listed (i.e. not permitted to connect to the network as it has been reported as stolen or is not of an approved type). This provides a good level of access control between the terminal devices themselves and the network.

Relatively little attention is paid to the authentication of the person using the handset or their access to services. Authentication of the subscriber to the terminal is normally achieved via a Personal Identification Number (PIN), which is also held in the SIM. This is a facility that the subscriber must enable on the handset before any protection is provided and, assuming they have done this, the level of protection can still vary between devices. On some systems, the PIN will only be invoked when the handset is first switched on, whereas on others the subscriber also has the option to put the device into a 'locked' state whilst it is still in standby mode (requiring PIN entry before further actions are possible).

Having said this, PIN protection can generally be considered commensurate with the level of risk associated with unauthorised use. Unless the terminal is lost/stolen (in which case the subscriber would be expected to report it and access would be denied by the operator), the window of opportunity for unauthorised use by an impostor who has breached the PIN would be relatively brief, with relatively contained potential consequences.

Requirements for security in third generation (3G) devices

The proposed services of UMTS (Cox, 1997) demand a more secure subscriber-based authentication system in order to protect personal information in the event of masquerade attacks. On a typical second-generation handset, the consequences from theft or impostor access can be broadly grouped into two categories:

- financial loss, as a result of the thief making calls at the legitimate subscriber's expense (depending upon the policy of the operator, these losses may not be passed on to the subscriber once the handset is reported as stolen).
- breach of personal privacy, as a result of the names of the subscribers' contacts and their telephone numbers being held within the SIM card. However, it is acknowledged that this is a fairly limited amount of information, the disclosure of which would not normally be considered highly sensitive. Stored text messages may potentially have more significance, but would not generally represent a significant body of information.

When considering the nature of a 3G device, however, the potential consequences become more severe. The reason for this is that we are likely to witness convergence with Personal Digital Assistant (PDA) type devices and an expansion in the range of possible services that can be accessed. As such, a device might also store:

- financial details to enable mobile commerce payments;
- electronic certificates for digital signatures;
- full contact details of friends and associates;
- miscellaneous information of a commercially sensitive or private nature (e.g. entered into scheduler or notepad applications).

The need for security within UMTS has already been recognised and relevant standards work is progressing in a number of areas, including (3GPP, 2000):

- definition of a UMTS security architecture and specification of underlying elements;
- detailing of security requirements for UMTS service provision (e.g. user access, billing fraud control) and physical network elements (e.g. user identity module, core network and interfaces to non-UMTS networks);
- requirements specification of cryptographic algorithms;
- development of security guidelines.

Aspects such as these will inform the implementation of UMTS networks and services by the international community.

One significant consideration is whether security monitoring should reside within the subscriber's terminal or within the network. Compared to GSM, UMTS does not share the concept of a home network – the 'universal' aspect suggested in the name is based upon roaming between operators to suit the service required. This indicates a need for security to be focused within the handset, as to rely on it within the network will only be as strong as the weakest link (in terms of operators). However, a counter-argument is that UMTS also supports personal mobility, where a subscriber may register with any terminal (fixed or mobile) in order to access services. In this scenario, the subscriber's profile would need to be accessed from the network in order to determine valid services. A terminal-based approach has the advantages that the confidentiality of security details is in the hands of the subscriber, as opposed to being held by the network operator. In addition, authentication and supervision may be performed without imposing any network traffic overhead and independently of link/bandwidth availability. With network-centric monitoring, details would need to be collected on the terminal and then transmitted for remote analysis. A hybrid approach is likely to represent the most appropriate solution.

In addition to terminal and network security, certain services, such as e-commerce, may also incorporate their own security safeguards in addition to the standard facilities within the network and the terminal. This can already be seen to be the case with current e-commerce web sites, which typically require supplementary identification and authentication via their own usernames and passwords before the user is permitted to make purchases.

Non-intrusive security options

Even in 2G systems, PIN codes do not represent an ideal form of subscriber authentication. Their use can be criticised in a similar manner to traditional passwords in desktop IT systems, in that subscribers may introduce vulnerabilities by sharing them with other people or writing them down (Jobusch and Oldehoeft, 1989). In addition, PINs can be considered to be intrusive, as they require specific actions from the subscriber in order to authenticate themselves. Where a subscriber wishes to make a *quick call* or mobile-based transaction, the need to firstly enter a PIN can be a hindrance. As a consequence, many subscribers do not make use of the facility to lock their handsets between transactions (leaving them in a vulnerable state if lost or stolen). Ideally, there is a requirement for non-intrusive or transparent protection measures, such that the provision of security does not unduly interrupt or inconvenience the legitimate subscriber.

One of the stated requirements for secure UMTS service provision is that it should be possible for service providers to "authenticate users at the start of, and during, service delivery" (3GPP, 1999). Authentication *during* service delivery represents a departure from the standard approach of 2G systems and again implies the need for some form of transparent measure to avoid disrupting a subscriber's legitimate activity. Options for achieving this may be related to periodic/continuous supervision of activity, utilising profiling techniques or biometrics.

There is already a significant emphasis upon subscriber profiling in order to counter fraud, with operators applying data analysis techniques to network data in order to identify and flag potentially fraudulent transactions (Modisette, 1999). The same principles could be extended to address user authentication (i.e. to prevent masquerade attacks) and anomaly detection. Profiling could encompass factors such as the types of services typically accessed and the times/durations of access in order to construct a model of the subscriber's normal behaviour. Such techniques have been the focus of work in general IT for some time and have been incorporated into network-based intrusion detection systems (Porras and Neumann, 1997).

The features of 3G terminals that will enable more advanced subscriber services will also offer the potential to facilitate more advanced security options. For example, a number of biometric approaches (Cope, 1990) could conceivably be integrated in a non-intrusive manner, depending upon the nature of the mobile device and the service being accessed. Suitable options include:

- voice verification, for use in traditional voice-telephony scenarios;
- facial-recognition, for videophone applications;
- fingerprint recognition, to detect that the correct person is holding the handset (such a technique already exists the Sagem MC 959 ID handset– see www.sagem.com);
- keystroke analysis, enabling authentication via key interactions (Furnell *et al.*, 1996);
- handwriting recognition, in scenarios where the user may interact via a pen and touch-screen combination.

Such information could be gathered to facilitate real-time identity verification, leading to progressive withdrawal of accessible services (e.g. e-commerce transactions, international call capability) as more potential problems are identified. Anomaly detection could also be based upon current activity, matching overall rules that have been pre-determined to suggest anomalous conditions. Significant departure from a subscriber profile could trigger further levels of response, such as locking the terminal or authentication via a human intermediary (an operator), who could then take the necessary steps to verify the users legitimacy.

It is considered that information such as that listed above could be most usefully handled within a flexible security framework, which is able to intelligently monitor the available characteristics based upon the current activity of the subscriber. For example, voice verification could be utilised during a voice call, but during an e-commerce transaction it could be replaced by other characteristics that are more appropriate to the context, such as keystroke analysis. The monitoring system would determine which characteristics, from those available on the terminal, should be assessed at any given time and then pass on the relevant data for analysis. The analysis itself could be network or terminal-based. However, to avoid traffic overhead (as previously mentioned), the latter approach may be preferable. The terminal could then securely send the results to a network-based monitoring agent for access decisions (the involvement of the network level ensures that the network operator / service provider is kept aware of potential compromise). In this scenario, the network ultimately remains in control of the security and could request re-sampling by the terminal if the authentication results were inconclusive. Such an arrangement is illustrated in figure 1 below. The approach would be non-intrusive in the sense that the terminal user would be unaware of the security system unless compromise is suspected.

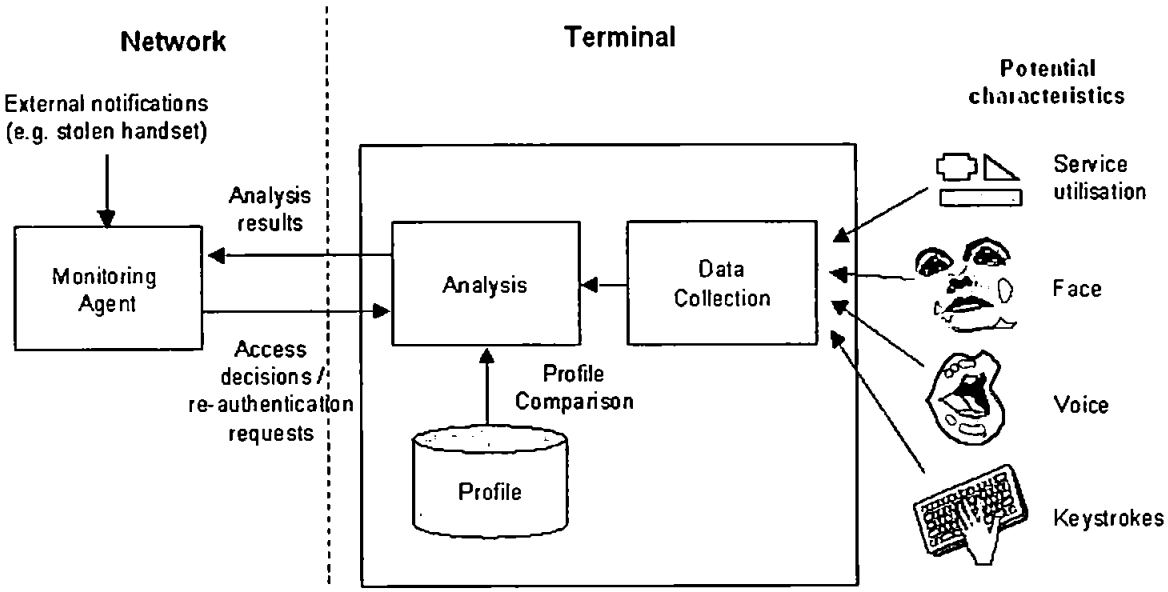


Figure 1: Potential subscriber monitoring scenario

In this scenario, PIN or password-based methods could still be utilised, but would represent a baseline approach, invoked only when other monitoring methods are not able to provide sufficient data for conclusive analysis. The authors are currently in the early stages of a research project addressing these issues.

Conclusions

The capabilities of 3G mobile systems will open up a range of new service opportunities and, as a consequence, will impose new security requirements. This paper has identified the requirement for non-intrusive methods of subscriber authentication and supervision. Further work is required to establish an appropriate monitoring framework and the monitoring methods best suited to mobile application. While biometric systems have been evaluated in the context of desktop IT systems, little work has been conducted to assess their effectiveness in the mobile environment. As such, further research is required to determine whether existing methods can be tailored or, indeed, whether new approaches identified.

References

3GPP. 1999. *3G Security: Security Threats and Requirements*. 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects. Document 3G TS 21.133 version 3.1.0).

3GPP. 2000. *Terms of Reference: Services and System Aspects – Working Group 3*. TSG SA WG3 – Security. http://www.3gpp.org/TSG/ToR/TSG-SA/sa3-tor.htm

3GPP TS 25.855 High Speed Downlink Packet Access (HSDPA); UTRAN description
3GPP TS 25.856 High Speed Downlink Packet Access (HSDPA); Layer 2 and 3 aspects
3GPP TS 25.876 Multiple-Input Multiple-Output Antenna Processing for HSDPA
3GPP TS 25.877 High Speed Downlink Packet Access (HSDPA) - Iub/Iur Protocol Aspects
3GPP TS 25.890 High Speed Downlink Packet Access (HSDPA); User Equipment (UE) radio transmission and reception (FDD)

Cope, B.J.B. 1990. "Biometric Systems of Access Control". *Electrotechnology*, April/May: 71-74.

Cox, A. 1997. "New Services for UMTS". *Proceedings of UMTS – The Next Generation of Mobile*, London, UK, 27-29 October 1997.

GSM Association. 1999. "GSM Worldwide Networks on Air". GSM Association, 'GSM World' website. 6th Sept. 1999. http://www.gsmworld.com/membership/networks_on_air.html.

Furnell, S.M.; Green, M.; Hope, S.; Morrissey, J.P. and Reynolds, P.L. 1996. "Non-Intrusive Security Arrangements to support Terminal and Personal Mobility". *Proceedings of EUROMEDIA 96*, London, UK, 19-21 December 1996: 167-171.

Intekom. 1999. "Latest Global & Regional Cellular Statistics - World Cellular Indicators". http://home.intekom.com/cellular/statistics_latest.htm.

Jobusch, D.L. and Oldehoeft, A.E. 1989. "A Survey of Password Mechanisms : Part 1", *Computers & Security*, Vol. 8, No. 7: 587-604.

Modisette, L. 1990. "State-of-the-Art in Preventative Fraud Systems". *Proceedings of The 1999 GSM World Congress – Day 2*. Cannes, France, 23-25 February 1999.

Mouly, M. and Pautet, M. 1992. *The GSM System for Mobile Communications*. Mouly and Pautet, 4 rue Elisee Reclus, F-91120 Palaiseau, France.

Porras, P.A. and Neumann, P.G. 1997. "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", *Proceedings of 20th National Information Systems Security Conference*, 9 Octber 1997.

Rushe, D. and Oldfield, C. 2000. "The biggest game in town", The Sunday Times, Business Focus, 16 April 2000: 3.

UMTS Forum. 1998. *The Path towards UMTS – Technologies for the Information Society*. Report no. 2. The UMTS Forum. http://www.umts-forum.org/reports.html

H3 Poster Presentation

Britain's Younger Engineers in 2000

4 December 2000, House of Commons, Houses of Parliament, London, UK.

"Advanced Authentication and Intrusion Detection Technologies"

Advanced Authentication and Intrusion Detection Technologies

Paul Dowland, Dr Steven Furnell, George Magklaras, Maria Papadaki, Prof Paul Reynolds, Philip Rodwell, Harjit Singh
Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK

Abstract

Security is a vital consideration in the age of modern networks and Internet-based communications, and represents an essential underpinning of emerging applications such as electronic commerce. Within this domain, the ability to ensure the authorised and correct use of systems is an area of significant challenge. The research to be presented is centred around the Intrusion Monitoring System, a conceptual architecture for real-time user authentication and supervision, which has been defined by an earlier project within the Network Research Group. The current research encompasses advanced authentication technologies, based upon biometric techniques and user behaviour profiling. These approaches improve considerably upon the traditional user name and password combination, which has been proven to be weak and susceptible to compromise. While enhanced authentication will combat external impostors and internal masqueraders, further research addresses methods of identifying system misuse originating from authorised users, whom independent surveys have established account for around 80% of computer abuse incidents. Another important consideration relates to methods of responding to suspected intrusions in a manner that will trap genuine impostors and misfeasors, without unduly disrupting legitimate user activity in cases where a false classification has occurred. The research considers the application of these authentication and intrusion detection approaches within both traditional desktop environments and third generation mobile networks.

The Intrusion Monitoring System architecture

The Intrusion Monitoring System (IMS) is the focus of security research in the Network Research Group. IMS is an architecture for intrusion monitoring and activity supervision, based around the concept of a centralised host handling the monitoring of a number of networked client systems. Intrusion detection is the system is based upon the comparison of current user activity against both historical profiles of 'normal' behaviour for legitimate users and intrusion specifications of recognised attack patterns. The architecture is comprised of a number of functional modules, addressing data collection and response on the client side and data analysis and recording at the host (as illustrated in the figure below).

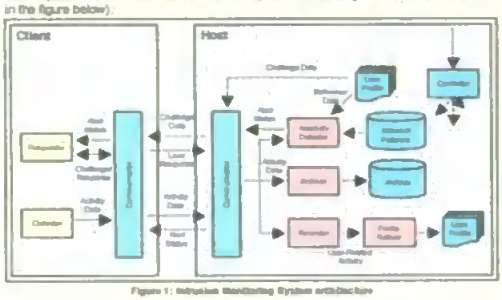


Figure 1: Intrusion Monitoring System architecture

Related Research Projects

The current IMS related research projects are listed below, a number of these involve collaboration and/or sponsorship from Orange Personal Communications Services.

1. User authentication and supervision in networked systems
This project concerns the investigation and evaluation of composite authentication techniques. The study recognises that a variety of authentication techniques are available which, when used in isolation, have known error rates in terms of false rejection and false acceptance. The research is focused upon the specification, implementation and evaluation of a composite authentication approach, in which a range of technologies are available and can be applied intelligently by the system as appropriate to the active user and their current task.

2. Behavioural profiling and intrusion detection systems using data mining
This project seeks to develop profiles of user behaviour by applying intelligent analysis techniques to system data collected in real-time during Windows NT sessions. The profile would represent a model of the legitimate users normal behaviour and could subsequently be utilised in a real-time supervision context to ensure that the activities of the user match those expected of the claimed identity. As such, the technique offers the potential to identify impostors and misusers within the system. This project contributes to the profiling aspect of the IMS architecture.

3. Generic approaches for intrusion specification and misuse detection
This project seeks to design and develop a generic intrusion specification language, which may then be used to specify intrusion characteristics in detection systems such as IMS. This work leads on to specific consideration of how to detect misfeasor attacks – that is, misuse of the system by a legitimate user. In terms of the IMS architecture, this project will contribute to the mechanisms utilised by the Anomaly Detector module.

4. Classifying and responding to network intrusions
This project seek to determine a comprehensive taxonomy of system-detectable intrusions and misuse, leading to the consideration of how the IMS system should respond to them. The work will involve design and practical evaluation of alternative response strategies, assessing factors such as the effectiveness against the nominated class(es) of intrusion and any negative effects that the response could have upon a legitimate user in a false rejection scenario.

5. Non-intrusive security for third generation mobile systems
This project highlights the need for improved methods of user authentication in future mobile systems such as the Universal Mobile Telecommunications System (UMTS). The work is focused upon an investigation of user-to-terminal and user-to-network forms of authentication for use in future mobile networks and devices.

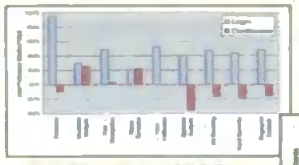


Figure 2: User Perference of Authentication and Supervision Methods (173 respondents)

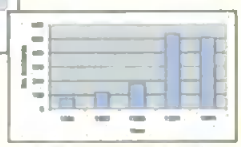


Figure 3: Reported Computer Crime Incidents (source: Audit Commission)

Authentication & Intrusion Detection Approaches

IDS techniques are based on the assumption that an intruder's behaviour will be different from that of a legitimate user. In order to detect this deviation from normal user behaviour, IDSs collect audit data such as system resource usage. Providing this continuous monitoring involves processing and analysing vast amount of audit data. Hence relying on human expertise is time consuming, knowledge intensive and infeasible past a certain volume of data. Therefore intelligent data analysis techniques are required to automate some of the process. The research is investigating techniques to automate some of the data analysis using Data Mining (DM) techniques and methodologies (figure 4 illustrates initial results).

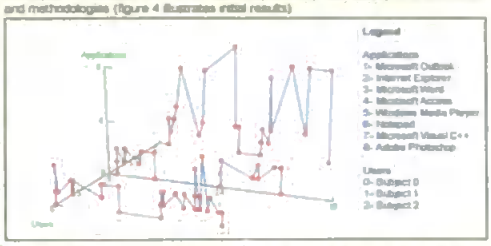


Figure 4: Graphical representation of applications run by users (IMS - Behavioural Profiling)

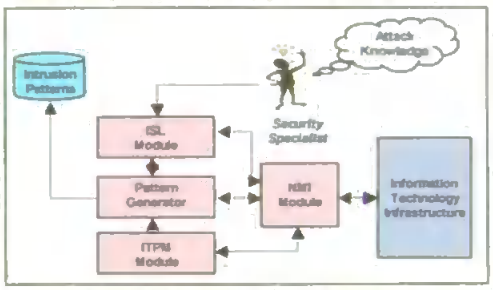


Figure 5: Functional Modules of an Intrusion Specification Language

ISL module The Intrusion Specification Language module, responsible for describing intrusions in a standardized, system independent manner. Used by the security specialist/architect.

Pattern generator module It converts the ISL descriptions into system-specific patterns. It also performs optimised pattern matching functions that are essential for real-time intrusion detection.

ITPM module The Insider Threat Prediction Model tries to sense the level of sophistication of a legitimate user. It can then estimate the probability that a particular user will misuse the infrastructure. This is an experimental/new approach of tackling the insider IT misuse problem.

NMI module The Network Management Integration module is responsible for utilising network management protocols in order to collect information and co-ordinate selected IDS responses from a variety of IT infrastructure components.

Information Technology Infrastructure The set of computer hardware, software and telecommunication components that perform a useful function inside an organisation.

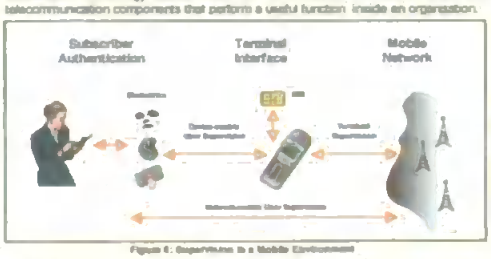


Figure 6: Supervision in a Mobile Environment

Summary

The techniques under investigation represent a considerable departure from traditional methods of authentication and access control, and aim to provide an added level of protection for IT systems. Modern society is increasingly dependant upon IT infrastructures. At the same time, surveys from bodies such as the Audit Commission and the FBI are reporting increased levels of computer crime and abuse (originating from both outside the organisation and from within). In view of these factors, the additional safeguards provided by advanced security techniques will become ever more necessary. As the research has identified, the techniques are relevant to both traditional networked PC environments, as well as other scenarios such as third generation mobile systems.

Dowland, P.S, Furnell, S.M, Illingworth, H.M and Reynolds, P.L. 1998. "Computer Crime and Abuse: A Survey of Public Attitudes and Awareness", Computers & Security, vol. 18, no. 8, pp715-729.

Dowland, P. and Furnell, S. 2000. "Enhancing Operating System Authentication Techniques", Proceedings of the Second International Network Conference (INC 2000), Plymouth, UK, 3-6 July 2000, pp253-261.

Furnell, S.M, Illingworth, H.M, Katsikas, S.K, Reynolds, P.L., and P.W.Sanders. 1997. "A comprehensive authentication and supervision architecture for networked multimedia systems", Proceedings of IFIP CMS '97, Athens, Greece, 22-23 September 1997, pp227-238.

Furnell, S.M. and Dowland, P.S. 2000. "A conceptual architecture for real-time intrusion monitoring", Information Management & Computer Security, vol. 8, no. 2, pp65-74.

Furnell, S.M, Dowland, P.S, Illingworth, H.M, and P.L.Reynolds. 2000. "Authentication and supervision: A survey of user attitudes", Computers & Security, vol. 19, no. 6, pp529-539.

Papadaki, M. 2000. A Taxonomy of I.T. System Intrusions. M.Sc. Thesis, University of Plymouth, Plymouth, UK.

Rodwell, P.M, Furnell, S.M. and Reynolds, P.L. 2000. "Non-intrusive security requirements for third generation mobile systems", Proceedings of PG Net 2000 – 1st Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, Liverpool, UK, 19-20 June 2000, pp7-12.

http://ted.see.plym.ac.uk/nrg

H4 Published Paper

Euromedia 2001

18-20 April 2001,Universidad Politecnica de Valencia, Spain.

"A Conceptual Security Framework to support Continuous subscriber Authentication in third generation mobile networks"

A Conceptual Security Framework to support Continuous subscriber Authentication in third generation mobile networks

P.M.Rodwell†, S.M.Furnell† and P.L.Reynolds‡
† Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, Plymouth, United Kingdom.
‡ Orange Personal Communications Services Ltd, St James Court, Great Park Road, Bradley Stoke, Bristol, United Kingdom.

KEYWORDS

UMTS, Authentication, Security, RM-ODP.

ABSTRACT

This paper discusses a conceptual framework addressing the issue of continuous subscriber authentication for 3rd generation mobile networks, based upon the International Telecommunications Union Reference Model for Open Distributed Processing (RM-ODP). Security provisions within current 2nd generation mobile networks such as GSM, are primarily aimed at secure communications through data encryption and *terminal* authentication via use of a smart card (SIM). Proposed services of the Universal Mobile Telecommunications System (UMTS) demand a more secure subscriber based authentication system, in order to protect personal information in the event of masquerade attack. Any authentication technique will be an integral part of an overall real-time security framework in order to offer continuous protection. In exercising the first three viewpoints of the RM-ODP, a summation of key security issues and a conceptual framework presented.

INTRODUCTION

It is not difficult to see that we are currently in the middle of a mobile communications revolution. From the appearance of mobile communication devices in school playgrounds, to more abstract applications of the technology, such as GSM equipped clothing (Philips, 1999). Owing to its circuit switched nature and a limited bandwidth of only 9.6kbit/s, it is recognised that the current GSM air interface is only *practically* suitable for voice telephony, text messaging and rudimentary data services. However, the next few years will witness the evolution of GSM technologies into a wireless Internet of advanced packet switched data services exhibited by the General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE) standards; culminating sometime in the next few years in 3rd Generation (3G) networks. Proposed by the International Telecommunications Union (ITU) initiative, IMT-2000, 3G mobile communications for Europe will come under the banner of UMTS (UMTS Forum, 2000). The proposed increases in bandwidth available will enable service providers to support significantly wider application scenarios than voice and the rudimentary data services of current cellular networks. This expansion of services, especially data services and the subsequent increase in personal and private data, will demand a parallel and corresponding increase in the level of protection provided by the terminal devices and the associated network operators.

This paper will introduce and justifying one of the most important of these security requirements; enhanced subscriber authentication; proceeding to discuss key issues pertaining to a conceptual security framework capable of supporting alternative advanced authentication techniques, in addition to the principle of non-intrusive and continuous monitoring. Although this paper does not discuss any specific continuous authentication mechanisms, the bias is towards biometrics, owing to its inherent suitability to non-intrusive application. (Biometrics Consortium, 2000).

The framework discussed in this paper takes a top-down approach to the problem, introducing and discussing relevant issues through the use of the ITU Reference Model for Open Distributed Processing.

ENHANCED AUTHENTICATION - A 3RD GENERATION REQUIREMENT

When considering the proposed services of UMTS (Cox, 1997), and the nature of future 3G devices, we realise that a more secure subscriber-based authentication system is essential in order to protect personal information in the event of masquerade attack (3GPP, 1999). A primary reason for this is the hastening convergence of mobile devices with Personal Digital Assistant (PDA) type devices, and the subsequent expansion in the range of possible services enabled as a consequence. In spite of the impoverished Man-Machine Interface (MMI), inherent to these devices (Nielsen, 1999), there is still a growing trend towards Internet style services through developments like the Wireless Application Protocol (WAP), Europe and I-Mode, Asia. The potential consequences, therefore, of masquerade attacks are far more severe owing to the additional and more personal information that these mobile/PDA devices are now storing and exchanging:

- financial details facilitating m-commerce
- electronic certificates for digital signatures
- full contact details of family and associates
- commercially sensitive miscellaneous information (e.g. scheduler/notepad files)

A key aspect of any proposed security framework is the balance of storage and distribution of the sensitive subscriber signature data within the communications device (handset) and across the network.

Compared to GSM, UMTS does not share the concept of a home network – the 'universal' aspect suggested in the name is based upon roaming between operators to suit the service required. In order to support true personal mobility, where a subscriber may register with any terminal interface (fixed or mobile) in order to access services, profiles need to be distributable throughout the network. The subscriber's profile could theoretically be accessed from any point within any compliant network in order to authenticate access to valid subscribed services. In such a network-centric solution, security details would be collected on the terminal and then securely transmitted and securely stored within the network for remote analysis.

REFERENCE MODEL OF OPEN DISTRIBUTED PROCESSING

The Reference Model of Open Distributed Processing (RM-ODP, 1994) was a joint effort by the International Standards Organisation (ISO) and the ITU-T to develop a coordinating framework for the standardisation of open distributed processing (ODP), supporting heterogeneous interworking between systems. The model describes an architecture, integrated into which are distribution, interworking, interoperability and portability. The RM-ODP framework takes a top-down approach, defining five abstract system viewpoints: Enterprise, Information, Computation, Engineering and Technology. The different viewpoints enable one to move progressively away from the conceptual world of user interfaces and enter into the tangible world of the supporting technologies and hardware infrastructures.

Viewpoints

The prescriptive framework, RM-ODP Part3, proposes five viewpoints decomposing the specification of the ODP system, focusing on the separate concerns. Using the conceptual structures rules and functions, a fundamental framework is generated specifying and bounding the proposed ODP system.

The five viewpoints of the RM-ODP are briefly categorised as follows:

- Enterprise: Purpose, Scope & Policy analysis. Organisational policies, per formative actions.
- Information: Semantics and Information Processing. Required information through the use of Schemas.
- Computational: Functional Decomposition. Functionality of ODP application, object handling.
- Engineering: Infrastructure to support the distribution.
- Technology: Technology for implementation.

Using this top-down approach, a large and complex system specification can be broken down into smaller, separate and manageable pieces, each focusing on the relevant issues to a particular working group.

CONCEPTUAL FRAMEWORK TO SUPPORT CONTINUOUS MOBILE AUTHENTICATION

This section addresses conceptual issues when considering techniques for discrete real-time authentication over a mobile communications network. The discussion covers the first three viewpoints of the *Requirements Analysis* and *Functional Specifications* sections of the RM-ODP schematic, Figure 1.

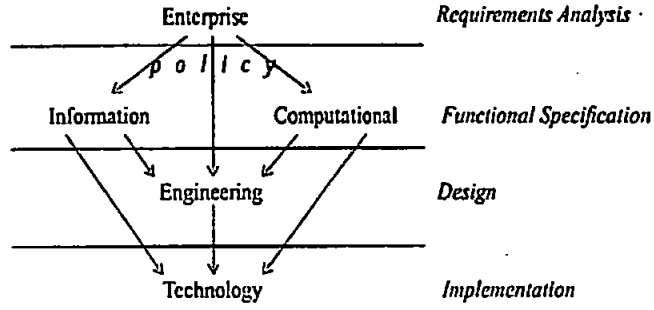


Figure 1: RM-ODP Viewpoints

Low level engineering and hardware infrastructure issues have not been considered at this stage.

Enterprise (business) Viewpoint

The enterprise viewpoint, addresses the performative actions governing the proposed framework. This is achieved through the use of active and passive *objects*, where an object is any unique entity within the framework; groups of objects or *object communities*, purposefully grouped to achieve a larger goal; and object permissions/prohibitions or *roles of objects*.

Top Level Objects

Under normal operation, there is only one *active* object within the security framework:

- the subscriber.

In the extreme case that the system is unable to resolve a security issue autonomously, a human operator could intervene in the decision making process, but essentially and for the majority of the time, the subscriber will be under network control.

The passive objects forming the top of the framework:

- the mobile network (community)
- the network interface handset (community)
- the subscriber account
- the archived subscriber reference profile
- the handset generated subscriber profile
- subscriber data packets
- subscriber payments (money)

Treating the network and handset as single entities/object communities, negates the need to break them down into their hardware infrastructures. Separate payment objects recognise those subscribers who prefer to pay in advance, rather than via contractual schemes. As these objects are not authentication issues, they are omitted from subsequent discussions.

Communities
The primary top-level object communities consist of 'the network, the subscriber account, the subscriber profile' and 'the interface handset, the subscriber authentication profile'; both objects share the data and subscriber objects.

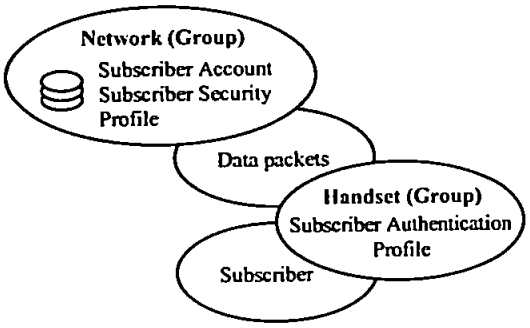


Figure 2: Enterprise Object Communities

Roles of Objects
Identifying the rules bounding the objects within the conceptual framework through:

- Permissions - What CAN be done
- Obligations - What MUST be done
- Prohibitions - What MUST-NOT be done.

Permissions:
A subscriber can choose to:

- access their network account at any time;
- change their network interface handset;
- terminate their account at any time.

The network can choose to:

- issue an authentication challenge at any time;
- maintain more than one profile for each subscriber.

Obligations:
A user:

- must have a valid network account;
- must continuously satisfy authentication;
- must sufficiently fund their network access.

The network:

- must act on authentication failure;
- must provide suitable protection of subscriber profiles; under legislation like the EU Data Protection Directive (Lloyd, 1996).

Prohibitions:
A subscriber:

- can only access *their* account;
- cannot initiate authentication profile changes;
- cannot bypass authentication;
- authentication profile cannot be artificially generated by any casual means.

Information viewpoint

This viewpoint presents the schemas involved with handling the state and structure of the pre-defined data object schemas at particular times:

- Static - state of an object at a particular time.
- Invariant - restricts state/structure at all times.
- Dynamic - defines permitted state changes.

Static schemas

- At Point-Of-Entry, a user is unauthenticated.
- At fixed or variable network defined intervals authentication is transparently requested.

Invariant schemas

- Continuous authentication is always active.
- The network handset must be authenticated to access the network.

Dynamic schemas
A subscriber:

- state change - authenticated to unauthenticated.
- profile is permitted to change over time; e.g. with age, health, behaviour etc.
- is permitted to change their handset(s) over time without affecting archived profiles.

Computational viewpoint

This view specifies the functional interactions between system objects at a low level. From this viewpoint, it can be argued that authentication may exist at several levels, as illustrated in Figure 3.

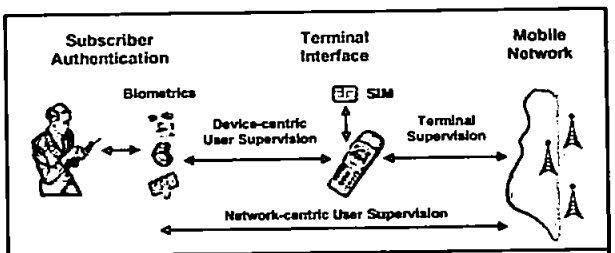


Figure 3: Mobility Authentication

It is considered that a suitable framework for achieving this is not dissimilar to previous security work carried out in the area of real-time network monitoring; i.e. The Intrusion Monitoring System (IMS), (Furnell, S.M., Dowland, P., 2000). Building on this work, it can be demonstrated that with suitable modifications, the IMS can be remodelled to meet the requirements of a continuous authentication system for mobile applications, where a detected anomaly is represented by a failed subscriber authentication. Considering the architecture in a purely authentication-based role (i.e. where misfeasor abuse is not considered), a suitable conceptual structure is shown in Figure 4.

In this revised structure, the client is represented by the subscriber handset and several of the modules have been renamed from the original IMS to reflect the more restricted authentication-only role (on the network side, the Archiver function has been removed altogether, reflecting the fact that the system is looking to perform real-time authentication, rather than ongoing activity monitoring).

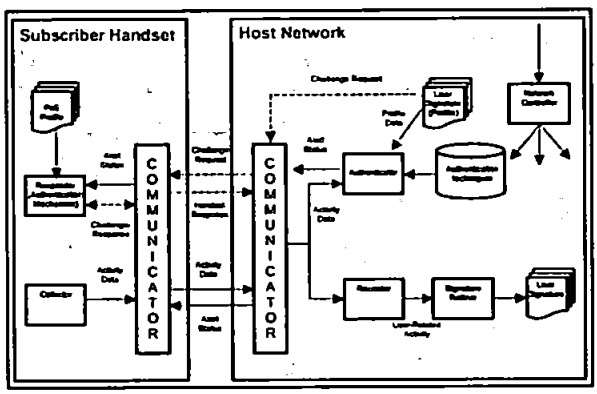


Figure 4: Enhanced Mobile Authentication System

The authentication function need not reside completely within the network. Point of Entry (PoE) authentication in particular could reside in the subscriber terminal, using an appropriate technique as the basis (e.g. the baseline method could still be a PIN, but more advanced methods like fingerprint recognition could also be used if a handset was suitably equipped). However, rather than being an isolated function within the terminal, it could be linked into the wider network-based monitoring system. For example, the network could be notified of any handset login failures, which would enable its alert status to proceed from an initially higher starting point than it would have otherwise done in the case of a completely successful login at the first attempt. More advanced, ongoing supervision would be network-based and, in this sense, the role of the handset becomes that of collecting relevant authentication data, upon request from the host network, and then responding as instructed when the data has been remotely analysed. It can be seen that the decision making process is retained within the network under the control of the network operator 'Authenticator' module. This is a basic security issue, offering advantages to both the operator and the subscriber: For the operator, it removes control and possibility of casual authentication tampering from the subscriber handset, for the subscriber, it offers the service of subscriber mobility.

There can be a number of mechanisms in place to trigger the authentication challenge request process:

- a simple chronological time-out.
- significant change of destination tolling.
- change from normal usage profile, i.e. departure from normal calling pattern, etc.
- mobile cell handover, a point of potential system weakness to a system abuser.
- e-commerce transaction.

Any combination of the above should transparently trigger re-authentication. In addition, there are other quality-of-service considerations to be addressed:

- network loading issues.
- reception conditions.
- available network bandwidth when roaming.
- remaining life-cycle of GSM handsets.

It can be argued that a brick wall lock out is not necessarily the best solution to authentication failure. As mentioned previously, quality of service is critical, and a low False Rejection Rate is fundamental to any continuous authentication scenario. It is advisable to exercise a form of phased service lockout, ranging from logging of user activity to a complete system bar.

CONCLUSIONS

This paper introduced and justified the need for improved subscriber authentication within the next generation of mobile communication devices. Through the approach of the ITU RM-ODP, the rules for a conceptual discrete real-time authentication framework have been generally defined and, through on going work on the IMS at the University of Plymouth, a suitable core architecture proposed.

REFERENCES

3GPP. 1999. "3G Security: Security Threats and Requirements." Technical Specification Group Services and System Aspects. Document: 3G TS 21.133 v3.1.0.

Biometric Consortium. 2000. "An introduction to biometrics", The Biometric Consortium, *http://www.biometrics.org/html/introduction.html*

Cox, A. 1997. "New Services for UMTS". *Proceedings of UMTS – The Next Generation of Mobile*, London, UK, 27-29 October 1997.

Furnell, S.M., Dowland, P. "A conceptual architecture for real-time intrusion monitoring", Information Management & Computer Security, vol. 8, no. 2.

Lloyd, I. 1996. "An outline of the European Data Protection Directive". *The Journal of Information, Law and Technology*, 1996.

Nielsen, J. 1999. "The Graceful Degradation of Scaleable Internet Services", *Alertbox*, 31 October, *http://www.useit.com/alertbox/991031.html*

RM-ODP, 1994. "Reference Model of Open Distributed Processing". Standards: ISO #10746. ITU-T #X.900.

BIOGRAPHY

Philip Rodwell was educated in Communication Engineering at the University of Plymouth, England; where he received his B.Eng. Honours degree in 'Personal Communications and Networks'. The programme included a one-year placement at Philips Consumer Communications, Le Mans, France; where he was part of the DECT team responsible for developing software for the Xalio range of cordless products. He is currently studying for his PhD within the Network Research Group at the University of Plymouth, researching 'Non-Intrusive Security Systems for 3rd Generation Mobile Networks', in association with Orange PCS, Bristol, England.

H5 Journal Article

British Computer Society – South West Journal

April 2001

"User authentication for current and future mobile telephony: Assessing subscriber acceptance"

User authentication for current and future mobile telephony: Assessing subscriber acceptance

N.Clarke, P.M.Rodwell†, S.M.Furnell† and P.L.Reynolds‡
† Network Research Group, DCEE, University of Plymouth.
‡ Orange Personal Communications Services Ltd, Bradley Stoke, Bristol.
Email: nrg@jack.see.plym.ac.uk

Introduction

The worldwide market for mobile telephone technologies has experienced dramatic growth in recent years and it is not difficult to see that we are currently in the middle of a mobile communications revolution. Recent figures indicate that the number of cellular subscribers today is nearly 479.5 million worldwide, with forecasts for the end of 2003 estimating the number to be around 1.073 billion [1].

The mobile technologies themselves have already evolved from the voice-only analogue systems of the mid 1980s, to the current second generation (2G) digital systems, first introduced in the early 1990s. Owing to its circuit switched nature and a limited bandwidth of only 9.6kbit/s, it is recognised that the current GSM air interface is only realistically suitable for voice telephony, text messaging and rudimentary data services. However, the next few years will witness the evolution of current GSM technologies into a wireless Internet of advanced packet switched data services exhibited by the General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE) standards; culminating sometime in the near future in 3rd Generation (3G) networks. Proposed by the International Telecommunications Union initiative, IMT-2000, 3G mobile communications for Europe will come under the banner of UMTS (Universal Mobile Telecommunications System) [2]. As an indication of the commitment UK mobile operators have already made to UMTS, the auction of the five UK licenses in April 2000 raised an incredible £22.47 billion [3]. The proposed increases in bandwidth available under UMTS will enable service providers to support significantly wider application scenarios than the rudimentary voice and data services of current cellular networks. This expansion of services, especially data services and subsequent increase in private data, will demand a corresponding increase in the levels of protection provided by the network hardware.

Security in the current second generation GSM system

The most widespread second generation mobile system in use in the world today is the Global System for Mobile Communications (GSM) [4], which, by September 1999, accounted for 344 operational networks in 127 countries, 63% of the worlds total cellular market today (Intekom, 2001). Security provision within GSM are largely geared towards secure communication (i.e. radio interface encryption) and terminal-based authentication. The latter being achieved via the combination of the familiar SIM smart card (Subscriber Identity Module) and the less familiar IMEI (International Mobile Equipment Identifier). The SIM holds all the subscriber's personal details, such as contact numbers, text messages, in addition to network operator registration details like the IMSI (International Mobile Subscriber Identifier). Mobile hardware is uniquely identified via an IMEI, which is used in conjunction with an operators EIR (Equipment Identity Register) to determine a devices security status, e.g. has it been reported stolen.

Relatively little attention is attributed to the authentication of the actual subscriber. Authentication of the subscriber to the terminal SIM is achieved through use of an impersonal and optional PIN (Personal Identification Number); stored in the SIM. This facility must be enabled by the subscriber before any level of protection is provided. Assuming this is done, the level of protection can still vary between devices depending on the handset manufactures implementation. Having said this, PIN protection can generally be considered commensurate with the level of risk of unauthorised use within a GSM environment.

Requirements for security in third generation Networks

When considering the proposed services of UMTS [5], and the nature of future 3G devices, we realise that a more secure subscriber-based authentication system is essential in order to protect personal information in the event of masquerade attack [6]. The primary reason for this is the hastening convergence of mobile devices with Personal Digital Assistant (PDA) type devices, and the subsequent expansion in the range of possible services enabled as a direct result. The potential consequences, therefore, of a masquerade attack will therefore become far more severe owing to the additional and more private information that these hybrid devices are now storing:

- financial details enabling mobile electronic commerce transactions
- electronic certificates for digital signatures
- full contact details of family and associates
- commercially sensitive miscellaneous information (e.g. scheduler/notepad files)
- medical records as a result of telemedicine or teleconsultations.

Attitudes to security provision within mobile networks

Within the University of Plymouth, a survey was conducted into the attitudes of mobile users to the current security provision within their mobile telephones and possible areas of improvement should they feel them inadequate for present and future systems. The survey was distributed locally to a broad range of mobile telephone users, in both hard copy and as an on-line questionnaire. There were a total of 161 responses completed both on paper and on-line.

Opinions on current security

As discussed previously, the primary method of personal security within a mobile handset is the PIN. Although 89% of respondents knew about the PIN facility, only 56% of them actually used it. The survey shows that 76% of respondents had phones with only a single level of security (at power on). Of those users that did have access to keypad PIN lockout in standby, only 46% of them used this facility on a regularly basis. 41% of respondents felt that entering a PIN number was inconvenient, with the same percentage also feeling unconfident in the level of protection the PIN provided. Although the results are not conclusive for or against the effectiveness of the PIN, there are a number of points that can be drawn from the data:

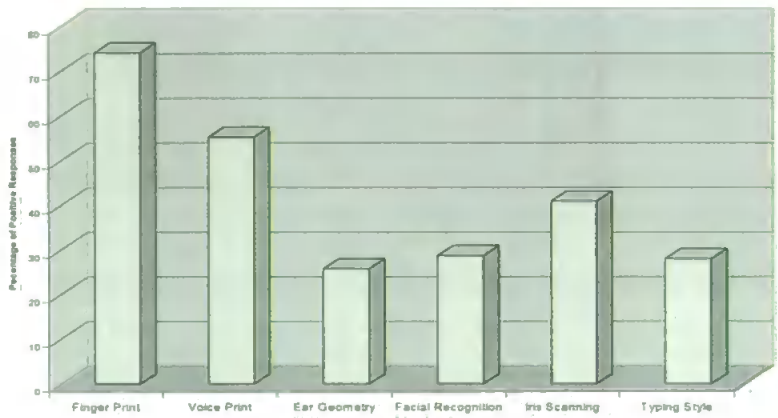
- 11% of respondents did not even know about the PIN facility. Scaled up this could represent up to 52.8 million subscribers worldwide.
- Of the 44% of respondents who did not use the PIN facility, 65% gave the reason as being its inconvenience; that is it's intrusive nature.
- Actually providing additional levels of security does not *necessarily* mean that a subscriber will actually use them. A significant 64% of respondents did not even use the more convenient PIN facility of keypad lockout whilst in stand-by (where available).
- A large number of respondents, 41%, have little confidence in the protection offered by the PIN facility, believing their handset is still at risk even with the facility active.

Opinions on having additional security

With telephone technology progressing rapidly to provide users with additional data services, this survey already identifies users accessing 2G data services and willing to continue to do so into the 3G technology. It is an encouraging sign that these users also recognise the need for security, with 81% believing it would be either *good* or *very good* to have increased security. Only 2 respondents thought it a bad idea. Although not proposing any specific scheme for improved authentication, the bias is towards biometrics, owing to its inherent suitability to non-intrusive application. [7].

Contributor's responses to the implementation of additional security show a strong preference towards fingerprint analysis; over 70%. Voiceprint and iris scanning also achieved good responses. Analysing the results does however indicate that respondents have possibly reacted more positively to those authentication mechanisms that they are already aware of.

Fingerprints have for a long time, primarily through Police use, been known to provide a reliable means of identification. In fact finger print recognition is already being used by Sagem in a mobile handsets for advanced e-commerce authentication purposes [8]. Voice print analysis has also attracted much attention recently through computer software and also in the telephone industry as a means of dialling numbers. Techniques such as ear geometry and typing style (keystroke analysis) are more recent, as such, less research exists on them.



Positive responses to six main authentication techniques

The survey not only found users wanting more security for their handsets but 63% of respondents, who were not indifferent, also felt a non-intrusive continuous authentication method during a session to be a good idea. Obviously some authentication techniques lend themselves to this technique much better than others, for instance voiceprint, as the user would probably already be talking on the telephone.

Conclusions

Up until now, PIN protection has generally been regarded as providing enough access protection, since the information contained on handsets has been relatively benign in nature, telephone numbers, simple text messages, etc. and thus of little value to a thief. More recently, with the advent of WAP enabled 2G handsets, there is a movement towards the storage of more sensitive material. This will culminate in the near future with the merger of PDA's and mobile telephones into 3G devices carrying all the associated data both these devices may contain. This does beg the question, how far can we rely on numerical passwords, how secure are they and how secure do users believe them to be? The findings of the survey have demostrated a perceived weakness in the current PIN technique in the eyes of it's users. They have however, responded positively towards alternative authentication techniques, principally fingerprint and speaker verification.

References

[1] Intekom, 1999. "Latest Global & Regional Cellular Statistics". http://home.intekom.com.
[2] UMTS Forum, 1998. *The Path towards UMTS – Technologies for the Information Society*. Report no. The UMTS Forum. http://www.umts-forum.org/reports.html
[3] Radiocommunications Agency. http://www.spectrumauctions.gov.uk
[4] Mouly, M. and Pautet, M., 1992. *The GSM System for Mobile Communications*, 4 rue Elisee Reclus, F-91120 Palaiseau, France.
[5] Cox, A., 1997. "New Services for UMTS". *Proceedings of UMTS – The Next Generation of Mobile*, London, UK, 27-29 October 1997.
[6] Third Generation Partnership Project, 1999. http://www.3gpp.org
[7] The Biometrics Consortium, 2000. http://www.biometrics.org
[8] Sagem MC-959-ID. Smart Card 2000 Show, London. http://www.sagem.com

H6 Poster Presentation

Britain's Young Engineers in 2001

3 December 2001, House of Commons, Houses of Parliament, London, UK.

"Non-Intrusive Subscriber Authentication for 3G Mobile System"

Non-Intrusive Subscriber Authentication for 3G Mobile Systems

Nathan Clarke, Paul Dowland, Dr Steven Furnell, Prof Paul Reynolds and Philip Rodwell
Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK

Abstract

Mobile phones are now an accepted part of everyday life, with users becoming more reliant on the services that they can provide. In the vast majority of systems, the only security to prevent unauthorised use of the handset is a Personal Identification Number (PIN). Although this may be argued to be commensurate with the requirements of current mobile applications, it is considered that the extended range of services that will be accessible through future third generation (3G) devices will increase the need for stronger methods. The research relates to the investigation, design and evaluation of advanced subscriber authentication techniques, suited to application within the context of a mobile handset. A survey of 161 mobile subscribers was conducted to assess their attitudes towards the security available in current second generation devices, and their likely acceptance of more advanced methods to support emerging applications. These results support the concepts design of a user authentication architecture for 3G mobile systems, using the concepts of biometrics as the basis for achieving a transparent, non intrusive method of authentication that does not disrupt the user's activity unless an anomaly is suspected. The viability of the concept will be illustrated by presenting details of a practical keystroke analysis system, which has been implemented to authenticate users on a modified mobile handset. The results observed from this prototype implementation will be discussed.

Subscriber Security Requirements for 3G Systems

The subscriber security provisions in current second generation mobile networks, such as GSM, are relatively limited, with the vast majority of devices relying upon Personal Identification Number (PIN) based methods. However, it can be argued that the level of security here is commensurate with the requirements of the devices, as the potential consequences from theft or impostor access can be broadly categorised as financial loss (which the legitimate user can limit by reporting the theft of the phone and getting it blocked by the operator) and breach of personal privacy, due to the impostor gaining access to contact details and text messages held on the device. However, it is acknowledged that this is a fairly limited amount of information, the disclosure of which would not normally be considered highly sensitive. Stored text messages may potentially have more significance, but would not generally represent a significant body of information. By contrast, the proposed services third generation (3G) networks demand a more secure subscriber-based authentication system in order to protect personal information in the event of masquerade attacks. The primary reason for this is the hastening convergence of mobile devices with Personal Digital Assistant (PDA) devices, and the subsequent expansion in the range of possible services enabled as a result. The potential consequences of a masquerade will, therefore, become far more severe owing to the additional and more private information that these hybrid devices will store.

- financial details enabling mobile electronic commerce transactions
- electronic certificates for digital signatures
- full contact details of family and associates
- commercially sensitive miscellaneous information (e.g. scheduler/notepad files)
- medical records as a result of telemedicine or telecontultations

A Survey of Current Mobile Subscribers

A survey was conducted to determine the attitudes of mobile users in relation to their use of existing PIN-based security, and their views about potential future methods. The survey was distributed to a broad range of mobile phone users, and a total of 161 responses completed both on paper and on-line.

Although 89% of respondents knew about the PIN facility, only 56% of them actually used it. The survey showed that 79% of respondents had phones with only a single level of security (at power on). Of those users that had the facility to PIN protect the phone in standby mode, only 36% used it. Other key findings included:

- 11% of respondents did not even know about the PIN facility. Scaled up this could represent up to 52.8 million subscribers worldwide.
- Of the 44% of respondents who did not use the PIN facility, 65% gave the reason as being as inconvenience.
- Providing additional levels of security does not necessarily mean that a subscriber will actually use them, as evidenced by those users who did not use the PIN to lock phones in standby.
- A large number of respondents, 41%, have little confidence in the protection offered by the PIN facility, believing their phone is still at risk even with the facility active.

Respondents did, however, recognise the need for security, with 81% believing it would be either good or very good to have increased security. As far the form that such security would take, subscribers were asked to comment upon the acceptability of a range of biometric measures, and the results were as shown in the graph below.

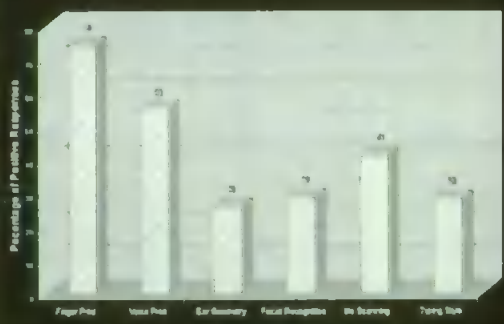


Figure 1: Acceptability of biometric authentication options

88% of users wanted to be able to access additional data services, such as m-commerce, video conferencing and web browsing from their devices – highlighting the need to better authentication in future devices.

One of the stated requirements for secure 3G service provision is that it should be possible for service providers to "authenticate users at the start of, and during, service delivery" (3GPP, 1999). Authentication during service delivery represents a departure from the standard approach in 2G systems and again implies the need for some form of transparent measure to avoid disrupting a subscriber's legitimate activity. Options for achieving this may be related to periodic or continuous supervision of subscriber activity, utilising profiling techniques or biometric monitoring.

Of the respondents who indicated that they would like more security, 67% also felt that the a continuous technique during normal phone use would be a good idea. Obviously some authentication methods lend themselves to this much better than others, and it would be important from the user acceptance perspective to ensure that chosen method(s) could be applied in a non-intrusive manner.

An Architectural Framework for Authentication

Authentication could most usefully be handled within a flexible security framework, which is able to intelligently monitor the available characteristics based upon the current activity of the subscriber. For example, voice verification could be utilised during a voice call, but during an e-commerce transaction it could be replaced by other characteristics that are more appropriate to the context, such as keystroke analysis. The monitoring system would determine which characteristics, from those available on the terminal, should be assessed at any given time and then pass on the relevant data for analysis. The analysis itself could be network or terminal-based. However, to avoid traffic overhead, the latter approach may be preferable. The terminal could then securely send the results to a network-based monitoring agent for access decisions (the involvement of the network level ensures that the network operator / service provider is kept aware of potential compromise). In this scenario, the network ultimately remains in control of the security and could request re-sampling by the terminal if the authentication results were inconclusive. Such an arrangement is illustrated in the figure below. The approach would be non-intrusive in the sense that the terminal user would be unaware of the security system unless compromise was suspected.

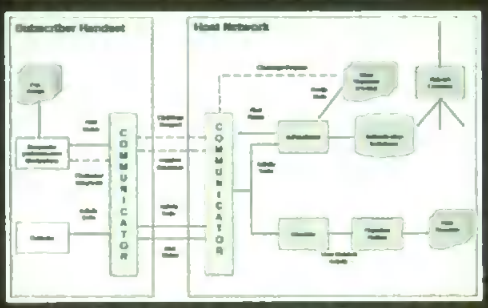


Figure 2: Components of an Authentication Framework

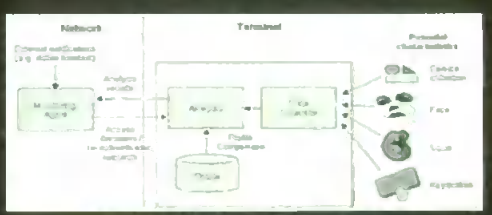
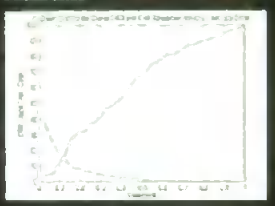


Figure 3: Potential Subscriber Monitoring Scenario

An Example Biometric

Initial experimental work has been conducted to assess the feasibility of applying keystroke dynamics within a mobile phone context, to authenticate users by assessing their interactions on the keypad (building profiles of characteristic inter-keystroke latency timings for different users). The initial study has assessed two types of keypad input, namely 4-digit PIN codes and standard telephone numbers.

The study involved 16 test subjects, with neural networks being trained in an attempt to differentiate between legitimate users and impostors. Data input was collected from a modified mobile phone handset, connected to a PC, in order to preserve the tactile content of a mobile device.



	FAR	FRR	EER
PIN code	18.1	12.5	15
Varying telephone	36.3	24.3	32
Fixed telephone	16	15	15

Note: Individual networks performed as well as 0% FRR and 1.3% FAR.

Summary

The capabilities of 3G mobile systems will open up a range of new service opportunities and, as a consequence, will impose new requirements for security. The survey findings indicated a weakness of the current provisions, in that the authentication technology is optional and, therefore, often unused. However, subscribers have shown the desire for additional security, and have responded positively towards a number of alternative techniques. Given that many respondents do not use the current security techniques that are available to them, it can be assumed that a non-intrusive method of authentication may prove to be most acceptable and widely utilised by end users. Viable architectural frameworks can be specified to support this, and suitable biometrics can be identified to provide the underlying authentication methods.

Clarke, N.L., Furnell, S.M., Rodwell, P.M. and Reynolds, P.L. 2001: 'Acceptance of subscriber authentication methods for mobile telephony devices', to appear in Computers & Security.

Furnell, S.M., Magopoulos, H.M., Karzaklas, S.K., Reynolds, P.L. and P.W. Sanders. 1997. 'A comprehensive authentication and supervision architecture for networked multimedia systems', Proceedings of IFIP CMS '97, Athens, Greece, 22-23 September 1997, pp227-238.

Furnell, S.M., Dowland, P.S., Magopoulos, H.M. and P.L. Reynolds. 2000. 'Authentication and supervision: A survey of user attitudes', Computers & Security, vol. 19, no. 6, pp529-539.

Rodwell, P.M., Furnell, S.M. and Reynolds, P.L. 2000. 'Non-intrusive security requirements for third generation mobile systems', Proceedings of PG Net 2000 – 1st Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, Liverpool, UK, 19-20 June 2000, pp7-12.

Rodwell, P.M., Furnell, S.M. and Reynolds, P.L. 2001. 'A Conceptual Security Framework to support Continuous Subscriber Authentication in Third Generation Mobile Networks', Proceedings of Eurosmode 2001, Valencia, Spain, 18-20 April 2001, pp135-138.

http://www.plymouth.ac.uk/nrg

H7 Published Paper

Third International Conference on 3G Mobile Communication Technologies

8-10 May 2002, London, UK.

"Advanced Subscriber Authentication Approaches For Third Generation Mobile Systems"

Advanced subscriber authentication approaches for third generation mobile systems

N.L.Clarke[†], S.M.Furnell[†], P.L.Reynolds[‡] and P.M.Rodwell[†]

[†] University of Plymouth, United Kingdom
[‡] Orange Personal Communications Services Ltd, United Kingdom

INTRODUCTION

Recent years have witnessed substantial and well-documented growth within the mobile communications sector, with global mobile subscribers forecast to rise from 768m in 2001 to 1,848m by 2004 [1]. However, in parallel with this rise in ownership there has been a rise in mobile related abuse, suggesting the need for greater security measures to prevent unauthorised use. Mobile handsets are already recognised as being prime targets for theft and research findings published by the UK Home Office has estimated that over 700,000 handsets were stolen from subscribers during 2001 [2]. It can be conjectured that the more advanced capabilities of third generation (3G) handsets will make them even more desirable targets in this respect. Additionally, the increased bandwidth available in 3G will enable service providers to support significantly wider application scenarios than the rudimentary voice and data services of current cellular networks. This expansion of services and subsequent increase in private data will demand a corresponding increase in the level of protection provided by the terminal and network hardware.

This paper presents consideration of the security requirements for 3G, considering specifically the issue of subscriber authentication. The discussion includes the results of a survey of current mobile subscribers, to determine their attitudes towards existing security measures, leading into architectural considerations and initial experimental results in relation to future techniques.

SUBSCRIBER SECURITY REQUIREMENTS FOR 3G SYSTEMS

Security provisions within 2G networks such as GSM are largely geared towards secure communication (i.e. radio interface encryption) and terminal-based authentication. The latter is achieved via the combination of the SIM (Subscriber Identity Module) and the IMEI (International Mobile Equipment Identifier), and enables the legitimacy of the terminal to be determined before allowing it to utilise the network. By contrast, relatively little attention is devoted to ensuring the legitimacy of the current user, and subscriber authentication provisions in the vast majority of devices rely upon Personal Identification Number (PIN) based methods. This facility must be enabled by the subscriber before any level of protection is provided. Even assuming this is done, the level of protection can still vary between devices depending on the handset manufacturer's implementation. Nonetheless, it can be argued that the level of security delivered by the PIN is commensurate with the requirements of the devices, as the potential consequences from theft or impostor access can be broadly categorised as financial loss (which the legitimate user can limit by reporting the theft of the phone and getting it blocked by the operator) and breach of personal privacy, due to the impostor gaining access to contact details and text messages held on the device. However, it is acknowledged that this is a fairly limited amount of information, the disclosure of which would not normally be considered highly sensitive. Stored text messages may potentially have more significance, but would not generally represent a significant body of information. By contrast, the proposed services 3G networks demand a more secure subscriber-based authentication system in order to protect personal information in the event of masquerade attacks. The primary reason for this is the hastening convergence of mobile devices with Personal Digital Assistant (PDA) devices, and the subsequent expansion in the range of possible services enabled as a result. The potential consequences of a masquerade will, therefore, become far more severe owing to the additional and more private information that these hybrid devices will store:

- financial details enabling mobile electronic commerce transactions;
- electronic certificates for digital signatures;
- full contact details of family and associates;
- commercially sensitive miscellaneous information (e.g. scheduler/notepad files);
- medical records as a result of telemedicine or teleconsultations.

ATTITUDES TO SECURITY PROVISION WITHIN MOBILE NETWORKS

A survey was conducted to determine current mobile subscribers' attitudes towards the security provisions within their devices, and possible areas of improvement. The survey was distributed to a broad range of mobile phone users, in both printed and

online formats, yielding a total of 161 responses. Full details of the results can be found in [3], but relevant summary information is presented below.

As discussed previously, the primary method of personal security within a mobile phone is the PIN. Although 89% of respondents knew about this facility, only 56% actually used it. The survey showed that 76% of respondents had phones with only a single level of security (at power on). Of those users that had the facility to PIN protect the phone in standby mode, only 36% used it. Other key findings included:

- 11% of respondents did not even know about the PIN facility. Scaled up this could represent up to 84.5 million subscribers worldwide.
- Of the 44% of respondents who did not use the PIN facility, 65% gave the reason as being its inconvenience.
- Providing additional levels of security does not necessarily mean that a subscriber will actually use them, as evidenced by those users who did not use the PIN to lock phones in standby.
- A large number of respondents, 41%, have little confidence in the protection offered by the PIN facility, believing their phone is still at risk even with the facility active.

Given these results, even in a 2G context, the prognosis for the successful application of the same methods in 3G is not encouraging. At the same time, the survey also revealed that 88% of users wanted to be able to access additional data services, such as m-commerce, video conferencing and web browsing, from their devices – highlighting the need for better authentication in future devices.

Despite their reluctance to use the existing PIN-based methods, the survey results revealed that respondents recognised the need for security, with 81% believing it would be either *good* or *very good* to have increased protection. Only 2 respondents thought it a bad idea.

Responses to the implementation of additional security showed a strong preference towards fingerprint analysis; over 70%. Voiceprint and iris scanning also achieved good responses. Analysing the results does however indicate that respondents have possibly reacted more positively to those authentication mechanisms that they are already aware of. Fingerprints have, for a long time, been known to provide a reliable means of identification. In fact fingerprint recognition has already being demonstrated by Sagem for advanced e-commerce authentication purposes in mobile phones [4]. Voice print analysis has also attracted much attention recently through computer software and also in the phone industry as a means of dialling numbers.

Techniques such as ear geometry and typing style (keystroke analysis) are more recent and, as such, less research has been done on them. Preliminary results in relation to keystroke analysis on mobile phones will be considered later in the paper.

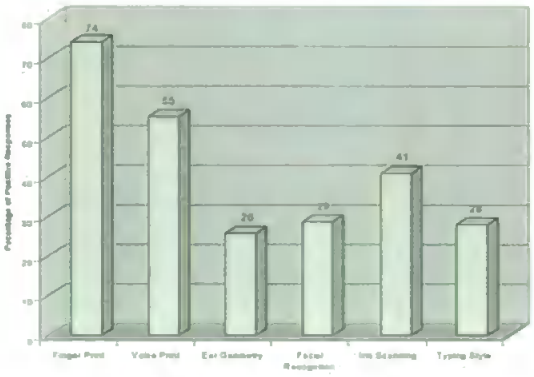


Figure 1: Positive responses to six main authentication techniques

Of the respondents who indicated that they would like more security, 63% also felt that a continuous technique during normal phone use would be a good idea. This apparent acceptance of continuous authentication is compatible with one of the stated requirements for secure 3G service provision; namely that it should be possible for service providers to "authenticate users at the start of, and during, service delivery" [5]. Authentication *during* service delivery represents a departure from the approach in 2G systems, and again implies the need for some form of transparent measure to avoid disrupting subscriber's legitimate activity. Options for achieving this may be related to periodic or continuous supervision, adopting profiling techniques or biometric monitoring. Some authentication methods clearly lend themselves to this better than others, and it is important from the user acceptance perspective to ensure that chosen method(s) could be applied in a non-intrusive manner.

AN ARCHITECTURAL FRAMEWORK FOR AUTHENTICATION

Authentication could most usefully be handled within a flexible security framework, which is able to intelligently monitor the available characteristics based upon the current activity of the subscriber. For example, voice verification could be utilised during a voice call, but during an e-commerce transaction it could be replaced by other characteristics that are more appropriate to the context, such as keystroke analysis (see later discussion). The monitoring system would determine which characteristics, from those available on the terminal, should be assessed at any given time and then pass on the relevant data for analysis.

The concept of such an arrangement is illustrated in Figure 2. The approach would be non-intrusive in the sense that the terminal user would be unaware of the security system unless compromise was suspected.

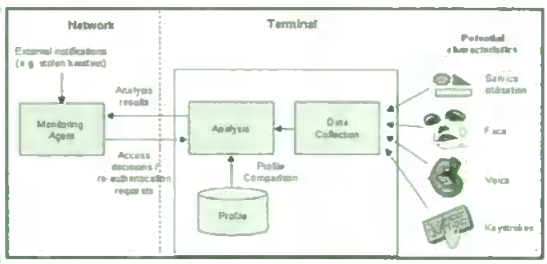


Figure 2: Potential Subscriber Monitoring Scenario

It can be seen from Figure 2 that elements of the functionality are split between the network and the terminal. However, the approach depicted in the diagram is by no means the definitive solution, and a fundamental issue is whether the security monitoring should be decentralised within the subscriber handset (and SIM), or centralised within the mobile network. Compared to GSM, UMTS does not share the concept of a home network – the 'universal' aspect suggested in the name is based upon roaming between operators to suit the service required. This raises a number of important issues, not least of which being that any security system needs to transcend the technology infrastructures of both software and hardware, raised by the different operator networks.

Terminal Issues

A terminal-based approach, where the subscriber's biometric profile is held within the handset, or more likely within the SIM card, places responsibility for the security of the profile, and consequently security of the network portal, in the hands of the subscriber. From an operator's perspective, this negates the need for additional government confidentiality legislation or network server security; there is also less need for a legal pathway of non-repudiation. As biometric authentication and supervision would be performed within the handset, it can be achieved without imposing additional network traffic overhead and enabling authentication to be performed independent of link availability.

There are also hardware issues relevant to the terminal-centric solution. For example, any additional processing within the handset would consume valuable CPU cycles and potentially reduce the performance for other tasks. It would also have an associated impact upon battery life and subsequent recharge interval, especially if the technique were to be applied continuously.

Network issues

There are some very strong arguments for introducing a centralised network based security system. It can be argued that placing security into the handset, and effectively into the hands of the subscriber, is inherently insecure to begin with. It could, for example render the profile more vulnerable to misuse or compromise if the terminal is stolen. From the operator's perspective, holding the profile, and performing any analysis, within the network may represent a more trusted solution.

Another potential advantage offered by the network centric system is that of increased personal mobility, where a subscriber may register with any network terminal in order to access their network operators' services under their personal subscription. Although GSM was originally designed to offer personal mobility via the SIM, the reality is that hardware, software, and operator network incompatibilities, as well as network locking agreements, have often restricted mobility to within a subscriber's own network. Additionally, the modern plug-in SIM generally resides behind the battery and is inherently too small and inconvenient to be of practical use as a token of true personal mobility. By replacing the token with a biometric, and centralising the authentication system, true personal mobility can potentially become a reality.

There are however some consequences to the personal mobility scenario, two primary drawbacks being increased data traffic over the wireless link and subscriber signature confidentiality. Taking the first point, the increased bandwidth of proposed next generation networks should have little trouble handling the extra handshaking required by any biometric and potentially continuously monitoring security system, especially compared to the bandwidth of a video signal. The second point of subscriber signature confidentiality reverses the trust issue mentioned earlier. Now the onus on data confidentiality is in the hands of the network operators, with subscribers trusting their sensitive and personal biometric data to not necessarily their network operator but perhaps even a third party associate.

In reality, the network-centric solution is more elegant, enabling network operators to better protect themselves against rogue users, and ultimately offering the more secure option for both of the legitimate parties.

In either scenario, the approach requires suitable biometrics to be available to monitor from the handset. Some experimental findings in relation to one such technique are presented in the next section.

MOBILE SUBSCRIBER AUTHENTICATION VIA KEYSTROKE DYNAMICS

Keystroke Dynamics is the term given to a biometric authentication technique that is able to classify, authenticate or identify a person according to their typing pattern. The use of keystroke dynamics as an authentication technique for mobile phones has two distinct advantages over other biometric techniques, in that it requires no additional hardware and can be implemented in a completely transparent environment.

The principal typing feature that is used to characterise behaviour in keystroke dynamics is the inter-keystroke latency. Many studies have taken place over the years, dating back to the 1980's, such as Joyce and Gupta [6], Leggett and Williams [7], Napier et al [8], which have all demonstrated that characteristic patterns can be discerned from an individual's typing style, which in many cases can be used to distinguish that individual from a would-be impostor. However, these studies have all centred upon the verification or identification of a user typing on a full computer keyboard. One previous study investigated authenticating users from a numerical input entered on a standard numerical keypad [9]. Although not identical to a mobile phone keypad, due to tactile qualities and typing context, the study concluded successfully, suggesting the potential for further experimental evaluation in a telephony context.

Experimental investigations

From the foundation provided by previous studies, a series of investigations were designed to examine the feasibility of using keystroke dynamics on a mobile handset. Three experiments were conducted, each involving a total of 16 participants:

1. the entry of a four digit number, analogous to the PINs used on current devices;
2. the entry of a series of varying telephone numbers;
3. the entry of a fixed telephone number.

The first and third investigations required the participants to enter the numeric keystroke sample thirty times, with twenty samples then being used to create a reference profile, and the remaining ten for subsequent testing. The second investigation required a larger number of samples due to the changing nature of the input string, and thus the need to train the authentication system more accurately. Fifty samples were taken, with thirty for training and twenty for testing.

Previous studies have shown neural networks to provide an effective foundation for keystroke analysis [9,10], and they have consequently been used in these investigations. The neural network structure is constructed on the feed-forward back-propagation network [11]; best exemplified for pattern recognition techniques.

Results

Brief analysis of the input data has identified two types of variance that enable or inhibit the classification process. The inter-user variance, which is essentially a measure of similarity between users and ideally would be as large as possible, and the inter-sample variance, which is a measure of similarity between individual samples of a particular user, and would ideally be zero. Neither of these variances are near their respective ideals, giving rise to the following results, as indicated in Table 1 and illustrated in Figure 3. Each investigation gives rise to a characteristic curve with two competing error rates. The False Acceptance Rate (FAR), the rate at which impostors are accepted by the system, and the False Rejection Rate (FRR), the rate at which the authorised user is rejected by the system. As can be seen from the figure it is possible to reduce one of the error rates only at the expensive of increasing the other. Therefore a decision has to be made between high security and low user acceptance (due to inconvenience), or low security and high user acceptance. Table 1 illustrates a threshold level chosen to have a compromise between error rates. The Equal Error Rate (EER) is also given as this can often be used as a performance measure when comparing biometric systems [12]. The figures in the table are, of course, averages across all of the test subjects involved. It is relevant to note, however, that some individual networks performed as well as 0% FRR and 1.3% FAR – showing that in some cases the technique has a much more significant potential than the average results would seem to imply.

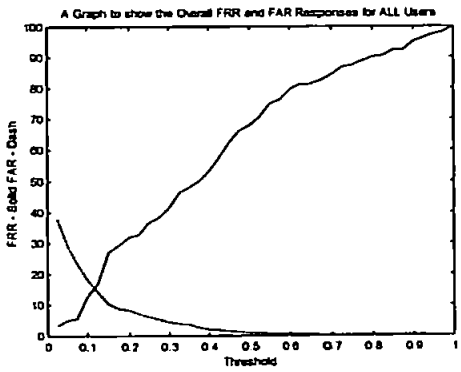


Figure 3: Performance Curves for the PIN Investigation

Investigation	*FAR*	*FRR*	*EER*
PIN Code	18.1	12.5	15
Varying Telephone	36.3	24.3	32
Fixed Telephone	16	15	15

Table 1: Keystroke Dynamics Investigation Results

The results demonstrate the potential to distinguish authorised users from impostors, although arguably not to any great accuracy. However, the experimental procedure used in this study was performed under controlled conditions; with users all entering the same input data - a condition that is unlikely in the real world. Additionally, the design, and implementation of the neural network used for classification was primitive and un-optimised. Continuation of the study beyond this feasibility stage requires variables such as pre-processing, generalisation, network sensitivity and network configuration to be considered and analysed.

Further development of the technique will also consider other forms of user interaction with mobile handsets, in order to attempt to profile behaviour in different contexts. For instance, the way in which someone types when entering an SMS message is likely to be different to the way in which they enter a telephone number. Some users will use certain applications or functionality on the phone more often than others; will dial certain number more than others; and equally as important will not use or dial certain people or services. All of these factors could potentially be used as discriminating characteristics, leading to a stronger overall verification technique.

CONCLUSION

The capabilities of 3G mobile systems will open up a range of new service opportunities and, as a consequence, will impose new requirements for security. The survey findings indicated a weakness of the current provisions, in that the authentication technology is optional and, therefore, often unused. However, subscribers have shown the desire for additional security, and have responded positively towards a number of alternative techniques. Given that many respondents do not use the current security techniques that are available to them, it can be assumed that a non-intrusive method of authentication may prove to be most acceptable and widely utilised by end users. Viable architectural frameworks can be specified to support this, and appropriate biometric measures can be identified to provide the underlying authentication methods.

Keystroke dynamics can only be considered to be a transparent technique when the user is interacting with the keypad. If the user begins a voice or video conference call, the approach becomes an intrusive and impractical method for continuous authentication. In order to overcome this, the use of two or more biometric techniques could be used in a hybrid non-intrusive manner, i.e. keystroke dynamics for typing authentication, voice recognition whilst speaking, and facial recognition for video conferencing. The effective and intelligent management of these biometrics would provide the necessary security required in a 3G environment.

REFERENCES

Giussani, B. 2001. *Roam – Making Sense of the Wireless Internet.* Random House Business Books, London, UK.

BBC. 2002. "Huge surge in mobile phone thefts", BBC News report, 8 January 2002. http://news.bbc.co.uk/hi/english/uk/newsid_1748000/1748258.stm

[3] Clarke, N.L., Furnell, S.M., Rodwell, P.M. and Reynolds, P.L. 2002. "Acceptance of subscriber authentication methods for mobile telephony devices". *Computers & Security.*

[4] Sagem. 2000. *Sagem MC-959-ID.* Smart Card 2000 Show, London. http://www.sagem.com

[5] 3GPP. 1999. *3G Security: Security Threats and Requirements.* 3G Partnership Project. Technical Specification Group Services and System Aspects. Document 3G TS 21.133 version 3.1.0.

[6] Joyce, G., Gupta, G. 1990. "Identity Authentication Based on Keystroke Latencies". Communications of the ACM, Vol 39. pp168-176.

[7] Leggett, J., Williams, G. 1988. "Verifying Identity via Keystroke Characteristics". International Journal of Man-Machine Studies, Vol. 28.

[8] Napier, R., Laverty, W., Mahar, D., Henderson, R., Hiron, M., Wagner, M. 1995. "Optimising digraph-latency based biometric typist verification systems: Inter and intra typist differences in digraph latency distributions". Int. Journal of Human-Computer Studies, Vol. 43, pp579-592.

[9] Ord, T. and Furnell, S.M. 2000. "User authentication for keypad-based devices using keystroke analysis", Proceedings of the Second International Network Conference (INC 2000), Plymouth, UK, 3-6 July 2000: 263-272.

[10]Cho, S., Han, C., Hee Han, D., Kim, H. 2000. "Web based keystroke dynamics identity verification using neural networks". Journal of Organisational Computing & Electronic Commerce, Vol. 10, No. 4, pp. 295-307.

[11]Bishop, C. 1995. *Neural Networks for Pattern Recognition.* Oxford University Press.

[12]Ashbourn, J. 2000. *Biometric. Advanced Identity Verification. The Complete Guide.* Springer

H8 Journal Paper

Computers and Security ***(Elsevier Science)***

June 2002, Vol. 21, no.3, pp.220-228(9).

"Acceptance of subscriber authentication methods for mobile telephony devices"

Acceptance of subscriber authentication methods for mobile telephony devices

N.L.Clarke, S.M.Furnell, P.M.Rodwell and P.L.Reynolds

Corresponding Author

S.M. Furnell
Head of Group

Network Research Group
Department of Communication and Electronic Engineering
University of Plymouth
Plymouth
United Kingdom

Tel: +44 1752 233521
Fax:+44 1752 233520

Email : sfurnell@plymouth.ac.uk

Other Authors

N.L.Clarke Research Student Network Research Group Department of Communication and Electronic Engineering University of Plymouth Plymouth United Kingdom Tel: +44 1752 233520 Fax: +44 1752 233520	P.M. Rodwell Research Student Network Research Group Department of Communication and Electronic Engineering University of Plymouth Plymouth United Kingdom Tel: +44 1752 233520 Fax: +44 1752 233520
P.L.Reynolds Manager Strategy and Trials Orange Personal Communications Services Ltd St James Court Great Park Road Bradley Stoke Bristol United Kingdom Tel: +44 973 746050	

Acceptance of subscriber authentication methods for mobile telephony devices

Abstract

Mobile phones are now an accepted part of everyday life, with users becoming more reliant on the services that they can provide. In the vast majority of systems, the only security to prevent unauthorised use of the handset is a four digit Personal Identification Number (PIN). This paper presents the findings of a survey into the opinions of subscribers regarding the need for security in mobile devices, their use of current methods, and their attitudes towards alternative approaches that could be employed in the future. It is concluded that, although the need for security is understood and appreciated, the current PIN-based approach is under-utilised and can, therefore, be considered to provide inadequate protection in many cases. Surveyed users responded positively towards alternative methods of authentication, such as fingerprint scanning and voice verification. Based upon these findings, the paper concludes that a non-intrusive, and possibly hybrid, method of authentication (using a combination of techniques) would best satisfy the needs of future subscribers.

Keywords

Authentication, Mobile, GSM, UMTS, Biometrics.

Introduction

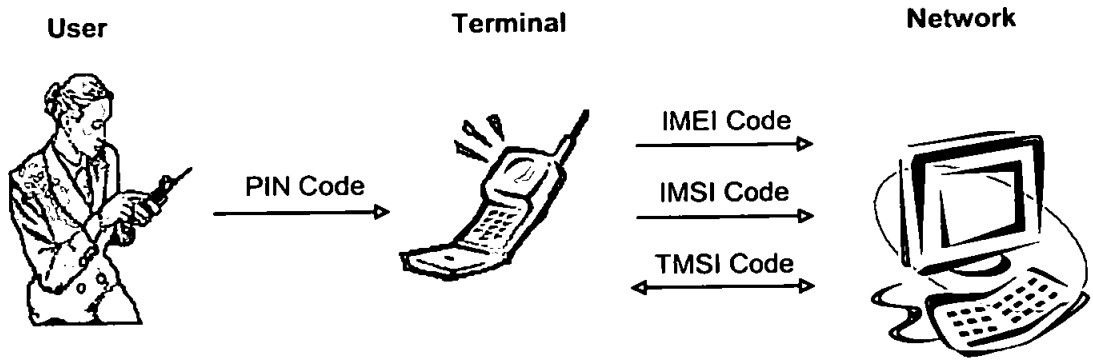
The mobile phone market has witnessed phenomenal growth in recent years, such that the phone itself is now regarded as an essential everyday item by millions of people. Indeed, cellular subscribers currently total around 479.5 million worldwide, a 56.87% growth on the previous year, with forecasts for the end of 2003 estimating that the number of subscribers will be in the region of 1.073 billion [1].

In addition to increasing subscribers, the capabilities of the phones themselves will also improve. With the introduction of third generation mobile devices, part of the ITU IMT-2000 initiative [2], a broadband service of up to 2 Mbps will be on offer, providing the potential for true multimedia services [3]. As the technology advances, the range of potential services also expands. Whereas the first generation analogue phones of the 1980s were purely aimed at the provision of voice telephony services, the arrival of second generation (digital) phones in the early 1990s ushered in basic data services such as SMS (Short Message Service) text messaging. In more recent years, devices supporting the Wireless Application Protocol (WAP) have facilitated limited Internet access, and the emergence of faster access technologies, such as GPRS (General Packet Radio Service) and UMTS (Universal Mobile Telecommunications System), will hasten the convergence of the mobile phone with Personal Digital Assistant (PDA) devices. This, in turn, will significantly increase the range of in-built and network-based applications of the device, thus also increasing the range of potentially sensitive and private information that the devices will hold.

As the sensitivity of information stored on a mobile device increases, the need for effective security also increases. The 3rd Generation Partnership Project (3GPP), who provide the technical specifications and regulations for UMTS, have recognised the need for secure data communications and produced appropriate standards [4]. However, security over the air interface is only one aspect of the problem, and it is also important to ensure appropriate protection of the device against unauthorised access. Current mobile handsets do incorporate some level of protection in this respect, but it is fairly rudimentary, and as the need for security increases there is the potential to incorporate more advanced methods. At this stage, however, questions remain about the security measures that customers would expect, and tolerate, to protect their personal information. This paper considers the need for security on mobile handsets, end-user attitudes towards current authentication measures, and their views in relation to future service opportunities and the consequent security requirements that these will impose.

Subscriber authentication in mobile systems

At the time of writing, the dominant mobile network standard is GSM (Global System for Mobile communications), which accounts for 63% of the global cellular market [1]. The authentication security that the GSM networks currently provide is focused between the terminal devices and the network, as shown in Figure 1, with a number of checks being made to ensure that the handset is permitted to use the network, has not been reported stolen etc. By contrast, the security between the terminal and the subscriber is currently quite rudimentary, with subscriber authentication based upon the use of a Personal Identification Number (PIN).



PIN - Personal Identification Number
IMEI - International Mobile Equipment Identifier
IMSI - International Mobile Subscriber Identifier
TMSI - Temporary Mobile Subscriber Identifier

Figure 1 : User - Terminal – Network Security Processes

For the majority of mobile phones, the PIN is the only form of authentication required in order for a user to be able to access the device. The authentication process will typically only allow the user to enter the number incorrectly a finite number of times (typically three) before the Subscriber Identity Module (SIM) within the phone becomes locked and requires a special unlock password (PUK) from the network service provider. In this way, brute force attacks on the PIN code (where every combination is

systematically tried) are avoided. However, the security here assumes two things: firstly, that the PIN facility is activated, and secondly, that the user has not compromised its protection (e.g. by not changing it from the factory default, by writing it down, or by telling someone else) in the many that frequently occurs with other knowledge-based authentication approaches, such as passwords [5].

If the PIN facility is enabled, it may (depending on the make/model of phone) provide two levels of authentication. All phones can be configured to request the PIN when they are switched on (normally only allowing emergency calls in its absence). Some models also allow locking of the keypad when switched on, requiring PIN re-entry before each use. As such, the PIN is capable of providing protection, and to date it has generally been regarded as providing sufficient security, given that the information held on the devices is relatively limited (e.g. telephone numbers, simple text messages, etc.), and thus of little value to a thief. Therefore the main threat comes through unauthorised usage of the phone, which only exists in a finite window before the phone is reported stolen and subsequently disabled by the network operator. Recently, with the advent of WAP-enabled second-generation phones, there has been a movement towards the storage of more sensitive material. For example, some handsets contain a credit card reader that is able to make transactions over WAP-enabled web sites. Although this still requires a PIN identification before use, it does pose the question of how far we can rely on PIN codes, how secure they are, and how secure users believe them to be.

Whereas PIN-based authentication relies on something the user *knows*, an alternative method is authentication via something the user *is*, a domain more commonly referred to as biometrics. There are two categories of biometric authentication [6]:

- Physiological biometrics, based upon bodily characteristics (e.g. fingerprint analysis, facial recognition, iris scanning and ear geometry).
- Behavioural biometrics, based upon the way people do things (e.g. voice print, typing style).

Much research has gone into developing these techniques into practical systems, and they are already employed as alternative authentication methods in desktop PC environments - for example, 9% of the respondents to the 2001 CSI/FBI Computer Crime and Security Survey claimed to use biometric security technologies [7]. In addition, there is already evidence of their application within the mobile domain. The Sagem MC959 handset, for example, incorporates a fingerprint recognition system into the back panel [8]. When considering the application of biometrics, in the context of mobile handsets, appropriate thought needs to be given to the practicality of the technique. It is noticeable, for example, that physiological techniques generally require additional hardware, such as the fingerprint scanner, to be added, whereas behavioural techniques do not. Implementation of behavioural techniques can be achieved through software only. Clearly, for mass-market devices, component cost is a major consideration, and handset prices are already subsided by network operators in many countries in order to keep the cost down for the consumer. However another major consideration to take into account is how the subscribers actually feel about security. Customers in today's world dictate the success or failure of a product, so their attitudes and opinions are important factors to take into consideration.

A survey of subscriber attitudes towards mobile security

A survey was conducted to assess the attitudes and opinions of current mobile subscribers towards authentication on their phones. To this end, a questionnaire was devised that assessed the following aspects:

- how the phone is used (e.g. voice communications, text messages etc.) and how subscribers would like to use their phones in the future. This gauges the level to which additional security is necessary - if the phone is used purely for voice communications then the need for increasing security is questionable;
- users opinions about the current form of authentication, the PIN;
- whether users believe there is a need for increasing security, and if so how would they like to see a solution implemented.

The survey was distributed as hard copies to a wide range of people, with one proviso – in order to be able to offer a valid opinion, the respondents had to be current or past users of mobile phones. A total of 138 paper-based copies where returned. An on-line version was also created, achieving another 23 responses. Thus, a final total of 161 responses were obtained, and the results are analysed in the sections that follow.

General

The survey was not aimed at any specific age group or gender, the hope being to obtain a good cross section of users. As shown in Figure 2 below, 53.5% of respondents were in the 17-24 age group. Although at first glance this figure does not suggest a particularly representative sample, it is actually a fair reflection of mobile phone ownership in the UK, where the survey was focused. Recent market research studies have illustrated that teenagers now account for a significant proportion of phone purchases, particular in relation to pre-pay phone options [9]. With this in mind, the predominance of younger respondents in this study is less surprising, and serves to make the results a more accurate reflection of typical subscriber attitudes.

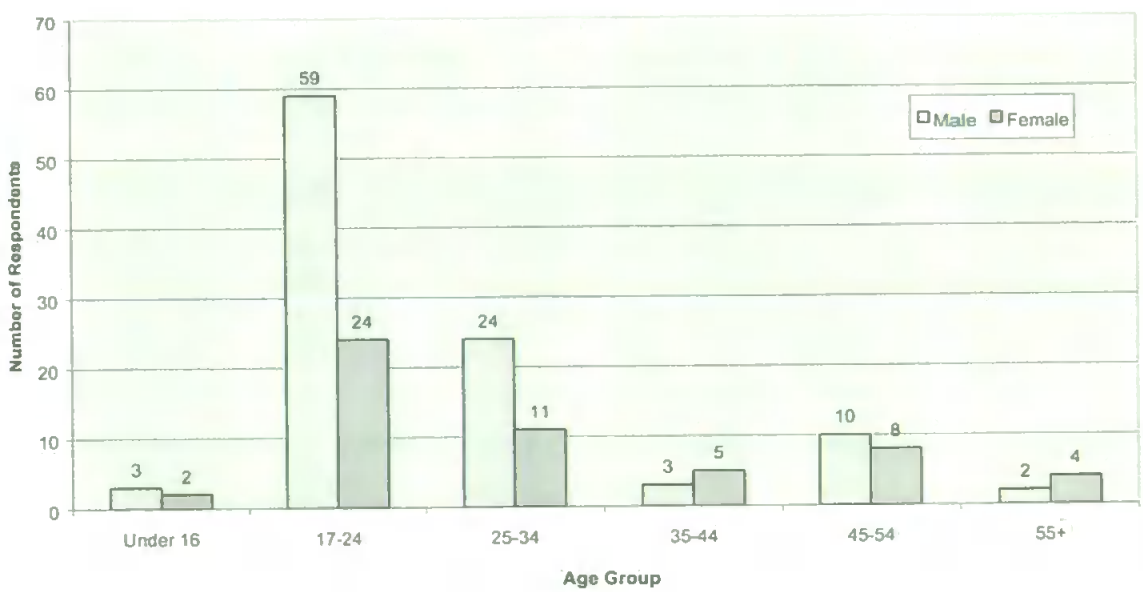


Figure 2 : Gender and age split in the respondent group

The desire to remain contactable is apparent from how long respondents leave their handsets switched on. 57% of those questioned said they kept their phone switched on for greater than ten hours a day, with 19% claiming between six and ten hours, and the percentage descending in order to 11% for less than one hour a day. These findings have a couple of implications:

- The need to leave the phone on comes in part from the need to stay in touch. So is the mobile phone the users principle means of doing this? Those switching on for less than one hour are likely to be users who only switch on when they wish to use the phone themselves. Thus either do not wish to be kept in contact with or have another principle means of communication, for instance a landline phone. Those leaving their phones on for a long period of time are likely to consider their phones to be there major means of contact, showing a possible long-term commitment towards the use of mobile phones.
- With the large number of respondents leaving their phone on, this could have implications for security, especially those who do not have or do not use a PIN facility to lock their keypad on standby.

Different phone manufacturer's, although providing a range of different phones, often keep the same software functionality, i.e. Nokia and its proprietary menu system. Nokia and Motorola's use of the PIN is no different in principle. However, whereas Motorola provides the facility to lock the keypad whilst on standby, Nokia however does not. In this particular sample, 57% of respondents are Nokia owners, of whom 96% leave their phone on for more than one hour a day, and 87% leave it on for more than six hours a day. This results in a significant number of unlocked phones on stand-by mode for long periods of time every day, leaving them with effectively no defence from un-authorised use if lost or accidentally left unattended.

Mobile phone usage - present and future

Unsurprisingly, results indicate that the vast majority use their mobile phone for talking. More interestingly, however, 90% of respondents regularly use text messages as a means of communication. Figure 3 illustrates these findings, in addition to responses for a range of other current services. The other services are newer, and from the responses have not been adopted as widely at present. A possible discrepancy in the data exists surrounding the use of the email service. Although this service is currently available on only a small proportion of handsets, 64% responded 'yes' or 'no' to the question of whether they used the facility. It is considered likely that many respondents who answered 'no' were doing so because their phone does not offer them the option (and, therefore, they should ideally have selected the 'not available' option on the questionnaire). This hypothesis also applies to the use of WAP services. However, it is valid to note the proportion of users that do use their phone for WAP and email services stands at 6% and 9% respectively, indicating an emerging acceptance and use of advanced data services.

Respondents were also asked whether they would consider using a small range of other services that are likely to be offered by future mobile handsets.

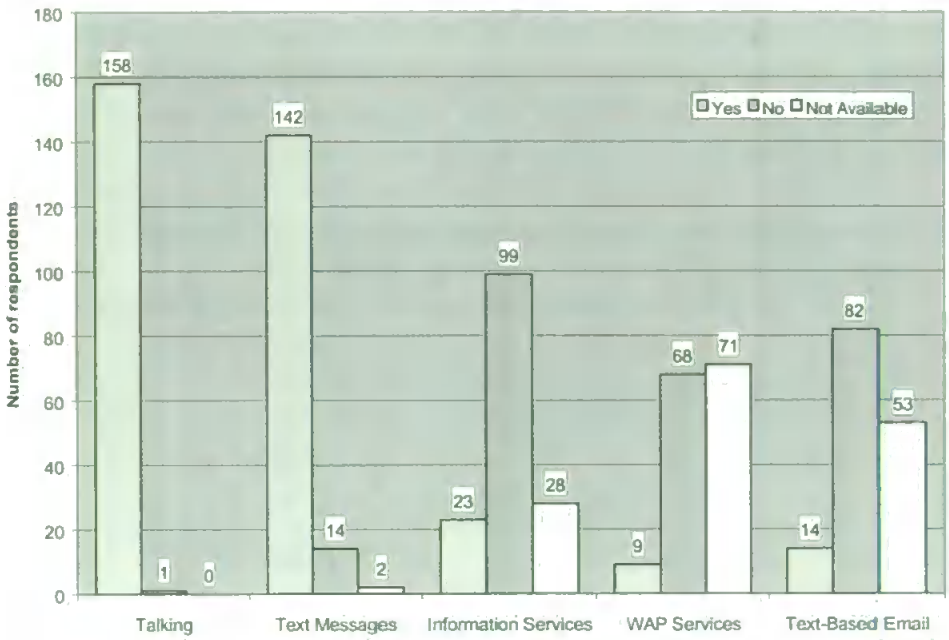


Figure 3 : Services used by respondents

The questionnaire specifically suggested the options 'video conferencing', 'online shopping', 'World Wide Web', 'Downloading music' and 'Personal Organiser', as well as offering respondents the option to suggest other ideas that would interest them. The results strongly suggested that the adoption of advanced mobile service is likely to continue, with 40% looking to use video conferencing, 43% interested in online shopping, 58% desiring mobile web access, 53% wishing to download music, and 73% wanting an integrated personal organiser. Although the latter would not necessarily involve communication between phones and the network, the data stored in personal organisers could well contain sensitive information such as bank account details etc. The additional services that were suggested by respondents included 'digital money', 'radio', and 'global positioning system' – all of which are very likely to emerge in combination with telephony handsets. Overall, it is also worth noticing that 88% of respondents did want to use some form of additional service.

Usefulness of current security

As previously discussed, the primary method of user authentication for mobile phones is the PIN, which is able to provide up to two levels of security. Although 89% of respondents knew about the PIN facility, only 56% of them use it in either form. The survey shows that 76% of respondents had phones with only one level of security (at power on). Of those users that did have both levels of security, only 46% of them used the second level on a regularly basis. Asking whether the respondents feel entering a PIN number is inconvenient, 41% responded 'yes' with the same percentage also expressing doubts about the level of protection the PIN can provide. Although the results are not conclusive enough to put an argument for or against the usefulness of the PIN facility, there are a number of significant points that can be drawn from the data:

- 11% of respondents did not know about the PIN facility. On the face of it, this is a relatively small percentage, but on a worldwide scale that accounts for 52.8 million subscribers who do not even know that security is available.
- Of the 44% of respondents who do not use the PIN facility, 65% of them considered it to be inconvenient, thus suggesting a good reason why they do not use it.
- Providing additional levels of security does not necessarily provide the user with additional protection if s/he does not use it through inconvenience. 64% of respondents for whom the ability to PIN-protect the phone between calls is available, still do not use the facility because they find entering the PIN inconvenient.
- A significant proportion of respondents, 41% do not have confidence in the protection the PIN facility provides, indicating users believe their phone is still at risk from misuse even if the PIN facility is in use.
- 52% of female respondents do not use the PIN facility compared to 39% of males.

The survey also asked respondents to comment about issues relating to the compromise of security. When asked to consider compromise by another party, only 11% of users believed that their phone had been used without their permission. The real percentage is likely to be higher, from misuse that has gone undetected. For instance people who may use the phone briefly without the owner's knowledge. Those respondents who answered positively to this question are likely to have had their phone stolen, and thus detected the misuse. The questions also considered compromise of protection arising from the subscribers' own actions. There are several ways in which subscribers may invalidate the PIN security, such as revealing the number to someone else, forgetting it, or writing it down. Table 2 presents a summary of the findings here.

	Yes (%)	No (%)
Forgotten It	17	83
Told Someone Else	26	74
Taken a Written Note Of It	6	94

Table 2 : Respondents who invalidate their PIN protection

Attitudes towards future authentication options

With mobile handset manufacturers and network operators both aiming to provide users with additional services, the need for security is likely to increase. This survey has identified that users are already using data services, and are willing to use future services as and when they become available. It is an encouraging sign that the respondents also recognise the need for security, with 81% believing it would be either good or very good to have more security. Only two respondents thought it would be bad idea. This recognition shows that users are aware of the need for security, and are also possibly worried about their current level of protection. Interestingly, however, the desire for more security shows a downward trend as the respondents' age increases, as shown in Table 3.

Age Group	Responded positively (%).
Under 16	100
17-24	89
25-34	72
35-44	66
45-54	68
55 or older	42

Table 3 : Respondents opinions on having additional security

Having established that respondents were generally accepting of additional authentication measures, the survey proceeded to assess their preferences for the forms that it could take. Having determined that PIN-based protection is problematic, it is considered that other authentication methods based upon something the user *knows* (e.g. passwords) would be equally under-utilised or inconvenient. The implication of this is that the most sensible route for improving authentication is to base the approach upon a biometric technique (the other option for authentication, basing it upon something the user *has*, is likely to offer little advantage, as the phone itself is something the user has, and any supplementary authentication token would be likely to be kept with the device). With this in mind, the survey respondents were presented with a range of biometric authentication options and asked to indicate which of them would be preferable to the PIN. The biometrics offered as options were as follows: fingerprint recognition, voice print recognition, ear geometry, facial recognition, iris scanning, and typing style All of these techniques have been the focus of previous research, and some are already widely recognised as commercial products in the domains of physical access control and desktop computing [10]. The respondents' opinions in relation to the techniques are illustrated in Figure 4.

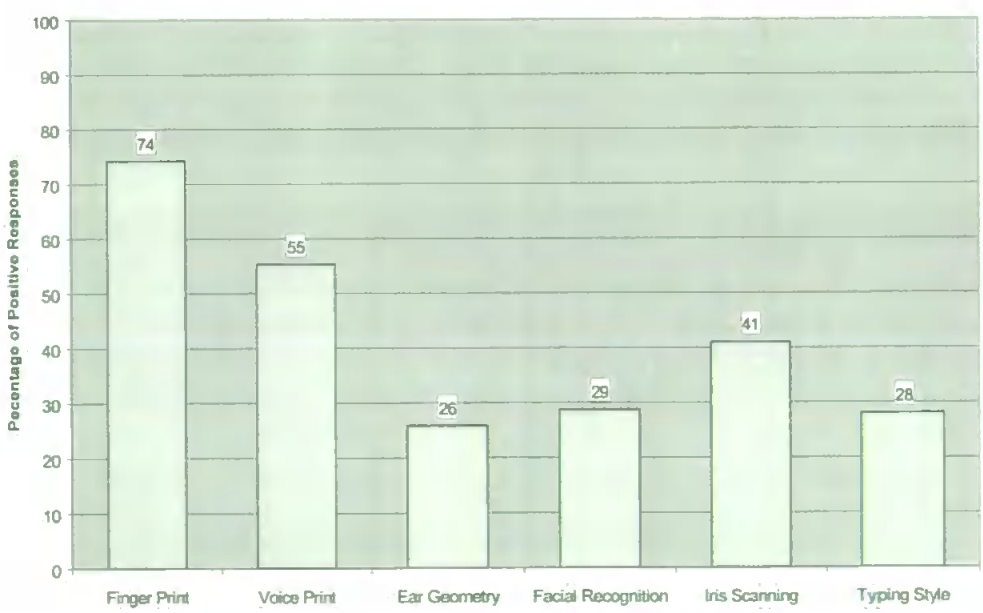


Figure 4 : Positive responses to biometric authentication techniques

Techniques such as ear geometry (in which the subscriber would be identified by the physical shape of their ear) and typing style (in which authentication would be based upon characteristic inter-keystroke latencies observed when subscribers dial numbers or otherwise interact with the keypad) are less recognised in the marketplace, but are considered particularly suited to non-intrusive application in a telephony context.

The results showed a strong preference towards fingerprint analysis, with approximately three quarters of the respondents selecting this option. Voice print analysis and iris scanning also achieved good scores, albeit significantly lower than fingerprint analysis in both cases. The remaining three techniques were demonstrably less popular, appealing to just over a quarter of respondents in each case. However, any conclusions drawn from these results should be tempered with the observation that the respondents are likely to have responded most positively to those ideas that they have already heard of. Fingerprints have long been known to provide a means of successfully identifying people, and indeed such techniques are already being used in mobile phones. Voice print analysis has also attracted much attention through the media, computer software applications, and also in the phone industry (albeit in the context of voice recognition for dialling numbers, rather than as a means of authentication). It is also fairly easy to understand this authentication technique, as people generally sound different. Techniques such as ear geometry and typing style are newer, and less information is known about them. Although keystroke analysis techniques have been extensively researched for use in PC-based authentication [11,12], it is not a widely advertised or used technique. As for ear geometry, although it is not very difficult to imagine how this technique might possibly work, there are no current implementations on the general market, and knowledge about this technique would, therefore, have been very limited amongst the respondents.

The point, therefore, is not to regard the results as a conclusive attitude towards one technique over another. The key observation that can be made is that all techniques were (to some degree) considered favourably, and that if a technique were to be implemented that was less known about generally, a degree of education and awareness before wide scale adoption.

One advantage of certain biometrics when compared to the PIN is that they offer the potential for authentication to be performed on a continual basis rather than as a one-off judgement. Respondents were, therefore, asked whether they would consider continuous authentication during a call to be acceptable. The results revealed that 41% of respondents considered continuous authentication during a call to be a good idea, while 24% were against the idea, and 35% were indifferent to the idea. However, the actual number of users willing to break during their call to authenticate themselves is likely to be low, which implies that any continuous authentication method implemented would have to be non-intrusive (without explicit action by the user). Certain authentication techniques will clearly lend themselves to this better than others, for instance voiceprint, as the user would be talking on the phone already. Techniques such as keystroke analysis would not typically be viable during a traditional voice call, but could potentially provide a measure of authentication as each call is initiated, or during the conduct of keypad-oriented, non-voice sessions.

For all authentication techniques, including the PIN, some information needs to be stored so that a comparison is possible with the input data. The final objective of the

survey was to establish users' opinions on where this profile should be stored – on the phone or in the network. The advantage of storing the profile on the phone is that authentication can then occur completely on the phone, with the result that no personal details are communicated to and from the network, and the network traffic overhead is minimised. However, the disadvantage is that the user is then restricted to being authenticated on the one phone. By having profile information stored on the network, users would be able to login at any network access point, thus enhancing their personal mobility. It would also enable the network operator to monitor the success or failure rates for possible misuse. Where a preference was expressed, the opinions from the survey respondents clearly favoured the profile being held in the handset, with 52% of respondents selecting this option. By contrast, 26% favoured the network, while 20% did not mind and 2% did not understand the question. Given that the respondents were probably not be giving much thought to the issue of the network overheard, it is likely that their preference for the handset-based profile relates to the ability to retain control over their own profile data.

Discussion

Although the results have suggested the desire for a greater level of security, this clearly represents something of a contradiction when it is considered alongside the fact that many respondents do not even use the current method that has been provided for them. This suggests that it is the security technique, rather than the concept of security, that users are rejecting, and as such a move towards non-intrusive methods of authentication may provide the protection that users are looking for, but without the associated inconvenience that is currently perceived. Although fingerprint scanning was a favourite technique, it does not necessarily lend itself to non-intrusive implementation, as the user would need to place his/her finger on the scanner. If the scanner were to be placed in a natural area on the phone where a finger would normally be placed to hold the device, then the level of intrusiveness would be arguable. Voiceprint lends itself to both one-off and continuous monitoring of voice communications, but would either lose its non-intrusiveness, or the ability to authenticate, on data communications. Keystroke analysis also lends itself to non-intrusive authentication for one-off monitoring and would be more likely to facilitate continuous monitoring during the utilisation of keypad-oriented services.

Since none of the biometrics discussed can provide non-intrusive authentication for all possible scenarios, and secondly cannot provide 0% false acceptance and false rejection rates, it would seem logical to provide a hybrid model of authentication, using a number of non-intrusive methods as first/second line security, with the PIN (or some other knowledge-based methods) providing a fallback method if needed. Current research is focusing upon the realisation and evaluation of such an approach, and the authors are investigating the application of biometrics in this context. A preliminary investigation of keystroke analysis has been conducted to assess whether it is possible to authenticate people from the way in which they dial numbers on a standard GSM handset. Although the results are not conclusive at this stage (with false acceptance and false rejection errors of around 15% being observed), it is considered that refinement of the technique may yield better performance. The full results from this element of the investigation will be published in due course.

Conclusions

The survey findings have indicated a weakness of the current security provisions on mobile handsets, in that the authentication technology is optional and, therefore, not used by a large proportion of users. However, subscribers have shown both the need and the desire for additonal security, and have responded positively towards a number of alternative authentication techniques. At the same time, the results showed that many respondents do not use the current security techniques that are available to them. In view of this, it can be assumed that a non-intrusive method of authentication may prove to be most acceptable and widely utilised by end users.

With the introduction of the third generation phones, a range of new advanced services will become available, services that the respondents in the survey indicated that they would be keen to use. In this context, the protection of users' information must become a prime concern, especially when considering the possible sensitivity of the data, and the need for a sucessful transition into a multi-billion dollar mcommerce market. Security is, essential, and approaches must be employed that subscribers will tolerate and use.

References

[1] Intekom. 2001. *Latest Global & Regional Cellular Statistics*. http://home.intekom.com

[2] ITU. 2001. Full description of the IMT-2000 (International Mobile Telecommunications) initiative located on the ITU (International Telecommunications Union) website at www.itu.int, Radio-Communication (ITU-R) division.

[3] UMTS Forum. 1998. *The Path towards UMTS – Technologies for the Information Society*. Report no. 2. The UMTS Forum. http://www.umts-forum.org/reports.html

[4] 3GPP. 2000. *Terms of Reference: Services and System Aspects – Working Group 3*. TSG SA WG3 – Security. http://www.3gpp.org/TSG/ToR/TSG-SA/sa3-tor.htm

[5] Jobusch, D.L. and Oldehoeft, A.E. 1989. "A Survey of Password Mechanisms: 1", *Computers & Security*, Vol. 8, No. 7: 587-604.

[6] Cope, B.J.B. 1990. "Biometric Systems of Access Control". *Electrotechnology*, April/May: 71-74.

[7] CSI. 2001. '2001 CSI/FBI Computer Crime and Security Survey', *Computer Security Issues & Trends*, vol. VII, no. 1. Computer Security Institute. Spring 2001.

[8] SAGEM. 2000. "SAGEM points a finger at GSM", Press Release, 24 January 2000. http://www.sagem.com/en/communiques-en/cp-1sem2000-en.htm#mc 959 id empreinte

[9] Miller, S. 2001. "Mobile sales soar, driven by teenage market", MediaGuardian report, 23 May 2001. http://media.guardian.co.uk/newmedia/story/0,7496,495263,00.html.

[10] Polemi, D. 1997. *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication*, Institute of Communication and Computer Systems, National Technical University of Athens. April 1997.

[11] Legget, J. and Williams, G. 1988. "Verifying identity via keystroke characteristics", International Journal of Man-Machine Studies, 28.

[12] Joyce, R. and Gupta, G. 1990. "Identity Authentication Based on Keystroke Latencies", Communications of the ACM, Volume 33, February 1990.

H9 Poster Presentation

Third International Networking Conference (INC 2002)

July 2002, University of Plymouth, Plymouth, UK.

"Biometrics – Authentication You Are Born With"

Biometrics - *Authentication You Are Born With*

An investigation into Advanced Authentication by Mr.Philip Rodwell, PhD Research Student, University of Plymouth, United Kingdom.

Biometrics ?

Biometrics is based on measurable physiological and/or behavioral characteristics. Biometric security utilises the distinctive and unique nature of these characteristics.

Although traditionally used in high security scenarios: defence establishments, prison visitor systems etc. they have recently seen a boom owing to the growing need for more secure and reliable identity verification within modern electronic systems and networks.

This expansion has fundamentally been made possible by a massive growth in computing power and subsequent economies-of-scale of biometric hardware and powerful micro-controllers.

A Matter of Convenience...

Biometrics are as much about convenience as they are about security.

Biometrics are impossible to forget, like a knowledge based password system and they are impossible to leave-at-home or lose like a token based system.

Many biometric acquisition techniques can be performed transparently, therefore authentication can be performed continuously, offering much stronger security than traditional point-of-entry techniques.

HOWEVER, it should be noted that IF your biometric is somehow compromised, how do you easily get a replacement?

H10 Poster Presentation

Biometrics 2002

November 2002, Excel Centre, London, UK.

"Non-Intrusive Biometric Authentication for Mobile Devices"

Poster awarded 'Best Student Prize'

Non-Intrusive Biometric Authentication for Mobile Devices

Nathan Clarke, Dr Steven Furnell, Prof Paul Reynolds and Philip Rodwell
Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK

Introduction

In the vast majority of mobile devices, the only protection against unauthorised use comes from a Personal Identification Number (PIN). With the convergence of devices and the extended range of services that will be accessible through 3G networks, a strong argument exists for stronger and more robust methods of user authentication. The research relates to the investigation, design, and evaluation of advanced subscriber authentication techniques, suited to application within the context of a mobile device. This poster presents the continuing research from the Network Research Group, University of Plymouth, which is being conducted in collaboration with Orange.

The Current Problem

Subscriber authentication to current mobile networks, such as GSM, is relatively limited, with the vast majority of devices relying upon a Personal Identification Number (PIN) method.

A survey of 275 mobile subscribers reveals the problems of the PIN approach:

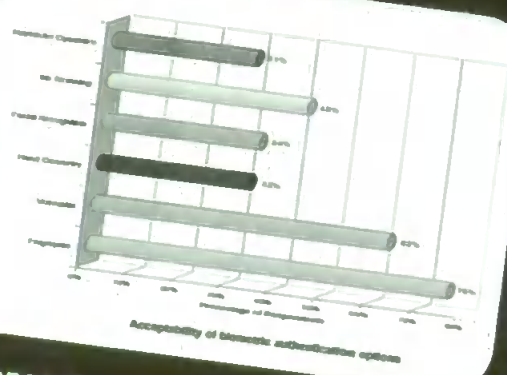
- 39% of respondents do not use the PIN
- 42% of respondents find the PIN an inconvenient authentication method
- 58% of respondents do not have confidence in the PIN

Third generation (3G) devices demand improved authentication methods due to their convergence with Personal Digital Assistant (PDA) devices, and the subsequent expansion in the range of possible services enabled as a result. The potential consequences of a masquerade will be far more severe.

The survey revealed opportunities for enhancing authentication methods:

- ✓ 64% of respondents believe more security to be a good idea
- ✓ 55% of respondents supported a continuous and non-intrusive authentication method

Respondents' opinions regarding the use of biometric techniques on a mobile handset are illustrated in the graph on the right.



The New Concept

Facial Recognition
- An internal camera could capture a digital image
- Processed to determine a series of characteristic vectors

Service Utilisation
- Profiling subscriber's typical interactions with their device
- Analysing usage patterns, utilising time and frequency

Keystroke Dynamics
- Based upon analysis of typing rhythm
- May be implemented in static or dynamic modes

Iris Scanning
- Based upon unique characteristics of the iris
- Could be done using a high resolution still image camera

Signature Recognition
- A touch screen could capture the user's signature
- May be measured statically or dynamically

Voice Verification
- An internal microphone could capture voiceprint information
- Verification may be text dependant or independant

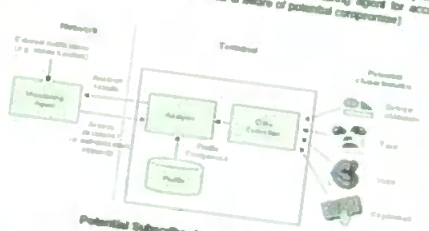
The Realisation

Authentication Framework

Advanced authentication may be handled within a flexible framework, which intelligently monitors the available biometrics based upon the subscriber and their current activity.

For example, voice verification could be utilised during a voice call, but during an e-commerce transaction it could be replaced by other characteristics that are more appropriate to the context, such as keystroke analysis.

The terminal would collect and locally compare the data against the subscriber profile, and then securely send the results to a network-based monitoring agent for access decisions (ensuring that the network operator is aware of potential compromise).



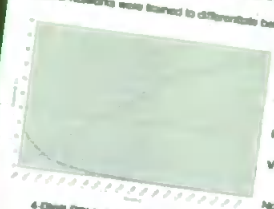
Example Biometric – Keystroke Dynamics

Initial experiments have been conducted to assess keystroke dynamics on a mobile phone - to authenticate users by assessing their interactions on the keypad.

The initial study involved 16 test subjects and utilised two types of keypad input: 4-digit PIN codes and standard telephone numbers.

Keystroke data was collected from a modified mobile phone handset, connected to a PC, in order to preserve the tactile context of a mobile device.

Neural networks were trained to differentiate between legitimate users and impostors.



4-Digit PIN Network Performance

	FAR	FRR	EER
PIN code	7.9	3.1	8.5
Fixed telephone	4.5	1.8	3.2
Varying telephone	17.1	15.1	18.1

Note: Individual networks performed as well as 0% FRR and 0% FAR

Summary

The capabilities of 3G mobile systems open up a range of new service opportunities and, as a consequence, impose new requirements for security. The survey findings indicated a weakness of the current provisions, in that the authentication technology is optional and, therefore, often unused. However, subscribers have shown the desire for additional security, and have responded positively to a number of alternative techniques. Given that many respondents do not use the current security techniques that are available to them, it can be assumed that a non-intrusive method of authentication may prove to be most acceptable and widely utilised by end users. Mobile architectural frameworks can be specified to support this, and suitable biometrics can be identified to provide the underlying authentication methods.

UNIVERSITY OF PLYMOUTH

www.network-research-group.org

orange

H11 Additional Published Works

Additional published works are expected to emerge from the HAT-related research.

At the time of going to press a journal paper entitled, *"A novel non-intrusive authentication mechanism for application in mobile devices"* was in final draft, pending submission to the journal, **Computers and Security** *(Elsevier Science).*

Appendix I

Patent Material

Appendix I Patent Material

I1 Patent Proposal

Copy of an original patent proposal, based on the core PhD Research, presented to Orange lawyers (circa2001), for legal formatting and formal UK & US patent application submission.

Patent Proposal

ABSTRACT

A proposal of an idea for a novel continuous, non-intrusive, biometric authentication technique; for initial application in a mobile communications environment. The technique will utilise wave propagation effects to extract and exploit a unique biometric based on the physiological modification of sound waves. The primary realisation of this technique will exploit the exclusive topography of the human head.

AUTHOR

Philip Rodwell, Orange PLC, Bristol.

CONTRIBUTORS

Prof. Paul Reynolds, Orange PLC, Bristol.
Dr. Steven Furnell, Manager Network Research Group, DCEE, University of Plymouth.

INTRODUCTION

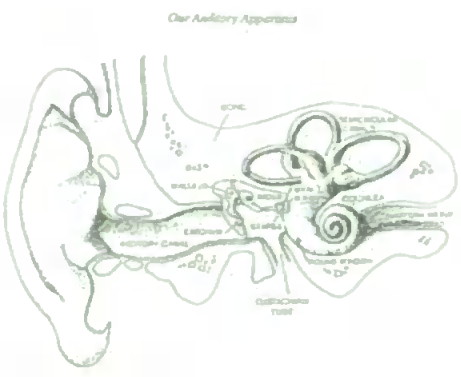
Security provisions within the current GSM European mobile telecommunications network are primarily aimed at secure communications through data encryption and *terminal* authentication via use of a smart card, the Subscriber Identity Module (SIM). The proposed services of 3rd Generation (3G) mobile systems demand a more secure subscriber based authentication system in order to provide greater protection of more advanced and personal information in the event of a masquerade attack.

Current security provision includes an International Mobile Equipment Identifier (IMEI), to identify and protect the Mobile Equipment (ME) and a Personal Identification Number (PIN), to authenticate a user to and subsequently access the SIM. As the PIN technique is fundamentally Point of Entry (PoE) authentication, is not physiologically personal to the actual subscriber, and is based on transferable knowledge, it is vulnerable to masquerade attacks. This proposal presents a technique, which can potentially overcome the problems of the current system, being both suitable for continuous authentication and being based on subscriber's individual physiological signatures. Such biometric authentication approaches are advantageous in that they cannot be forgotten, lost or stolen in the same way that would be possible with approaches based upon secret knowledge or the possession of physical tokens.

What is required is a biometric that can be applied effectively and non-intrusively in a telephony context.

DESCRIPTOR

When a person hears a sound, owing to the unique topography and sensitivity of the inner-ear and auditory canal, individually, that person will perceive a different sound to a second person listening to the same sound[1].



The idea proposes a way of utilising this exclusivity as a novel means of biometric authentication; with an initial leaning towards mobile communications.

[1] Auditory Perception, A New Analysis and Synthesis. R.M.Warren, ©Cambridge University Press, 1999.

While it is possible to identify numerous other physiological and behavioural biometric techniques (e.g. fingerprint recognition, face recognition), none are ideally suited to transparent and non-intrusive application within a voice telephony context.

The closest usable biometric authenticator for telephony is speaker verification, in which the subscriber may be authenticated based upon the analysis of their voice characteristics. Some examples of work in this important area are the European Commission funded, CAVE[1] and PICASSO[2] projects.

In practice, however, the speaker verification technique has several drawbacks that limit its application and the degree of protection that it can provide:

- Verification is most effective (accurate) when the user profile is constructed on the basis of known words or phrases. In this context (text dependent), authentication can only occur when the specific phrase(s) that have been profiled are then spoken – which may give limited opportunity in many scenarios.
- Continuous (text independent) verification is less reliable, which could lead to false rejections and, therefore, result in inconvenience to legitimate subscribers.
- The technique requires the subscriber to be speaking before an authentication judgement can be made. In certain scenarios, this would not need to be the case in order for security to be compromised (e.g. retrieval of sensitive messages from a voicemail system may require no spoken interaction from an impostor).

In developing a system to utilise the new proposed idea, one important criteria is the non-intrusive nature of the technique. This system transparency presents the novel possibility of continuous authentication within the mobile telephony environment.

There are a number of approaches to realising this novel biometric signature:

- The primary approach will use an inband (human auditory range) pulse of pink noise (band-limited white noise), of short enough duration as to be undetectable, or at least non-intrusive to the user. The resulting reflected spectrum will then be used as the authenticating signature. Using an inband pulse will prevent any onboard filtering from modifying the generated pulse and negate the need for modified hardware. The pulse will be initiated from the network as and when requested by the security architecture leaving control of security access to the network operator. In addition, it is possible to signature the pink noise pulse by varying the amplitudes at selected frequencies, adding a further level of security to the system. This pink noise signature could possibly be used unique to the network/user or varied according to a specific algorithm.
- A second approach will utilise the telephones side-tone (via the ether) as a reference sound source, making a comparison with the same original sound as it is detected at the earpiece of a handset after traversing through the skull of the user to the ear. The modified sound, will have been subjected to, in addition to other effects, the wave effects of reflection, summing, differencing in addition to the absorption characteristics of the varying densities and thicknesses of the solids and fluids in the human skull. This difference spectrum from the direct/indirect path could be used as the authentication signature, being compared with a reference stored in either the terminal or the network. One disadvantage of this system is that it would require the user to speak, or at least make a sound into the system before authentication could take place, unless a suitable pink noise tone was utilised for initial PoE authentication purposes.

[1] The European CAller VErification Project. http://www.ptt-telecom.nl/cave/
[2] Picasso Project. http://www.picasso.kpn-telecom.nl/

- A third approach is the use of frequencies in the out-of-band, ultra-sonic frequencies. This technique could adopt either of the first two principles of signature creations, being based either on reflection or modified transition owing to the skull. As this technique would be inaudible to the user, authentication would be completely transparent.

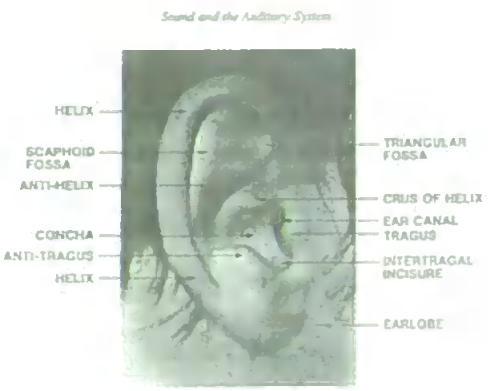
All of the above systems would need to be able to update user authentication signatures dynamically as a users physiology changes with age and/or health.

In determining the viability of the system for commercial application, research is addressing:

- the practicality of the resultant system;
- additional hardware requirements, specifically for mobile application;
- system efficiency in extracting exclusive biometric signatures;
- false Acceptance and False Rejection rates;
- the level of transparency to the end user.

BACKGROUND

After conducting an extensive literature search, I am unaware of any research applying these techniques to the area of authentication security. The nearest area of similar research involves ear-prints[1], based on outer ear geometry. This is applied in a similar way to the established biometric technique of hand geometry[2], where a unique signature is devised from a physical image of the user's hand, based purely on its 2-dimensional shape.



ADDITIONAL COMMENTS

Potentially such a system would be extremely secure, as working in continuous authentication mode, only an authorised users ear in close proximity to the ear-piece would permit the system to release information. As an extension to the system, it should also be possible to develop the system to work with a separate earpiece for authentication purposes outside of the mobile communications arena, e.g. PC based user authentication.

[1] Automatic Ear Recognition. - http://www.isis.ecs.soton.ac.uk/
Image, Speech and Intelligent Systems Research Group.
Department of Electronics and Computer Science, University of Southampton

[2] Hand Geometry Website: http://www.hand-scan.com

I2 UK Patent Application - no. 2,375,205

Copy of UK Patent Application: "Determining Identity Data for a User"

(12) UK Patent Application (19) GB (11) 2 375 205 (13) A

(43) Date of A Publication 06.11.2002

(21) Application No 0110931.3

(22) Date of Filing 03.05.2001

(71) Applicant(s)
Orange Personal Communications Services Limited
(Incorporated in the United Kingdom)
St. James Court, Great Park Road,
Almondsbury Park,Bradley Stoke, BRISTOL,
BS32 4QJ, United Kingdom

(72) Inventor(s)
Philip Maurice Rodwell
Paul Reynolds

(74) Agent and/or Address for Service
R.G.C.Jenkins & Co
26 Caxton Street, LONDON, SW1H 0RJ,
United Kingdom

(51) INT CL[7]
A61B 5/117

(52) UK CL (Edition T)
G4H HTG H1A H13D H14A
G4R RET R1X
U1S S2204 S2215

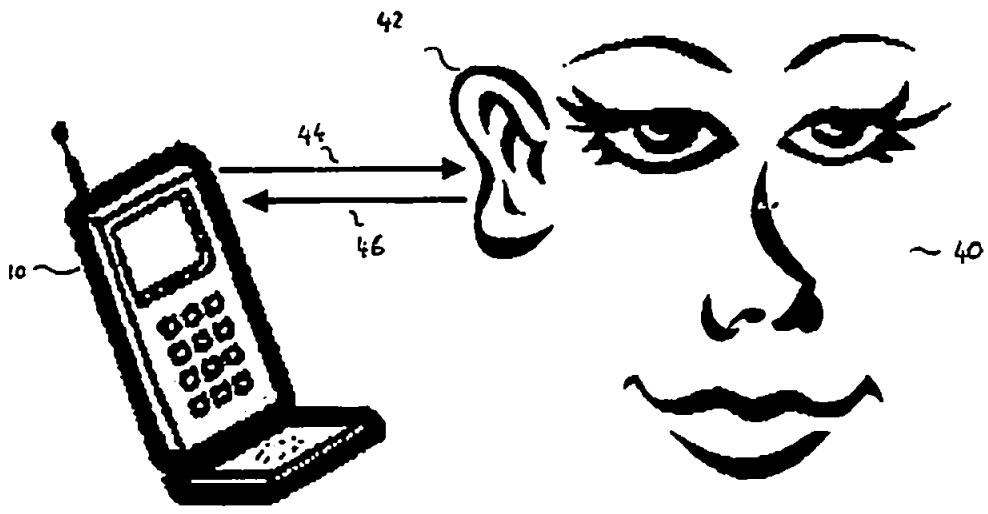
(56) Documents Cited
GB 1450741 A US 5787187 A

(59) Field of Search
UK CL (Edition T) G4H HTG , G4R RET
INT CL[7] A61B 5/00 5/117 , G07C 9/00
Online:WPI, EPODOC, JAPIO

(54) Abstract Title
Determining identity of a user

(57) An interacted sound signal resulting from an original sound signal interacting with a part of the body of the user is representative of a physiological characteristic of the user and is used to identify the user.

FIG. 3



GB 2 375 205 A

1

DETERMINING IDENTITY DATA FOR A USER

Field of the Present Invention

The present invention relates to determining identity data for a user of an electronic device using a biometric technique. More particularly, but not exclusively, the present invention relates to using a biometric technique for authentication of a user of a telephony device.

Background of the Present Invention

Historically, there has been a general need for user authentication in the fields of electronics, data processing, computer networks and telecommunications. For example, the user of an automated telling machine (ATM) will normally be required to enter a personal identification number (PIN) before being allowed access to bank account services or funds. Similarly, for user access to private or public computer networks, such as an intranet or the Internet, typically the user will need to enter a user name and password before being allowed access. Internet Service Providers (ISPs) typically implement authentication, authorisation and accounting (AAA) systems to a) ascertain who the user is (authentication), b) determine access rights for the user (authorisation), and c) set up the necessary charging mechanisms for the user (accounting). The processes of authorisation and accounting are both dependent on successful authentication. Similarly, individual network resources such as Web sites, and other services, may also implement conditional access systems using, for example, user name and password entry.

In the field of mobile communications, in particular with second generation systems such as the Global System for Mobile communications (GSM), security is implemented through data encryption and subscriber authentication via use of a smart card known as the Subscriber Identity Module (SIM). The mobile station may optionally be set to require entry of a PIN before allowing access to the data stored on the SIM and non-emergency calls.

However, the technique of requiring a PIN is not truly personal to the subscriber and is based on transferable knowledge – i.e. the PIN code. Thus, the technique is vulnerable to masquerade attacks whereby a third party obtains or successfully guesses the PIN number and is able to masquerade as the subscriber. The same can be said of any technique requiring a password, such as the user name and password technique.

Furthermore, PIN or user name and password techniques are point of entry techniques, which only perform authentication periodically on the occurrence of certain events, such as on switching on a mobile station. Thus, an unauthorised party obtaining a previously authenticated mobile station may not be required to undergo further authentication until the mobile station is switched off or runs out of power. This problem is exacerbated with improvements in power capacity of mobile stations whereby mobile stations need hardly ever be switched off.

Furthermore, the problems of point of entry authentication techniques, such as requiring a PIN code or a user name and password, are becoming exacerbated with the advent of "always on" telecommunications access whereby a user of a fixed or mobile telecommunications device is provided

with continuous access to network resources and services without having to periodically dial up a connection and undergo point of entry authentication.

With the advent of third generation mobile communications technologies, and with the convergence of fixed and mobile telecommunications and computer networks, more services of greater value will be accessible via both mobile and fixed stations. More advanced and potentially more sensitive information, such as bank account information, geographic location, private correspondence and so on, will be accessible from a multitude of telecommunications devices. For example, e-mail, e-commerce transactions, and location-based services may be available to users of both mobile and fixed telecommunications devices.

Thus, it can be seen that there will be an increasing need for greater security in future mobile and fixed telecommunications systems and, in particular, a need for enhanced, truly personal, and continuous, user-based authentication.

International publication no. WO 99/08238 discloses a portable client personal digital assistant (PDA) with a microphone and local central processing unit (CPU) capable of processing biometric data to provide user verification. The device includes a modem to provide direct communications with peripheral devices and is capable of transmitting or receiving information through wireless communication. Optionally, a biometric sensor may be provided for collecting biometric data such as a finger, thumb or palm print, a handwriting sample, a retinal vascular pattern, or a combination thereof, to provide biometric

verification. However, the document discloses a preference for biometric verification through voice data.

International publication no. WO 99/45690 discloses a protected access system for controlling access to networks such as telephone networks, which may use biometric characteristics for subscriber identification. The document discloses using any of three biometric characteristics for authentication, namely, retina patterns, speech or voice characteristics of fingerprints.

International publication no. WO 99/54851 discloses a device, such as a mobile telephone and SIM card, comprising sensors for detecting biometric characteristics and a data processing device for determining authentication information from the biometric characteristics. The document discloses using any of three biometric characteristics, namely, fingerprints, retinal patterns, and voice or speech characteristics.

US Patent no. 5,872,834 discloses a telephone provided with a contact imaging device for obtaining biometric data to identify or authenticate the user. Contact imaging devices are stated to include electrical contact imaging sensors such as capacitative fingerprint imagers and optical contact imaging sensors such as optical fingerprint imagers. The user must make physical contact with an electrical or optical component of the imager for biometric data to be obtainable.

The CAVE project (CAller VErification in banking and telecommunications) and the follow up project PICASSO (Pioneering Caller Authentication for Secure Service Operation) are known research projects in the field of speaker verification in which authentication of a user of a telephony

service is based upon an analysis of their voice characteristics. Both research projects focussed on text-dependent speaker verification, in the sense that the verification procedure assumes that the text of the spoken utterance is known by the verification system. This results in more accurate verification, but requires the user to utter known words or phrases for authentication may take place.

One problem with voice or speaker verification techniques is that for accuracy, the subject must utter pre-determined words or phrases, which may not be possible in many cases and may become inconvenient and tiresome for the subject. Furthermore, if text dependent techniques are used, continuous verification is not possible. In any case, whether text dependent or independent techniques are used, the subject is required to be speaking before an authentication judgement can be made. These and other problems are solved by the present invention.

Summary of the Present Invention

According to a first aspect of the present invention, there is provided a method of determining identity data in respect of a user of an electronic device such as a telephony device, the method comprising the steps of:

a) receiving an interacted sound signal resulting from an original sound signal interacting with a part of the body of the user;

b) deriving a signature from at least the interacted sound signal, the signature being representative of a physiological characteristic of the user, the physiological characteristic not being a characteristic of the voice or speech of the user;

c) determining the identity data in dependence on the signature.

The interacted sound signals may be received more or less continuously and provide data from which a physiological characteristic of the user can be determined. Thus an enhanced, truly personal, and, if desired, continuous, user-based method of authentication is provided.

According to a preferred embodiment of present invention, the electronic device generates the original sound signal. Preferably, the original sound signal is undetectable or non-intrusive to the user. The sound signal may be outside the human auditory frequency range or, alternatively, inside the human auditory frequency range but of sufficiently short duration so as to be undetectable or unobtrusive. Thus, identity data may be determined by comparing an original sound signal, with known characteristics, to the received interacted sound signal, without disturbing the user.

According to another preferred embodiment of present invention, the original sound signal has a pre-selected characteristic, and the step of determining the identity data in dependence on the signature is dependent on the pre-selected characteristic. Thus, improved accuracy of authentication may be achieved by selecting a sound characteristic appropriate to the physiological characteristic being used for authentication.

Preferably, in a first determination of identity data, the original sound signal has a first pre-selected characteristic, and in a second determination of identity data, the original sound signal has a second pre-selected characteristic different to the first pre-selected characteristic. For example, the sound characteristic may be selected on a random or pseudo-random basis. Thus,

security is generally improved against, for example, masquerade attacks by providing a varying "challenge" to the user.

Preferably, the pre-selected characteristic is selected by a process performed externally to the electronic device. Thus security is further improved against, for example, attacks in which the security processes of the electronic device have been determined by the attacker.

Preferably, the pre-selected characteristic is selected in dependence on a) an identity or characteristic of an authorised user of the electronic device; b) an identity or characteristic of an authorised user of a service accessible via the electronic device; and/or c) the identity or characteristic of a provider of a service accessible via the electronic device. Thus, a variable level of security may be selected appropriate to the particular circumstances of use.

In a further embodiment of the present invention, there is provided a method according to the first aspect, comprising the step of:

aa) receiving the original sound signal, wherein the original sound signal is produced by the user and the signature is derived from the interacted and original sound signals.

For example, the original sound signal may be the voice or speech of the user. Thus, authentication may take place using an original sound signal generated by the user without the need for the electronic device to generate sound signals for that purpose.

According to another preferred embodiment, the electronic device is a telephony device and comprises an earpiece for generating sound signals a mouthpiece for receiving sound signals and other sound signal processing

apparatus. Thus, authentication of a user of the telephony device may be performed by receiving and/or processing sound or signals representing sound using apparatus present in the device for other purposes, thereby taking advantage of existing apparatus in the telephony device.

According to another preferred embodiment, the physiological characteristic relates to the physiology of the auditory apparatus or head of the user. Thus, advantage is taken of the unique topographics of the human ear or human head to perform accurate authentication.

The method of determining identity data may be carried out by a telecommunications network comprising an electronic device connectable to one or more network nodes, or by a stand-alone electronic device. The electronic device may be a telephony device such as a mobile station of a mobile telecommunications network.

According to a second aspect of the present invention, there is provided a telephony device arranged to process sound signals for use in determining identity data in respect of a user, the telephony device comprising audio signal coding/decoding apparatus arranged to use a first data coding format for coding or decoding the voice or speech of a user and a second different data coding format for coding or decoding sound signals for use in determining identity data of a user. Thus, the data coding format used may be optimised to the characteristics of the sound signals used when determining identity data in respect of a user.

According to a third aspect of the present invention, there is provided a telephony device comprising a locally accessible data store, the data store

storing data representing one or more original sound signals, the telephony device being controllable by a remote device to generate a original sound signal using data stored in the data store and to receive an interacted sound signal resulting from the original sound signal interacting with a part of the body of a user for use in determining identity data in respect of the user. Thus, the quality of original sound signal generated may be guaranteed and network traffic reduced.

According to a fourth aspect of the present invention, there is provided a telephony device comprising a loudspeaker for generating an original sound signal and a microphone for receiving an interacted sound signal resulting from an original sound signal having interacted with a part of the body of a user of the telephony device, the telephony device being arranged so that, when in normal operation by a user, the loudspeaker and microphone are located adjacent to an ear of the user.

According to a fifth aspect of the present invention, there is provided an earpiece or headpiece for use with a telephony device, the earpiece or headpiece comprising a loudspeaker for generating an original sound signal and a microphone for receiving an interacted sound signal resulting from an original sound signal having interacted with a part of the body of a user of the telephony device, the earpiece or headpiece being arranged so that, when in normal operation by a user, the loudspeaker and microphone are located adjacent to an ear of the user.

According to a sixth aspect of the present invention, there is provided a method of determining identity data in respect of a user of an electronic device, the method comprising:

a) receiving a sound signal resulting from an original sound signal having interacted with a part of the body of the user;

b) determining the identity data in dependence on a characteristic derived from the received interected sound signal.

Further aspects of the invention are as set out in the appended claims.

There now follows, by way of example only, a detailed description of preferred embodiments of the present invention in which:-

Figure 1 is a schematic diagram of a known mobile station of a mobile telecommunications network for use in the present invention;

Figure 2 is schematic diagram of an adapted mobile station for use in the present invention;

Figure 3 is a schematic diagram showing the process of determining identity data for a user in a first mode where the mobile station generates the original sound;

Figure 4 is a schematic diagram showing the process of determining identity data for a user in a second mode where the mobile station generates the original sound; and

Figure 5 is a schematic diagram showing the process of determining identity data for a user in a third mode where the user generates the original sound.

Detailed Description of Preferred Embodiments of the Present Invention

Figure 1 is a schematic diagram of a known mobile station of a second generation mobile telecommunications network, such as a GSM network, for use in the present invention. The mobile station 10 comprises a transmit/receive aerial 12, a radio frequency transceiver 14, a speech coder/decoder 16 connected to a loudspeaker 18 and a microphone 20, a processor circuit 22 and its associated memory 24, an LCD display 26 and a manual input port (keypad) 28, and a removable SIM 30. The loudspeaker 18 and microphone 20 are both connected to the processor circuit 22 via speech coder/decoder 16. Speech coder/decoder 16 comprises an analogue to digital converter (ADC) connected to microphone 20 and a digital to analogue converter (DAC) connected to loudspeaker 18. Mobile station 10 may communicate with a mobile telecommunications network using radio signals transmitted by transmit/receive aerial 12.

Typically, coder/decoder 16 uses a digital coding format optimised for efficient transmission of data representing voice or speech over low bandwidth communications channels. In particular, the coding formats used generally do not substantially represent sound at frequencies outside the human auditory range. Thus, in embodiments of the present invention using standard, unadapted mobile stations for second generation mobile networks, the process of determining identity data is preferably performed using in-band (i.e. within the human auditory frequency range) sound signals. Alternatively, in embodiments of the present invention using out-of-band sound signals, in particular ultra-sonic signals, an adapted mobile station may be used in which

coder/decoder 16 is arranged to use a different data coding format, when being used for the purposes of determining identity data, the different data coding format being suited to represent the sound signals at the frequencies used.

Figure 2 is schematic diagram of an adapted mobile station for use in the present invention. The mobile station 10 of Figure 2 is as described with reference to Figure 1, save that an additional microphone 32 is located at the earpiece close to loudspeaker 18 and also connected to speech coder/decoder 16. A further ADC may also be provided in coder/decoder 16 connected to microphone 32 for separately converting the analogue signals received from microphone 32. Again, for embodiments of the present invention using out-of-band sound signals, coder/decoder 16 may be arranged, when being used for the purposes of determining identity data, to use a data coding format suited to represent the sound signals at the frequencies used. According to a further embodiment of the present invention, the functions of loudspeaker 18 and microphone 32 are both performed by a single sound transceiver located at the earpiece of mobile station 10.

Although Figures 1 and 2 show mobile stations using inbuilt loudspeakers and microphones, "hands-free" equipment consisting of a loudspeaker and/or microphone separate from but connectable to the mobile station, may also be used in the present invention. Furthermore, an adapted hands-free earpiece or headpiece comprising a loudspeaker and microphone corresponding to loudspeaker 18 and microphone 32 of Figure 2 may also be used when connected to an adapted mobile station such as shown in Figure 2.

Alternatively, the loudspeaker and microphone of the adapted earpiece or headpiece may be combined into a single sound transceiver as described above.

The process of determining identity data for a user of mobile station 10 may be controlled by either processor 22, the processor of SIM 30, or by one or more nodes of the mobile telecommunications network. We shall refer to the entity controlling the process of determining identity data as the authenticating entity. In embodiments of the present invention in which original sound signals are generated by loudspeaker 18 of mobile station 10, digital data representing an original sound signal, formatted in a suitable data coding format, is sent by the authenticating entity to coder/decoder 16 for decoding and causing the generation of the original sound signal at loudspeaker 18. Conversely, interacted sound signals received by microphones 20 or 32 are coded into digital data by coder/decoder 16 and are sent to the authenticating entity. Where the authenticating entity is the processor of SIM 30, the data is sent over the mobile station/SIM interface. Where the authenticating entity is a node of the mobile telecommunications network, the data is sent over the radio interface via radio frequency transceiver 14 and transmit/receive aerial 12.

In embodiments of the present invention in which original sound signals are generated by loudspeaker 18 of mobile station 10, a plurality of different original sound signals may be used. The authenticating entity may generate the data representing the original sound signal to be used, or select from one or more pre-generated data items stored in a data store accessible to it. For example, where processor 22 is the authenticating entity, pre-generated data may be stored in memory 24. Where, the processor of SIM 30 is the

authenticating entity, pre-generated data may be stored in a memory of the SIM card. Alternatively, the authenticating entity may control the generation of the data representing the original sound signal by another device, or control another device to select from one or more pre-generated data items stored in a data store accessible to the other device. For example, where the authenticating entity is a node of the network, the node may choose a pre-determined original sound signal to be used and control processor 22, or the processor of SIM 30, to generate or select pre-generated data representing the chosen signal.

Figure 3 is a schematic diagram showing the process of determining identity data for a user in a first mode where mobile station 10 generates the original sound signal. Mobile station 10 is an adapted mobile station as described with reference to Figure 2. When in normal operation, a user holds mobile station 10 to his or her head 40 so that the loudspeaker 18 and microphone 32 of the earpiece are adjacent an ear 42 of the user. When authentication is required by the authenticating entity, coder/decoder 16 is controlled to cause loudspeaker 10 to generate an original sound signal 44. Preferably, the generated sound signal is pink noise (i.e. band-limited white noise) within the human auditory range (approximately 20 – 20,000 Hz), so that the standard data coding format of coder/decoder 16 may be used. However, the signal is of short enough duration so as to be undetectable or at least non-intrusive to the user. In an alternative embodiment, out-of-band (i.e. outside the human auditory range) sound frequencies may be used, in particular ultra-sonic frequencies which enable a higher physical resolution than lower frequency signals. Ultra-sonic frequencies would be undetectable to the user thus

resulting in completely transparent authentication. In this case, coder/decoder 16 is arranged to use a data coding format suited to the frequency range of the signals 44 and 46 as described above.

Additionally, the original sound signal 44 may have a pre-determined signature. For example, a pink noise signal may be adapted by varying the amplitudes of the signal at selected frequencies. By selecting from a plurality of original sound signals with different signatures, further security is added to the system in that an attacker is presented with a varying "challenge". The sound signal 44 of pre-determined signature is preferably selected by the authentication entity. Selection may be on a random or pseudo-random basis, or in dependence on a) an identity or characteristic of an authorised subscriber of the mobile network, b) an identity or characteristic of an authorised user of services accessible via the mobile station and/or c) an identity or characteristic of the provider of services accessible via the mobile station. For example, varying levels of security may be required by different users or by different telecommunications networks or by the providers of services or resources available using the mobile station. More specifically, a subscriber authorised for voice calls only, may, for example, only be required to undergo low-level authentication, whereas a subscriber authorised to access highly personal information via the mobile station, such as bank account information or geographic or positioning information, may be required to undergo high-level authentication.

The interacted sound signal 46, having been reflected in the soft tissues of the inner ear and auditory canal of the user, is then received by microphone

32 and converted into digital data by coder/decoder 16. The digital data output from coder/decoder 16 is then sent to the authenticating entity for analysis. Data representing the original sound signal 44 and the received interacted sound signal 46 are then compared to determine a signature corresponding to the physiological topology of the inner ear and auditory canal of the user. This may be performed using known techniques of digital audio signal processing such as using Fast Fourier Transforms (FFTs) to obtain a frequency response. The generated physiological signature is then compared to a pre-stored physiological signature or statistical model for the authorised subscriber to determine authenticity. If the determined signature matches within a predetermined level of tolerance, then the user of mobile station 10 is authenticated. However, if the determined signature does not match within the tolerance level, then the user of mobile station 10 is not authenticated. The process of determining the degree of match between the generated physiological signature and the pre-stored physiological signature uses known techniques of statistical pattern matching.

The pre-stored physiological signature or statistical model for the authorised subscriber of mobile station 10 may be determined in much the same manner as for subsequent determination of identity data according to the present invention. More specifically, on registration, the subscriber may be required to undergo a process to determine the physiological signature or statistical model to be stored and used for subsequent determination of identity data. By generating a plurality of test original sound signals and receiving the corresponding interacted signals a single average physiological signature or a

more detailed statistical model indicating a normal range for the subscriber's physiological signature may be derived . Preferably, the test signals generated are sufficiently numerous so that an accurate average physiological signature or statistical model may be determined. Optionally, the test signals may comprise signals of different sound signatures corresponding to the different sound signatures that may be selected by the authenticating entity on subsequent determination of identity data.

Furthermore, because the topography of the inner ear and auditory canal may change gradually over time, especially with children and through ill health, the pre-stored signature or statistical model for a subscriber may be varied gradually over time in dependence on data determined during normal authentication procedures. For example, whilst a user presenting a radically different physiological topography will be rejected since the difference will exceed the predetermined level of tolerance, a gradual and consistent change within the predetermined level of tolerance may be interpreted as a normal change in the topography of the inner ear and auditory canal, and the pre-stored signature or statistical model for that subscriber altered accordingly.

Figure 4 is a schematic diagram showing the process of determining identity data for a user in a second mode where the mobile station generates the original sound. Mobile station 10 is the standard mobile station as described with reference to Figure 1. The processes for determining identity data are as described above for the first mode where the mobile station generates the original sound, save that the interacted sound signal 48 is received by the standard microphone 20 located at the mouthpiece of mobile station 10 rather

than by microphone 32 located at the earpiece. Thus, after loudspeaker 18 has generated an original sound signal 44, the interacted sound signal 48 is received by microphone 20 having traversed through the skull and soft tissues of the head of the user, and a signature is derived corresponding to the physiological topography of bone and soft tissues forming the user's head.

Optionally, sound signals transmitted from loudspeaker 18 to microphone 20 directly through the body of mobile station 10 may be cancelled from the received sound signal using signal processing techniques. For a given make and model of mobile station, the physical arrangement of components of the mobile station in normal operation is fixed. Thus, for a given original sound signal, a cancellation signal corresponding to the sound transmitted directly through the body of mobile station 10 may be determined and subtracted from the signal received by microphone 20. Thus a sound signal corresponding to the interaction of the original sound signal with substantially only the head of the user of mobile station 10 may be determined. In embodiments using hands-free equipment, the effect of sound transmission through the body of the mobile station is greatly reduced and cancellation may not be necessary.

Figure 5 is a schematic diagram showing the process of determining identity data for a user in a third mode where the user generates the original sound. Mobile station 10 is an adapted mobile station as described with reference to Figure 2. Whilst it has been described above how mobile station 10 may be used to generate the original sound for determining identity data for a user, in this alternate embodiment, the original sound signal is generated by the user of mobile station 10 – i.e. the original sound is the voice or speech 50

of the user. This original sound signal is received directly by microphone 20, located at the mouthpiece, and indirectly, having traversed the head of the user, by microphone 32, located at the earpiece. From these two received signals, a signature corresponding to the physiological topography of the bone and soft tissue of the user's head may be determined and the determination of identity data carried out as described above.

When generating the pre-stored signature or statistical model for an authorised subscriber, rather than the mobile station generating a series of test sound signals, as described above, the user is required to speak into the mobile station. Preferably, the user is required to recite a standard training passage of text of sufficient length and vocal variety to provide an accurate signature or model for the user.

Whilst preferred embodiments of the present invention using mobile stations of a mobile telecommunications network have been described above, it will be appreciated that the present invention has application to fixed or mobile telecommunications stations, for example telephone stations in networks such as the public switched telephone network (PSTN), fixed or mobile terminals or computing devices for access to private or public data networks, such as an intranet or the Internet, and in general to any electronic device where user authentication is needed, whether the device is capable of telecommunications or not. Furthermore, whilst it has been described that the physiological characteristics used for determining identity data are the topography of the inner ear and auditory canal, or the head of the user, it will be apparent that other physiological characteristics may be used, such as the topography of other parts

of the body of the user or other physiological characteristics measurable using sound.

CLAIMS:

1. A method of determining identity data in respect of a user of an electronic device, the method comprising the steps of:

a) receiving an interacted sound signal resulting from an original sound signal interacting with a part of the body of the user;

b) deriving a signature from at least the interacted sound signal, the signature being representative of a physiological characteristic of the user, the physiological characteristic not being a characteristic of the voice or speech of the user;

c) determining the identity data in dependence on the signature.

2. A method according to claim 1, wherein the electronic device generates the original sound signal.

3. A method according to claim 2, wherein the original sound signal is undetectable or non-intrusive to the user.

4. A method according to claim 2 or 3, wherein the frequency range of the original sound signal is substantially within the human auditory frequency range.

5. A method according to any of claims 2 to 4, wherein the frequency range of the original sound signal is substantially outside the human auditory frequency range.

6. A method according to any of claims 2 to 5, wherein the original sound signal has a pre-selected characteristic, and the step of determining the identity data in dependence on the signature is dependent on the pre-selected characteristic.

7. A method according to claim 6, wherein, in a first determination of identity data, the original sound signal has a first pre-selected characteristic, and in a second determination of identity data, the original sound signal has a second pre-selected characteristic different to the first pre-selected characteristic.

8. A method according to claim 6 or 7, wherein the pre-selected characteristic is selected on a random or pseudo-random basis.

9. A method according to any of claims 6 to 8, wherein the pre-selected characteristic is selected by a process performed externally to the electronic device.

10. A method according to any of claims 6 to 9, wherein the pre-selected characteristic is selected in dependence on an identity or characteristic of an authorised user of the electronic device.

11. A method according to any of claims 6 to 10, wherein the pre-selected characteristic is selected in dependence on an identity or characteristic of an authorised user of a service accessible via the electronic device.

12. A method according to any of claims 6 to 11, wherein the pre-selected characteristic is selected in dependence on the identity or characteristic of a provider of a service accessible via the electronic device.

13. A method according to claim 1, comprising the step of:

aa) receiving the original sound signal;

wherein the original sound signal is produced by the user and the signature is derived from the interacted and original sound signals.

14. A method according to claim 13, wherein the original sound signal is the voice or speech of the user.

15. A method according to any preceding claim, wherein the electronic device is capable of telephony and comprises an earpiece for generating sound signals and a mouthpiece for receiving sound signals.

16. A method according to claim 15, wherein the interacted sound signal is received at the earpiece.

17. A method according to claim 15, wherein the interacted sound signal is received at the mouthpiece.

18. A method according to any of claims 15 to 17, when dependent on any of claims 2 to 12, wherein the original sound signal is generated at the earpiece.

19. A method according to any of claims 15 to 17, when dependent on any of claims 2 to 12, wherein the original sound signal is generated at the mouthpiece.

20. A method according to any preceding claim, wherein the physiological characteristic relates to the physiology of the head of the user.

21. A method according to claim 20, wherein the physiological characteristic relates to the physiology of the auditory apparatus of the user.

22. Apparatus for performing the method of any preceding claim.

23. A computer program or computer programs for performing the method of any of claims 1 to 21.

24. A telecommunications network comprising an electronic device connectable over a telecommunications link to one or more network nodes, the telecommunications network being arranged to perform the method of any of claims 1 to 21.

25. A telecommunications network according to claim 24, wherein the electronic device performs step a) and the one or more nodes perform steps b) and c).

26. A telephony device arranged to perform the method of any of claims 15 to 21.

27. A mobile station of mobile communications network arranged to perform the method of any of claims 15 to 21.

28. A telecommunications network comprising a telephony device and one or more network nodes, the telecommunications network being arranged to perform the method of any of claims 15 to 21 wherein the telephony device performs step a) and the one or more nodes perform steps b) and c).

29. A telephony device arranged to process sound signals for use in determining identity data in respect of a user, the telephony device comprising audio signal coding/decoding apparatus arranged to use a first data coding format for coding or decoding the voice or speech of a user and a second

different data coding format for coding or decoding sound signals for use in determining identity data of a user.

30. A telephony device comprising a locally accessible data store, the data store storing data representing one or more original sound signals, the telephony device being controllable by a remote device to generate an original sound signal using data stored in the data store and to receive an interacted sound signal resulting from the original sound signal interacting with a part of the body of a user for use in determining identity data in respect of the user.

31. A telephony device comprising a loudspeaker for generating an original sound signal and a microphone for receiving an interacted sound signal resulting from an original sound signal having interacted with a part of the body of a user of the telephony device, the telephony device being arranged so that, when in normal operation by a user, the loudspeaker and microphone are located adjacent to an ear of the user.

32. An earpiece or headpiece for use with a telephony device, the earpiece or headpiece comprising a loudspeaker for generating an original sound signal and a microphone for receiving an interacted sound signal resulting from an original sound signal having interacted with a part of the body of a user of the telephony device, the earpiece or headpiece being arranged so that, when in normal operation by a user, the loudspeaker and microphone are located adjacent to an ear of the user.

33. A method of determining identity data in respect of a user of an electronic device, the method comprising:

a) receiving a sound signal resulting from an original sound signal having interacted with a part of the body of the user;

b) determining the identity data in dependence on a characteristic derived from the received interacted sound signal.

34. Apparatus substantially as hereinbefore described with reference to Figures 1 or 2.

ABSTRACT:

According to the present invention there is provided a method of, apparatus for, and computer programs for determining identity data in respect of a user of an electronic device, the method comprising the steps of:

a) receiving an interacted sound signal resulting from an original sound signal interacting with a part of the body of the user;

b) deriving a signature from at least the interacted sound signal, the signature being representative of a physiological characteristic of the user, the physiological characteristic not being a characteristic of the voice or speech of the user;

c) determining the identity data in dependence on the signature.

1/5

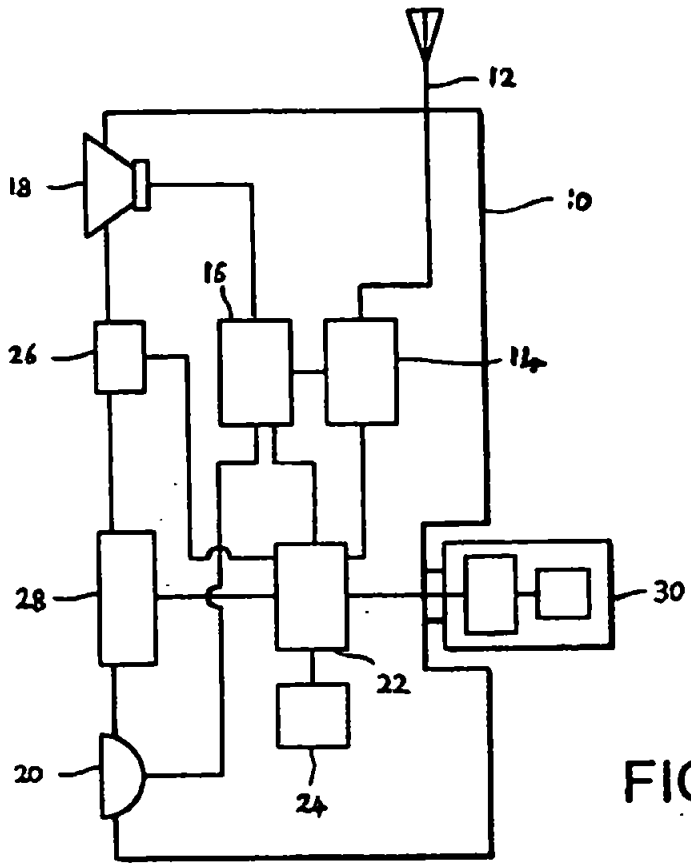


FIG. 1

2/5

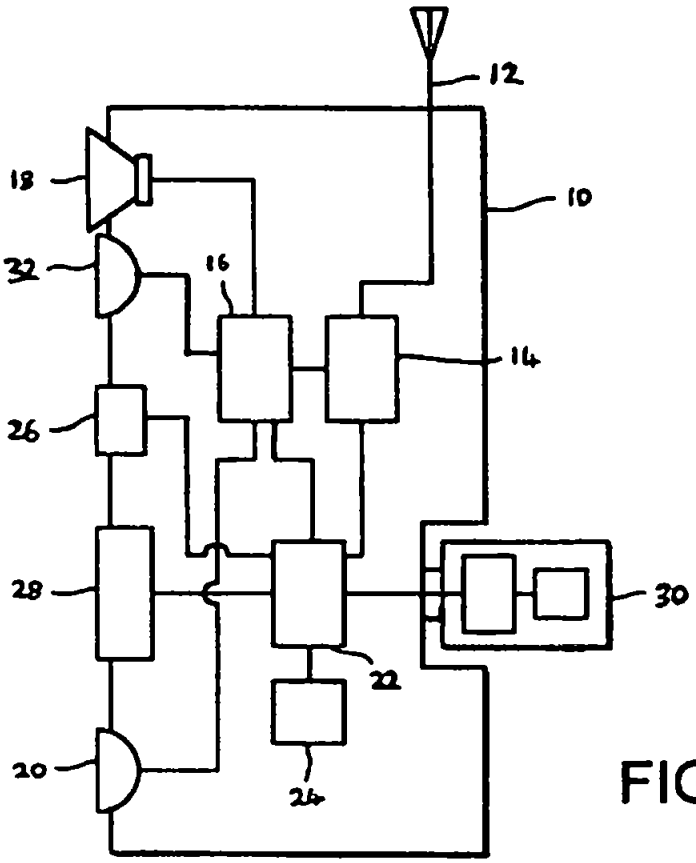


FIG. 2

3/5

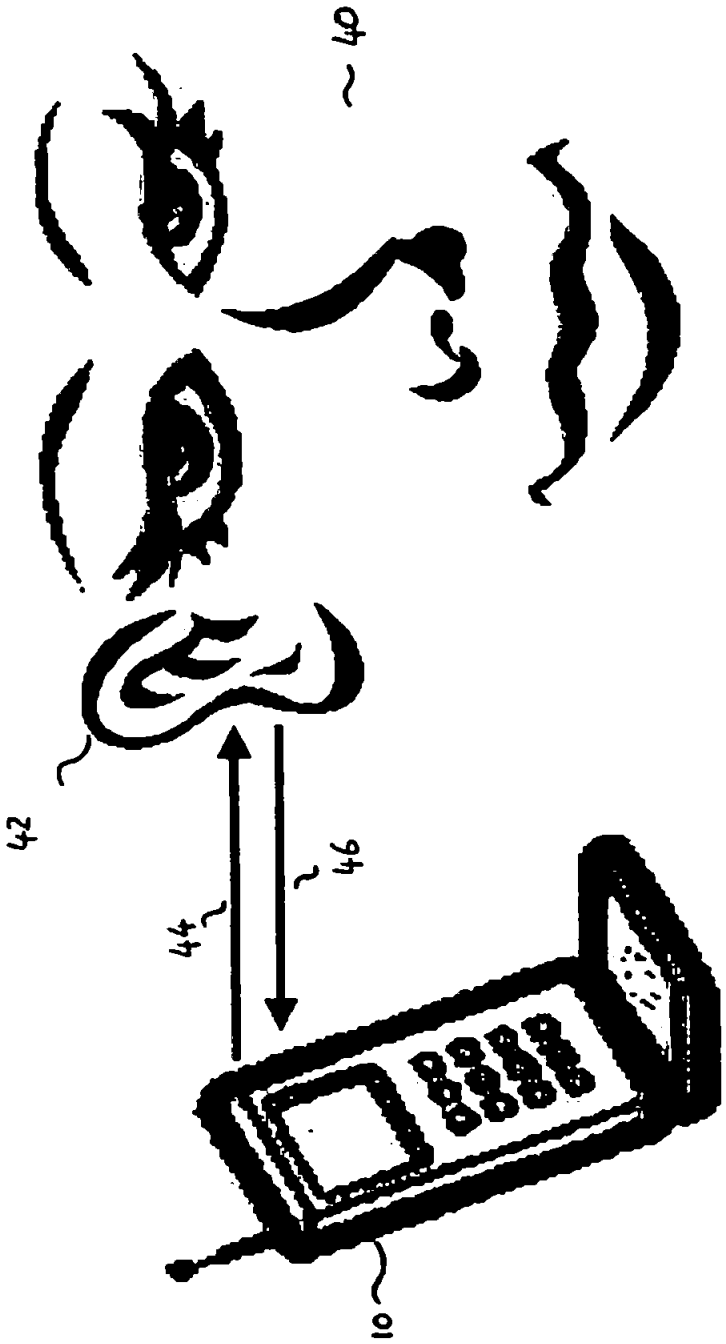


FIG. 3

4/5

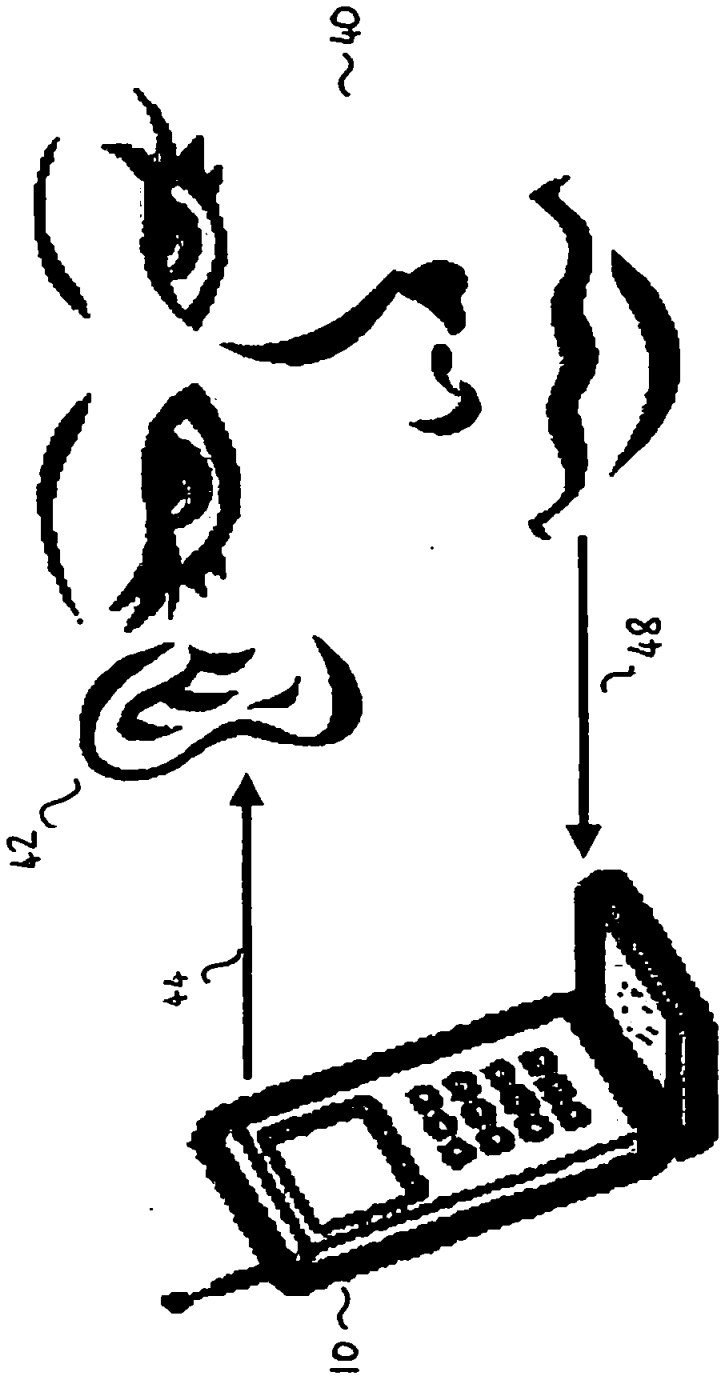


FIG. 4

5/5

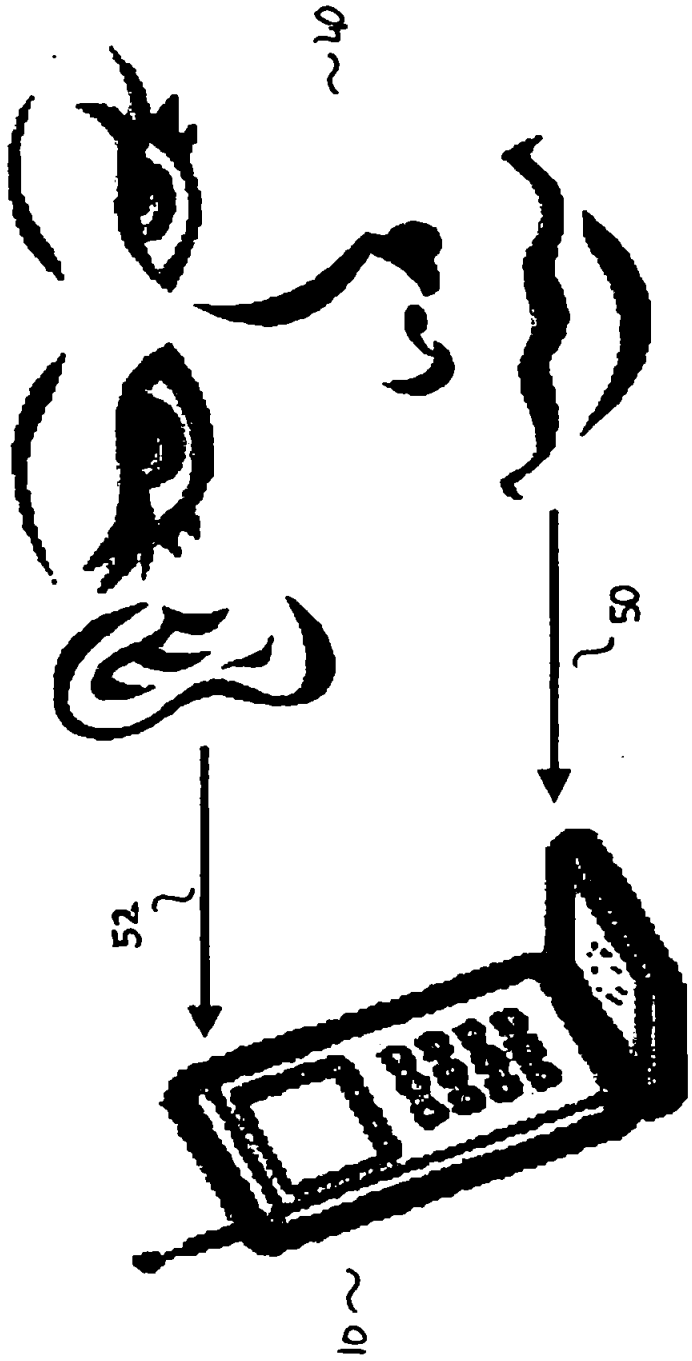


FIG. 5

I3 US Patent Application - no. 10/476,588

Copy of US Patent Assignment: "Determining Identity Data for a User"

ASSIGNMENT

WHEREAS, we,

Philip M. Rodwell, a citizen of Great Britain with an address at 17 Lower Fairfield, St. Germans, Cornwall PL12 5NH, Great Britain, and **Paul Reynolds**, a citizen of Great Britain with an address of St. James Court, Great Park Road, Almondsbury Park, Bradley Stoke, Bristol BS12 4QJ, Great Britain, ASSIGNORS, are the inventors of the invention in **DETERMINING IDENTITY DATA FOR A USER**, for which we have executed an application for a Patent of the United States, which was filed in the United States on October 31, 2003 as application no. 10/476,588.

WHEREAS, **ORANGE PERSONAL COMMUNICATIONS SERVICES LIMITED**, a British company having a place of business at St. James Court, Great Park Road, Almondsbury Park, Bradley Stoke, Bristol BS12 4QJ, Great Britain, ASSIGNEE, is desirous of obtaining our entire right, title and interest in, to and under the said invention and the said application:

NOW, THEREFORE, in consideration of the sum of One Dollar ($1.00) to us in hand paid, and other good and valuable consideration, the receipt of which is hereby acknowledged, we, the said ASSIGNORS, have sold, assigned, transferred and set over, and by these presents do hereby sell, assign, transfer and set over, unto the said ASSIGNEE, its successors, legal representatives and assigns, the entire right, title and interest in, to and under the said invention, and the said United States application and all divisions, renewals and continuations thereof, and all Patents of the United States which may be granted thereon and all reissues and extensions thereof;

AND WE HEREBY authorize and request the Commissioner of Patents and Trademarks of the United States, to issue the same to the said ASSIGNEE, its successors, legal representatives and assigns, in accordance with the terms of this instrument;

AND WE HEREBY covenant and agree that we have full right to convey the entire interest herein assigned, and that we have not executed, and will not execute, any agreement in conflict herewith;

AND WE HEREBY further covenant and agree that we will communicate to the said ASSIGNEE, its successors, legal representatives and assigns, any facts known to us respecting said invention, and testify in any legal proceeding, sign all lawful papers, execute all divisional, continuing, and reissue applications, make all rightful oaths, and generally do everything possible to aid the said ASSIGNEE, its successors, legal representatives and assigns, to obtain and enforce proper protection for said invention.

IN WITNESS WHEREOF, the undersigned inventors have affixed their signatures.

26th MAY 2004
Date

Philip M. Rodwell

On this 26 day of MAY, 2004, before me appeared **Philip M. Rodwell**, to me known and known to me to be the person of that name, who signed and sealed the foregoing instrument, and acknowledged the same to be his free act and deed.

26th May 2004
Date

KABrewer.
Witness
KERRY ANNE BREWER.

Docket No. 59015-00601

1 of 2

1 May 2004

Date

Paul Reynolds

On this _____ day of _____, 2004, before me appeared **Paul Reynolds**, to me known and known to me to be the person of that name, who signed and sealed the foregoing instrument, and acknowledged the same to be his free act and deed.

Date

Witness

Docket No. 59015-00601

2 of 2

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

0819/PTO Rev. 6/93 — U.S. Department of Commerce Patent and Trademark Office	Attorney Docket Number	59015-00601
	First Named Inventor	Philip M. Rodwell
COMBINED DECLARATION (37 CFR 1.63) AND POWER OF ATTORNEY FOR UTILITY OR DESIGN PATENT APPLICATION	*COMPLETE IF KNOWN*	
	Application Number	10/476,588
	Filing Date	October 31, 2003
	Group Art Unit	Unknown
[ ] Declaration Submitted with Initial Filing OR [X] Declaration Submitted after Initial Filing	Examiner Name	Unknown

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

DETERMINING IDENTITY DATA FOR A USER

the specification of which (*Title of the Invention*)

[ ] is attached hereto

OR

[X] was filed on 03 May 2002 as United States Application Number or PCT International Application Number PCT/GB02/02074 and was amended on (MM/DD/YYYY) [_____] (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37 Code of Federal Regulations. § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code § 119 (a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365 (a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
0110931.3	Great Britain	05/03/2001	[ ]	[ ]	[X]
			[ ]	[ ]	[ ]
			[ ]	[ ]	[ ]
			[ ]	[ ]	[ ]
			[ ]	[ ]	[ ]

[ ] Additional foreign application numbers are listed on a supplemental priority sheet attached hereto:

[Page 1 of 3]

DECLARATION	Page 2

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	[ ] Additional provisional application numbers are listed on a supplemental sheet attached hereto.

I hereby claim the benefit under Title 35, United States Code § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of Title 35, United States Code § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application Number	PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (*if applicable*)

[ ] Additional U.S. or PCT international application numbers are listed on a supplemental priority sheet attached hereto.

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Name	Registration Number	Name	Registration Number
David R. Yohannon	37,480	Christopher M. Tobin	40,290
John N. Coulby	43,565	Mark W. Rygiel	45,871
Seth A. Watkins	47,169	Gregory M. Murphy	52,494

[ ] Additional attorney(s) and/or agent(s) named on a supplemental sheet attached hereto.

Please direct all correspondence to:

Christopher M. Tobin
Collier Shannon Scott, PLLC
3050 K Street NW, Suite 400
Washington, D.C. 20007 U.S.A.

Telephone	(202) 342-8508	Fax	(202) 342-8451

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor: [ ] A petition has been filed for this unsigned inventor

Given Name	Philip	Middle Initial	M.	Family Name	Rodwell	Suffix	
Inventor's Signature	X P M Rodwell				Date	Y 26. MAY. 2004	
Residence: City	Cornwall	State		Country	Great Britain	Citizenship	Great Britain
Mailing Address	17 Lower Fairfield						
Mailing Address	St. Germans						
City	Cornwall	State		Zip	PL12 5NH	Country	Great Britain

[X] Additional inventors are being named on supplemental sheet(s) attached hereto

[Page 2 of 3]

DECLARATION								ADDITIONAL INVENTOR(S) Supplemental Sheet
Name of Additional Joint Inventor, if any:				[ ] A petition has been filed for this unsigned inventor				
Given Name	Paul	Middle Initial		Family Name	Reynolds		Suffix	
Inventor's Signature	x				Date	x 1 May 2004		
Residence: City	Bristol	State		Country	Great Britain	Citizenship	Great Britain	
Mailing Address	St. James Court, Great Park Road							
Mailing Address	Almondsbury Park, Bradley Stoke							
City	Bristol	State		Zip	BS12 4QJ	Country	Great Britain	

Name of Additional Joint Inventor, if any:				[ ] A petition has been filed for this unsigned inventor			
Given Name		Middle Initial		Family Name		Suffix	
Inventor's Signature					Date		
Residence: City		State		Country		Citizenship	
Mailing Address							
Mailing Address							
City		State		Zip		Country	

Name of Additional Joint Inventor, if any:				[ ] A petition has been filed for this unsigned inventor			
Given Name		Middle Initial		Family Name		Suffix	
Inventor's Signature					Date		
Residence: City		State		Country		Citizenship	
Mailing Address							
Mailing Address							
City		State		Zip		Country	
[ ] Additional inventors are being named on supplemental sheet(s) attached hereto							

[Page 3 of 3]

Notes

(Notes)

Table A-4: Thesis Statistics

	Chapter	Pages	Words	Figures	Tables
Core	Abstract	1	397	n/a	n/a
	Chapter 1	10	2575	1	0
	Chapter 2	36	8335	9	2
	Chapter 3	20	4474	13	0
	Chapter 4	41	9599	13	5
	Chapter 5	30	6905	12	1
	Chapter 6	46	6791	47	3
	Chapter 7	40	6837	32	1
	Chapter 8	7	2143	0	0
	Total (Core)	**231**	**48056**	**127**	**12**
	Total (Thesis)	**437**	**80034**	**131**	**15**

Table A-5: Development System

Hardware	Description
Processor	AMD Athlon XP2400+ (2000MHz)
Memory	1GB Corsair TwinX 3200C2PT (133)
Harddisk	Hitachi 250Gb, WD 200GB; 7200rpm
Graphics card	Asus A9600 (ATI core)
Soundcard	Creative Audigy2
Monitor	Sony CPD-4201G (19")
Printer	Epson Stylus Photo 950
Mouse	Logitech MX1000 (laser)