2016-09-01

# MORI: An Innovative Mobile Applications Data Risk Assessment Model

Alotaibi, S



10.20533/jitst.2046.3723.2016.0062
Journal of Internet Technology and Secured Transaction
Infonomics Society

# MORI: An Innovative Mobile Applications Data Risk Assessment Model

Saud Alotaibi[1], Steven Furnell[1, 2, 3] and Nathan Clarke[1, 2]
[1]*Centre for Security, Communications and Network Research*
*Plymouth University*
*Plymouth, UK*
[2]*Security Research Institute*
*Edith Cowan University*
*Perth, Western Australia*
[3] *Centre for Research in Information and Cyber Security*
*Nelson Mandela Metropolitan University*
*Port Elizabeth, South Africa*

## Abstract

*The daily activities of mobile device users range from making calls and texting to accessing mobile applications, such as mobile banking and online social networks. Mobile phones are able to create, store, and process different types of data, and these data, whether personal, business, or governmental, are related to the owner of the mobile device. More specifically, user activities, such as posting on Facebook, is sensitive and confidential processes with varying degrees of social risk. The current point-of-entry authentication mechanisms, however, consider all applications on the mobile device as if they had the same level of importance; thus maintaining a single level of security for all applications, without any further access control rules. In this research, we argue that on a single mobile application there are different processes operating on the same data, with different social risks based on the user's actions. More specifically, the unauthorised disclosure or modification of mobile applications data has the potential to lead to a number of undesirable consequences for the user, which in turn means that the risk is changing within the application. Thus, there is no single risk for using a single application. Accordingly, there is a severe lack of protection for user data stored in mobile phones due to the lack of further authentication or differentiated protection beyond the point-of-entry. To remedy that failing, this paper has introduced a new risk assessment model for mobile applications data, called MORI (Mobile Risk) that determines the risk level for each process on a single application. The findings demonstrate that this model has introduced a risk matrix which helps to move the access control system from the application level to the intra- process application level, based on the risk for the user action being performed on these processes.*

## 1. Introduction

The use of mobile devices in our daily lives has grown steadily, due to the combination of mobility with 24/7 multi-connectivity. In particular, mobile phones are used to perform activities such as sending emails, transferring money via mobile internet banking, making calls, texting, surfing the internet, viewing documents, storing medical, confidential and personal information, shopping online and playing games. Additionally, a forecast estimates that the number of smartphone users will reach about 44.9 million by 2017 [1]. Statista [2] asserts that, in 2020, expected growth of mobile app revenue will be 101 billion US dollars, up from 41.1 billion U.S. dollars in 2015.

For the remaining part of this paper, Section 2 presents a background assessment of current mobile authentication mechanisms, while Section 3 elaborates on some previous work related to risk assessment for mobile devices. A detailed explanation of the proposed model is presented in Section 4. Finally, Section 5 describes conclusions and future work.

## 2. Mobile Authentication Mechanisms

The most popular mobile device security is based upon secret knowledge approaches, such as the use of passwords or PINs, though these are considered inconvenient approaches [3]. Interestingly, 36% of mobile phone users did not safeguard their mobile phones by applying a PIN or password approach [4] and 44% of the surveyed respondents changed their password only once a year or less [3]. This method is a point-of-entry (PoE) technique, which means that the user needs to be verified only at the beginning of a session. Thus, an imposter is able to access all services, applications, and information without further authentication. McAfee [4] shows that the vast majority of respondents did not change the default password after purchasing the mobile device. Moreover, half of the users had passwords that were used by others, and 15% saved their password on the mobile device. As a result, this technique is considered insufficient for safeguarding mobile devices [5]. With the Android password pattern, the user is required to drag his/her finger across a touch screen on the three by three adjacent contact dots (i.e. to make a connecting pattern rather than remembering a sequence of characters) to access the mobile device. The points can never be used as

 

a combination again, thus producing fewer password combinations than the traditional PIN-based password technique. As a result, this method is vulnerable to a "brute force" [6].

With the evolution of mobile devices has come the introduction of a number of built-in features capable of sensing a variety of user biometric traits. These include features such as fingerprint-readers or face recognition technology, and are meant to provide a more secure authentication mechanism. Apple has presented a fingerprint technology that allows users to employ a fingerprint scan as a secure method of protecting their mobile devices. In Touch ID, the user places his/her fingerprints onto the home button and the system scans in order to build up a template, and then the user swipes his finger across the scanner to capture the fingerprint and complete the authentication process. This approach is quick (30 seconds to enroll five fingers) and normally the authentication is virtually instantaneous and fairly reliable [7]. Google, on the other hand, presents a face recognition technology that requires users to raise the phone and display their faces to the camera until a match is made. This method is considered to be intrusive compared to Touch ID. Generally, for an authentication method to be an ideal alternative, it is important that it meets the following essential criteria, as described by Elftmann [8]: elimination of the need for additional hardware; higher level of security; better memorability; simplicity and ease of use; and compatibility/applicability in various areas.

The current PoE authentication mechanisms consider all applications on the mobile device to have the same level of importance and maintain a single level of security for all applications, without applying any further access control rules [9]. However, Clarke et al. assert that different applications require different security provision. A bank account, for example, requires a different level of protection compared to an SMS message. Consequently, each application has a particular level of risk, which might serve to define the suitable level of security [10]. Although, several methods and systems from different perspectives have been proposed for solving the problem of mobile device security, only a few studies have investigated *when* to authenticate the mobile user. For instance, it is unnecessary to authenticate a user when the latter is reading the news or checking the weather forecast through a browser application [11].

Accordingly, it is important to ensure that the right person is allowed to access to the right information at the right time. As a result, any action that threatens data may lead to a number of undesirable consequences, such as embarrassment, financial loss, a threat to personal safety, or a breach of personal privacy or commercial confidentiality [12]. It is important, therefore, to classify data in order to strengthen data control and to apply risk analysis to each process. In addition, it is necessary to understand the nature of the risk to which these data are exposed in order to apply the appropriate protection.

Some of these active applications are considered sensitive and confidential, and are becoming of ever greater concern, and the risks are high for [13]. Mobile phones have gone from having a few megabytes of memory to having in excess 100 gigabytes, and so now have the potential to store vast amounts of data (albeit with much of this capacity often being consumed by music and video content which cannot typically be regarded as sensitive). However, we have seen relatively little parallel growth in the authentication technologies, with many phones still protected by nothing more than PINs/passwords, and even where more advanced methods are used (e.g. biometrics) they are currently making few inroads beyond PoE (although again there is some evidence of these being used for confirm purchases and other transactions, etc.).

## 3. Risk Assessment for Mobile Devices

Research has already been undertaken to establish how threats to mobile devices should be assessed. Ledermüller and Clarke (2011) [10] presented a mechanism to assess the risk level associated with particular apps and services in their study. In context of this research, applications or services that are associated with non-public information, such as emails and e-banking applications, would require a high level of security whereas normal applications would require a low level of security. Consequently, each application has a particular level of risk which might be an indicator of the suitable level of security. Similarly, Theoharidou et al., [14] proposed a risk assessment method for smartphones by identifying its assets and applicable threats. The method applies user input, with respect to impact valuation, coupled with statistics for calculating the likelihood of threats. The authors refined their previous work on smartphone risk assessment by proposing an approach for assessing the privacy risk of Android users [15]. Although, several methods and systems have been proposed from different perspectives for solving the problem of mobile security, none have explored the risk level for each process within the mobile applications. To the best of the author (s) knowledge, studying the risk for each process within the application has not been investigated.

Thus, the first step to explore the risk is to propose a taxonomy of mobile applications data. For this reasons, our previous work [16] presents a

 

novel taxonomy of mobile applications data, studying and analysing the risk for each process within the application. To accomplish this, 10 of the most popular mobile categories were analysed to gain a comprehensive understanding on various risk levels associated with user actions on those applications. The previous comprehensive analysis concluded that mobile application processes clearly have different levels of risk. From the set considered in the analysis, the results show that 81% of user actions are considered as risky processes, and may therefore merit additional protection beyond the PoE provision. Furthermore, the prior work [16] shows that, on a single mobile application, there are different processes operating on the same data, associated with different levels of social risk based on user actions. The previous work established impact classifications for key user actions within the ten most popular mobile applications, yielding the Table presented in the Table 1. Additionally, these findings suggest the need to move the access control system from the application level to the intra- process application level, on the basis of the risk to the user action being performed on these processes. As a result, the authors show that there is sensitive information beyond PoE, and that the risks are changing within applications. Hence the need to introduce a risk assessment model for mobile application data.

## 4. The MORI Model

Continuing from the foundation of previous work [16], this research has focused on introducing a risk assessment model for mobile applications data in order to determine the risk level for each process on a single application. The suggested risk model –MORI- would lead to the application of a usable approach for accessing mobile phones by considering the risk level for each sensitive process and introducing a level of authentication beyond the PoE approach. In the previous work, we argued that each application has different processes that utilise the underlying data, and can involve different levels of risk. More specifically, the unauthorised disclosure or modification of mobile applications data has the potential to lead to a number of undesirable consequences for the user. In this context, the methodology presented here is adapted from the CRAMM risk assessment approach. Impact types represent the way in which the data is affected if security is breached, and four main types are identified [12]:

- Disclosure: Unauthorized disclosure of data.
- Modification: Accidental or deliberate alteration of the data.
- Denial: Denial of access to data.
- Destruction: Destruction of the system or data.

In this context, data sensitivity has been considered in terms of the potential impact in the event of breaches of security that may result in loss of confidentiality, integrity and availability. Those factors are the basis to classified data. In this stage, only two impact types have been identified, based on Confidentiality and Integrity. In the previous work [16], there were three types of mobile application data taxonomy:

1. Based on impact type (disclosure, modification).
2. Based on information type (public, non-public).
3. Based on impact consequences.

The impact consequences have been adopted from CRAMM [12] as follows:

- C:Breach of commercial confidentiality
- D: Disruption
- E: Embarrassment
- F: Financial loss
- L: Legal liability
- PP: Breach of personal privacy
- PS: Threat to personal safety

These impact consequences are considered to be a relevant set of consequences in the context of mobile apps. For example, loss, modification, or unauthorized access to non-public data type can adversely affect an individual, and may cause financial loss from the user's bank account, or the leaking of personal information, such as, credit card numbers, bank accounts, and health information. Similarly, unauthorized disclosure such as access to photos and messages may result in embarrassment if shared by others. More specifically, different processes operate on the same application, with different levels of social risk, and so there is no a single risk for a single application.

Furthermore, there are complex personal aspects that need to be calculated: users may belong to different cultures and have received different levels of education. Traditionally, risk calculation is related to a combination of the Impact and Likelihood (i.e. Probability of Occurrence) as in the following equation:

$$\mathbf{Risk} = \mathbf{Impact\ consequence} \times \mathbf{likelihood} \quad (1)$$

Each specific impact type will have its own specific set of consequences.

Table 1. Mobile Applications categorization

| App | No. | User action | Impact type | Information type |
|---|---|---|---|---|
| **Facebook** | **1** | Search on Facebook | Disclosure | Public |
| | **2** | Read news feed | Disclosure | Non-public |
| | **3** | Read user profile | Disclosure | Non-public |
| | **4** | Post on a wall | Disclosure and Modification | Non-public |
| | **5** | Add photo/link | Disclosure and Modification | Non-public |
| | **6** | Tag friends/check in | Disclosure | Non-public |
| | **7** | Like | Disclosure and Modification | Non-public |
| | **8** | Comment | Disclosure and Modification | Non-public |
| | **9** | Share | Disclosure | Non-public |
| | **10** | Read notifications | Disclosure | Non-public |
| | **11** | Send message | Disclosure and Modification | Non-public |
| | **12** | Read message | Disclosure | Non-public |
| | **13** | Delete message | Disclosure and Modification | Non-public |
| | **14** | Join group | Modification | Non-public |
| | **15** | Voice call/video call | Modification | Non-public |
| | **16** | Change settings | Modification | Non-public |
| | **17** | Update information | Disclosure and Modification | Non-public |
| | **18** | Add friend | Modification | Non-public |
| | **19** | Remove friend | Modification | Non-public |
| **YouTube** | **1** | Search on YouTube | Disclosure | Public |
| | **2** | Watch on YouTube | Disclosure | Public |
| | 3 | Upload | Modification | Non-public |
| | **4** | Share | Disclosure | Non-public |
| | **5** | Like/dislike | Disclosure and Modification | Non-public |
| | **6** | Add a comment | Disclosure and Modification | Non-public |
| | **7** | Search history | Disclosure | Non-public |
| | **8** | Add to watch later | Modification | Non-public |
| | **9** | Subscribe | Modification | Non-public |
| | **10** | Unsubscribe | Modification | Non-public |
| | **11** | Read subscriptions | Disclosure | Non-public |
| | **12** | Read created playlists | Disclosure | Non-public |
| | **13** | Create a new playlist | Modification | Non-public |
| | **14** | Browse channels | Disclosure | Non-public |
| **Gmail** | **1** | Search on Gmail | Disclosure | Non-public |
| | **2** | Send an email | Disclosure and Modification | Non-public |
| | **3** | Read a new email | Disclosure | Non-public |
| | **4** | Read an old email | Disclosure | Non-public |
| | **5** | Reply to/forward | Disclosure and Modification | Non-public |
| | **6** | Delete an email | Disclosure and Modification | Non-public |
| | **7** | Chat on Gmail | Disclosure and Modification | Non-public |
| | **8** | Make a call | Disclosure and Modification | Non-public |
| | **9** | Change settings | Modification | Non-public |
| | **10** | Read user's contact | Disclosure | Non-public |
| | **11** | Read sent mail | Disclosure | Non-public |
| | **12** | Read important email | Disclosure | Non-public |
| | **13** | Read user's note | Disclosure | Non-public |
| **Google Drive** | **1** | Search on drive | Disclosure | Non-public |
| | **2** | Read file | Disclosure | Non-public |
| | **3** | Share file | Disclosure | Non-public |
| | **4** | Delete file | Disclosure and Modification | Non-public |
| | **5** | Upload file | Modification | Non-public |

| App | No. | User action | Impact type | Information type |
|---|---|---|---|---|
| | 6 | Download drive | Disclosure | Non-public |
| | 7 | Show recent file | Disclosure | Non-public |
| | 8 | Upgrade storage | Modification | Non-public |
| | 9 | Change settings | Modification | Non-public |
| Amazon | 1 | Search on Amazon | Disclosure | Public |
| | 2 | Read user's order history | Disclosure | Non-public |
| | 3 | Read user's account | Disclosure | Non-public |
| | 4 | Change user's account | Disclosure and Modification | Non-public |
| | 5 | Manage payment | Disclosure and Modification | Non-public |
| | 6 | Write a review | Disclosure and Modification | Non-public |
| | 7 | Add to basket | Modification | Non-public |
| | 8 | Proceed to checkout | Disclosure and Modification | Non-public |
| | 9 | Delete from basket | Disclosure and Modification | Non-public |
| | 10 | Edit basket | Disclosure | Non-public |
| | 11 | Share | Disclosure | Non-public |
| | 12 | Show browsing history | Disclosure | Non-public |
| | 13 | Create wish list | Modification | Non-public |
| | 14 | Sell on Amazon | Modification | Non-public |
| | 15 | Read wish list | Disclosure | Non-public |
| BBC News | 1 | Read news | Disclosure | Public |
| | 2 | Search on BBC News | Disclosure | Public |
| | 3 | Forecast the weather | Disclosure | Public |
| | 4 | Watch BBC News | Disclosure | Public |
| | 5 | Listen to BBC Radio 5 | Disclosure | Public |
| | 6 | Share | Disclosure | Non-public |
| Google Maps | 1 | Search on Google Maps | Disclosure | Public |
| | 2 | Read user's timeline | Disclosure | Non-public |
| | 3 | Add photo | Disclosure and Modification | Non-public |
| | 4 | Write a review | Disclosure | Non-public |
| | 5 | Share link | Disclosure | Non-public |
| | 6 | Read user's history | Disclosure | Non-public |
| | 7 | Search nearby places | Disclosure | Public |
| | 8 | Delete location history | Disclosure and Modification | Non-public |
| | 9 | Download all data | Disclosure | Non-public |
| | 10 | Get directions | Disclosure | Public |
| | 11 | Show traffic | Disclosure | Public |
| Gumtree | 1 | Search on Gumtree | Disclosure | Public |
| | 2 | Post an ad | Modification | Non-public |
| | 3 | Add a photo | Disclosure and Modification | Non-public |
| | 4 | Read user's ads | Disclosure | Non-public |
| | 5 | Read favorites | Disclosure | Non-public |
| | 6 | Send SMS/email | Disclosure and Modification | Non-public |
| | 7 | Delete ad | Disclosure and Modification | Non-public |
| | 8 | Change settings | Modification | Non-public |
| Google Photos | 1 | Search on Google Photos | Disclosure | Non-public |
| | 2 | Create a new album | Modification | Non-public |
| | 3 | Share | Disclosure | Non-public |
| | 4 | Delete an account | Disclosure and Modification | Non-public |
| | 5 | Back up and sync | Disclosure and Modification | Non-public |
| | 6 | Delete device copy | Disclosure and Modification | Non-public |
| | 7 | Add to album | Modification | Non-public |
| | 8 | Change setting | Modification | Non-public |
| Mobile Ba | 1 | Read transactions | Disclosure | Non-public |

| App | No. | User action | Impact type | Information type |
|---|---|---|---|---|
| | **2** | Read balances | Disclosure | Non-public |
| | **3** | Pay bill | Disclosure and Modification | Non-public |
| | **4** | Make transfer | Modification | Non-public |
| | **5** | Paym service | Disclosure and Modification | Non-public |
| | **6** | Read secure messages | Disclosure | Non-public |
| | **7** | Read account details | Disclosure | Non-public |
| | **8** | Change settings | Modification | Non-public |
| | **9** | Read products/services | Disclosure | Public |
| | **10** | Find HSBC branch | Disclosure | Public |
| | **11** | Read offers | Disclosure | Public |
| | **12** | Contact us/help | Disclosure | Public |

Each of these consequences could be assessed using a 1-10 rating scale, based on CRAMM, but this would make the methodology far too complex for the user. For simplicity, these impact consequences are rated at different levels, (low impact, medium impact, high impact), which provides a component of the measure of risk. Furthermore, it is possible to find disclosure and modification impact types on specific data, such as posting on a wall in a Facebook application. Thus, we have a 3 dimensional risk matrix containing the impact type (disclosure or modification or both), information type (public or non-public) and impact consequences (embarrassment, financial loss, data corruption, disruption, legal liability, threat to personal safety, breach of commercial confidentiality, breach of personal privacy). This risk model will apply to each action data on each application in order to investigate the risk.

To calculate the risk level based on the suggested risk model, there is a need to identify a process value (the degree of importance) and the maximum consequences of this action. In addition, the users are not in a position to make meaningful/informed decisions about the importance to them of the action and therefore, their perceptions are likely to be invalid. In this context, Process value (P) means the level of importance of this action is either:

- 0: not important
- 1: low importance
- 2: medium importance
- 3: high importance
- 4: very important

$$\textbf{Risk} = \textbf{Process value}, \max\{\mathbf{d}(\mathbf{c_{max}}), \mathbf{m}(\mathbf{c_{max}})\} \quad (2)$$

Where d: impact disclosure; m: impact modification; C: consequence.

The process value has been identified on the basis of the following equation:

$$\textbf{Process Value} = \textbf{Application Rank x Process Weight} \quad (3)$$

From Table 2, the application categories have been collected on the basis of the Google Play classification of the application type and been ranked on a scale from "1" to "3". The intention of this scale is to show the diversity between the levels of importance of the action within applications regarding the user's privacy and in order to appoint the sensitivity levels. Toward this goal, three number have been determined based on the level of importance of user data privacy "1" means the application category is not important, because it does not contain any user data (such as BBC Weather). "2" means a category of medium importance, because it contains user data, whereas "3" is an application category of high importance, because it includes-user sensitive data and any possible action on these data might concern, for example, the user's bank details These application categories have been pre-defined by experts for illustrating the idea of the suggested risk model.

Table 2. Application categories ranking

| Category | Rank | Example |
|---|---|---|
| Business | 2 | PDF Reader |
| Books and Reference | 2 | Kindle |
| Comics | 1 | Draw Cartoons |
| Communication | 3 | WhatsApp |
| Education | 2 | TED |
| Entertainment | 2 | BBC iPlayer |
| Finance | 3 | HSBC Bank |
| Food and Drink | 2 | Just Eat |
| Health and Fitness | 1 | Google Fit |
| Games | 1 | Pokémon |
| Lifestyle | 2 | IKEA Cat. |
| Maps | 2 | Google Maps |
| Medical | 2 | myGP |
| Music and Audio | 1 | SoundCloud |
| News and Magazines | 1 | BBC News |
| Personalisation | 2 | File Manager |
| Photography | 3 | Google Photos |

| | | |
|---|---|---|
| Productivity | 3 | Google Drive |
| Shopping | 3 | Amazon |
| Social | 3 | Facebook |
| Sports | 1 | Sky Sports |
| Tools | 1 | Alarm Clock |
| Travel and Local | 2 | Booking |
| Weather | 1 | BBC Weather |

The process weight will be given on the basis of the process type rankings from Table 3. These numbers are for illustration and have been pre-defined by experts. For example, reading news is considered a very low action due to the fact this action will be on a public data (disclosure public type), whereas sharing a user photo might be a high action (modification non-public type).

Table 3. Process weight

| **Process Type** | | **Process Weight** |
|---|---|---|
| Disclosure Public | **(DP)** | **0** |
| Modification Public | **(MP)** | **1** |
| Disclosure Non-public | **(DN)** | **2** |
| Modification Non-public | **(MN)** | **2** |

Furthermore, the risk levels might increase differently in relation to different consequences and the weight for each impact consequence will be given, as shown in Table 4. In this context, the weight value will be one of three (0, 1, and 2) to differentiate between impact consequences. Embarrassment, for example, will be higher than financial loss in the process type "disclosure non-public". The weight values for disclosure public will be 0 for all consequences, because there is no impact effect on the user. Therefore, there is no risk involved in the disclosure public type. Whereas the weight values for modification non-public will be 2 for all consequences. ((The reason for rating all consequence as 2 is because disclosure non-public will happen before the modification step, and therefore, the rate for all consequences should be bigger than the rate for all consequences in disclosure non-public type)). In the "modification public" type, the weight values will be different form one impact consequence to another. In practice, at the point of installation or at any time subsequently, the user has the chance/ability to set their own preferred rank based on how important they believe it to be and these weights have been pre-defined by experts for illustrating the idea of the suggested risk model.

Each consequence has three values (low, medium, and high) and each action or threat is mapped to at least one impact consequence. In cases where there is more than one impact consequence, the highest of the values is chosen. The resulting risk is measured on a scale of 0 to 6 according to the following criteria: 0 means No risk ,1 or 2 means low risk, 3 or 4 means medium risk, 5 or 6 means high risk.

Table 4. Consequences weight

| **PT / C** | **DP** | **DN** | **MN** | **MP** |
|---|---|---|---|---|
| **E** | 0 | 2 | 2 | 2 |
| **F** | 0 | 1 | 2 | 1 |
| **PP** | 0 | 2 | 2 | 1 |
| **L** | 0 | 1 | 2 | 1 |
| **PS** | 0 | 2 | 2 | 1 |
| **D** | 0 | 2 | 2 | 1 |
| **C** | 0 | 1 | 2 | 2 |

To assess the level of potential impact of each process (i.e. threat), the "worst-case scenario" principle has been adopted by answering the following question [15] and the answer will lead to a calculation of the impact for each process. The question is: which are the worst consequences if <your data > are disclosed to / modified by unauthorised users.

To create the basic risk matrix, in the initial setting for all m risk matrices representing (i.e. cardinality for C), n represents the cardinality of P, and o indicates the cardinality for set V= {low, medium, high}

Therefore:

$$RM_c^{n\times o} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \\ 4 & 5 & 6 \end{bmatrix}, \forall c \in C$$

$C = \{E, F, PP, C, L, PS, D\}$
And $V = \{low, medium, high\}$

Indices of the above matrix should preserve the order of set element as it is shown in both set *P* and V.
One can notice that the property holds:

$(rm)_{i,k} \leq (rm)_{j,l}$, $\forall i, j \in [1,n]$ and $\forall k, l \in [1,o]$ and $i \leq j, k \leq l$

We define a weighting vector of 7-dimentions such that each member serves as a scalar factor to be multiplied by each consequence matrix

$$W = (w_E, w_F, w_{PP}, w_{CC}, w_{\mathrm{LL}}, w_{\mathrm{PS}}, w_{\mathrm{D}}) \in \{0,1,2\}^7$$

$$RM_{weighted} = \mathrm{W} \circledcirc RM_c^{n\times o} = \{w_c . RM_c^{n\times o} : \forall c \in C \text{ and } w_c \in W\} \quad (4)$$

The above can be written as follows:

$$W \circledcirc RM_c^{n\times o} = \begin{bmatrix} 0 & 0 & 0 \\ 1w_c & 2w_c & 3w_c \\ 2w_c & 3w_c & 4w_c \\ 3w_c & 4w_c & 5w_c \\ 4w_c & 5w_c & 6w_c \end{bmatrix}$$

To adjust the matrix items, the ceiling function has been defined as:

$\lceil x \rceil : \mathbb{R} \to T$ To be $f(x) = \lceil x \rceil =$ a
If and only if $a - 1 < x <$ a and a $\in T$ such that a is an integer $\mathbb{z}$ and x is integer number, $\mathbb{R}$

$$RM_c = \{\text{ceil}(w_c \circledcirc RM_c^{n\times o}) |\ \forall c \in C \text{ and } w_c \in W\} \quad (5)$$

Again, the property should hold after adjusting the risk matrix:

$(rm)_{i,k} \leq (rm)_{j,l},\ \forall i, j \in [1,n]$ and $\forall k, l \in [1,o]$ and $i \leq j, k \leq l$

Table 5 shows the result of those multiplications in two scenarios based on impact consequences, at weight 1 and 2.

Table 5. Impact Consequences Weight

| | | **Impact Consequences Weight** | | | | | |
|---|---|---|---|---|---|---|---|
| | | When impact consequence weight = 1 | | | When impact consequence weight = 2 | | |
| | | **L** | **M** | **H** | **L** | **M** | **H** |
| **Process Value** | **0** | 0 | 0 | 0 | 0 | 0 | 0 |
| | **1** | 1 | 2 | 3 | 2 | 4 | 6 |
| | **2** | 2 | 3 | 4 | 4 | 6 | 6 |
| | **3** | 3 | 4 | 5 | 6 | 6 | 6 |
| | **4** | 4 | 5 | 6 | 6 | 6 | 6 |

Finally, Table 6 shows the simplified risk matrix.

Table 6. Simplified risk matrix

| | | **Impact Consequences Weight** | | | | | |
|---|---|---|---|---|---|---|---|
| | | When impact consequence weight = **1** | | | When impact consequence weight = **2** | | |
| | | **L** | **M** | **H** | **L** | **M** | **H** |
| **Process Value** | **0** | No Risk | No Risk | No Risk | No Risk | No Risk | No Risk |
| | **1** | Low | Low | Medium | Low | Medium | High |
| | **2** | Low | Medium | Medium | Medium | High | High |
| | **3** | Medium | Medium | High | High | High | High |
| | **4** | Medium | High | High | High | High | High |

Let assume $cs$ is a vector that represents the consequence selection of the impact of the consequence c, in which every element in *cs* is either 0, meaning no impact, or 1 means has impact, and *cs* has at most a single 1.

$cs \in \{0,1\}^{(m\times o)}$

The process risk has been assessed by calculating the maximum of vector component wise multiplication vector outcome, denoted by $\otimes$, between $RM_{adjusted}$ and $cs$ row given by process and $cs$ vector.

$$\text{Process Risk} = MAX([RM_E(Process\ value) | RM_F(Process\ value) | \cdots | RM_D(Process\ value)] \otimes cs) \quad (6)$$

Finally, the result of computation is a scalar value in $T$.

The pseudocode of mobile applications data risk assessment model is illustrated below, and can be summarised in Algorithm 1, as follows.

**Algorithm 1.** Mobile applications data risk assessment model

```
Input:  Application Rank; Process Type; Consequence selection
Output: Process Risk
1: if Process Type = "Disclosure Non-public":
2:   then Process Weight= 2 and Consequences Weight = (1, 0.5, 1, 0.5, 1, 1, 0.5)
3: else if Process Type = "Modification Non-public":
4:   then Process Weight= 2 and Consequences Weight = (1, 1, 1, 1, 1, 1, 1)
5: else if Process Type = "Modification Public":
6:   then Process Weight= 1 and Consequences Weight = (1, 0.5, 0.5,0.5,0.5, 0.5, 1)
7: else Process Risk = 0
8: end if
9: Process Value = Application Rank * Process Weight
10: New Risk Matrix [] = Ceil (Risk Matrix [] * Consequences Weight)
11: Process Risk = Max (New Risk Matrix [Process Value] * Consequence selection)
```

Table 7 provides a demonstration of the MORI risk assessment method, with different user actions within the application at all possible impact consequence weight scenarios. For further clarification, the following numbers have been calculated based on the equation 2 and 3 from the previous analysis to show the proposed risk model approach. In addition, these examples might help the user to understand the diversity level of the risk and thereby apply the appropriate level of an authentication method in a usable and a secure manner.

Table 7. Risk Assessment examples

| App | User action | Process Type | App Rank | Process Weight | Process Value | Risk |
|---|---|---|---|---|---|---|
| HSBC | Make transfer | MN | 3 | 2 | $6 \approx 4$ | 6 |
| | Read offers | DP | 3 | 0 | 0 | 0 |
| | Find HSBC branch | DP | 3 | 0 | 0 | 0 |
| | Read transactions | DN | 3 | 2 | 4 | 4 |
| | Read balances | DN | 3 | 2 | 4 | 4 |
| Weather | Forecast weather | DP | 1 | 0 | 0 | 0 |
| | Share with | MP | 1 | 1 | 1 | 1 |
| | Change setting | DN | 1 | 2 | 2 | 3 |
| Facebook | Search | DP | 3 | 0 | 0 | 0 |
| | Read news feed | DN | 3 | 2 | 4 | 4 |
| | Share | MP | 3 | 1 | 3 | 6 |
| | Read user profile | DN | 3 | 2 | 4 | 5 |
| | Post on a wall | MN | 3 | 2 | 4 | 6 |
| | Add photo/link | MN | 3 | 2 | 4 | 6 |
| BBC | Search | DP | 1 | 0 | 0 | 0 |
| | Watch BBC News | DP | 1 | 0 | 0 | 0 |
| | Share | MP | 1 | 1 | 1 | 3 |
| YouTube | Search on | DP | 2 | 0 | 0 | 0 |
| | Watch on YouTube | DP | 2 | 0 | 0 | 0 |
| | Upload | MN | 2 | 2 | 4 | 5 |
| | Add a comment | MN | 2 | 2 | 4 | 5 |
| | Search history | DN | 2 | 2 | 4 | 4 |
| | Read subscriptions | DN | 2 | 2 | 4 | 4 |
| SMS | Send a message | DN | 3 | 2 | 4 | 6 |
| | Read a message | DN | 3 | 2 | 4 | 5 |
| | Delete a message | MN | 3 | 2 | 4 | 6 |
| Calling | Make a call | DN | 3 | 2 | 4 | 6 |
| | Receive a call | DN | 3 | 2 | 4 | 4 |
| | Read a history call | DN | 3 | 2 | 4 | 4 |
| Whats App | Chat | DN | 3 | 2 | 4 | 5 |
| | Send a photo | DN | 3 | 2 | 4 | 6 |
| | Share a location | DN | 3 | 2 | 4 | 5 |
| | Share a document | DN | 3 | 2 | 4 | 5 |
| Email | Read an email | DN | 3 | 2 | 4 | 5 |
| | Send an email | DN | 3 | 2 | 4 | 6 |
| | Delete an email | MN | 3 | 2 | 4 | 6 |

## 5. Conclusion and future work

Although the majority of user actions are considered as risky processes, users of the device can perform almost all tasks at the beginning of a session, using a PIN or password, without having to periodically re-authenticate or re-validate their identity after the point-of-entry authentication. The purpose of this paper is to draw the attention of studying the risk for each process within the application. Based on our findings and result, this paper has suggested a novel risk assessment model for mobile applications data, called *MORI,* in order to determine the risk level for each process on a single application. In particular, the *MORI* model depends upon the value of user action and the worst consequences if user data are disclosed to unauthorised users or modified without permission. Finally, this model has introduced a risk matrix which might help to move the access control system from the application level to the intra- process application level, based on the risk for the user action being performed on these processes.

This risk matrix could, in the future, assist research activities to investigate the risks within the application. Future research will focus upon suggesting and applying a usable approach for accessing mobile phones by considering the risk level for each sensitive process and introducing the level of authentication beyond the PoE approach. Furthermore, the future work should focus on the usability and how the user interacts with the proposed risk matrix to ensure that it fits the best of the individual's favourite settings.

## 6. References

[1] Statista, (2016). "Forecast: smartphone users in the United Kingdom (UK) 2011-2018", available at:http://www.statista.com/statistics/270821/smartphone-user-in-the-united-kingdom-uk/[Accessed 4th September 2015]

[2] Statista, (2016b). "Worldwide mobile app revenues in 2015, 2015 and 2020 (in billion U.S. dollars)", available at: http://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/ [Accessed 21th November 2015]

[3] Rodwell, P. M., Furnell, S. & Reynolds, P.L., (2007). "A non-intrusive biometric authentication mechanism utilising physiological characteristics of human head" *Computer & Security*, vol.26, no.7, pp.468-478

[4] McAfee, (2015). Threats Predictions [online], available at:http://www.mcafee.com/es/resources/misc/infographicthreats- predictions-2015.pdf [Accessed 24 September 2015].

[5] Kurkovsky, S., & Syta, E., (2010). "Digital natives and mobile phones: A survey of practices and attitudes about privacy and security". *IEEE International Symposium on Technology and Society. IEEE, 441–449.*

[6] Aviv, A.J., Gibson, K., Mossop, E., Blaze, M. & Smith, J.M., (2010). "Smudge Attacks on Smartphone Touch Screens" *Proceeding in WOOT'10 Proceedings of the 4th USENIX conference on Offensive technologies.*

[7] Furnell, S., & Clarke, N., (2014). "Biometrics: making the mainstream." *Biometric Technology Today*, pp.5-9.

[8] Elftmann, P., (2006). "Secure Alternatives to Password-based Authentication Mechanisms, Lab. for Dependable Distributed Systems," *RWTH Aachen Univ.*

[9] Clarke, N., Karatzouni, S. and Furnell, S., (2009). "Flexible and transparent user authentication for mobile devices". *In IFIP International Information Security Conference (pp. 1-12). Springer Berlin Heidelberg.*

[10] Ledermüller, T. and Clarke, N.L., (2011), August. "Risk assessment for mobile devices". *In International Conference on Trust, Privacy and Security in Digital Business (pp. 210-221). Springer Berlin Heidelberg*.

[11] Alotaibi, S., Furnell, S. and Clarke, N., (2015). "Transparent authentication systems for mobile device security: A review". *In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 406-413). IEEE.*

[12] Davey, J., (1991). "Risk Analysis and Management. Data Protection and Confidentiality in Health Informatics", *IOS Press, pp.350-359.*

[13] Tam, K., Khan, S.J., Fattori, A. and Cavallaro, L., (2015). "CopperDroid: Automatic Reconstruction of Android Malware Behaviors", *In NDSS.*

[14] Theoharidou, M., Mylonas, A. and Gritzalis, D., (2012). "A risk assessment method for smartphones". *In Information security and privacy research (pp. 443-456). Springer Berlin Heidelberg.*

[15] Mylonas, A., Theoharidou, M., & Gritzalis, D., (2013). "Assessing privacy risks in android: A user-centric approach". *In Risk Assessment and Risk-Driven Testing (pp. 21-37). Springer International Publishing.*

[16] Alotaibi, S., Furnell S., and Clarke N., (2016). "A Novel Taxonomy for Mobile Applications Data". *In the International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol. 5, No. 3, pp115-121.*

 