Risk Assessment for Mobile Devices

Thomas Ledermüller[1,3] and Nathan L. Clarke[1,2]

[1] Centre for Security, Communications and Network Research,
University of Plymouth, Plymouth, UK
[2] School of Computer and Information Science, Edith Cowan University,
Perth, Western Australia
[3] Upper Austria University of Applied Sciences, Hagenberg, Austria
nclarke@plymouth.ac.uk

Abstract. With the market penetration of mobile phones and the trend towards the adoption of more sophisticated services, the risks posed by such devices, for the individual and the enterprise, has increased considerably. Risk assessment (RA) is an established approach with organisations for understanding and mitigating information security threats. However, it is also a time consuming process requiring an experienced analyst. Within mobile devices, the interested stakeholders range from administrators to the general public and an approach is therefore required that can establish RA in a fast, user convenient and effective manner. The proposed method utilises a number of approaches to minimise the effort required from the end-user, taking the different security requirements of various services into account and ensuring a level of flexibility that will enable all categories of user (from novice to expert) to engage with the process.

Keywords: Information security, risk assessment, mobile phone, smart phone, end-user risk assessment, computing, IT.

1 Introduction

Mobile phones (the single most popular category of mobile devices) have a market penetration of 119% in the developed world [1]. The technology has become ubiquitous with people increasingly reliant upon the services it provides. No longer is the device simply for telephony or text messaging, but rather a whole host of applications that enable the user to complete a variety of actions form banking to accessing corporate networks. This increasing range of functionality and the access to personal/corporate information they provide is becoming more and more the focus of attackers [2-3].

As such the risk posed by mobile devices has increased. Indeed, a number of surveys, such as the Computer Crime and Abuse Survey [4] indicate that 42.2% of respondents experienced laptop/mobile device theft – 6% of which reported loss of intellectual property due to the loss. Current approaches to RA tend to treat the mobile device in its entirety, without looking at the actual functions and information they store. Whilst this was appropriate when devices had little functionality, the level of sophistication of current mobile devices and services, requires a re-evaluation [5].

S. Furnell, C. Lambrinoudakis, and G. Pernul (Eds.): TrustBus 2011, LNCS 6863, pp. 210–221, 2011.

Whilst current RA methodologies could simply be extended to facilitate mobile devices, this is a rather narrow perspective to take – as only enterprise organizations will have the expertise, time and money to fund such an assessment. Mobile devices are not merely an enterprise-level technology, indeed all aspects of society use mobile devices – albeit to varying degrees. Nevertheless, an approach to RA is required that is able to access all levels of society and provide the robustness and flexibility to enable enterprise organizations to also benefit.

As no such existing methodology could be identified, the focus of this paper is to present a novel methodology that enables users with differing levels of knowledge about information security to understand and to assess the risks related to their mobile device. As well as providing a mechanism for informing users about the risks, the approach also provides detailed risk information regarding individual application and service usage. Such information could be directly used by security countermeasures to provide a more granular perspective on the problem [6]. In this manner, the device would assess the risk of access prior to deploying potentially inconvenient and intrusive security measures. For example, why enforce a 12-character password when the user simply wants to play a game on the device. Should they wish to access the users bank account, such a mechanism would be far more applicable. This paper develops the concept first proposed by [7].

The paper is begins with a review of the current RA approaches in section 2. In order to reduce the complexity of RA processes, Section 3 discusses the process of identification and categorization of applications. The risk calculation method is described in section 4 and the corresponding process is shown in the following section. Section 6 describes the developed prototype and preliminary end-user evaluation. Finally, the conclusion and future work is presented.

2 Classic Risk Assessment

RA is a well-established mechanism within information security for ensuring a commensurate level of security is provided given the risks. As such, various information security standards such as, ISO/IEC 27000 standards and the National Institute of Standards and Technologies Special Publication 800 Series were developed. Also various RA methodologies like for example OCTAVE(-S) [8], CRAMM [9], MEHARI[10] have also been designed to meet specific requirements.

All analyzed RA approaches treat mobile/smart phones as a single entity and make heavy use of workshops and interviews to identify assets, threats and vulnerabilities. The worth of an asset, the likelihood of a threat and the severity of vulnerabilities is mainly assessed through a qualitative rating scheme using different scales. As these ratings are subjective, knowledge in the area of information security and about the used assessment approach is imperative, in order to get realistic ratings. Furthermore, all methodologies are complex and time consuming. As the intended methodology shall be usable even by novice or average end-user, existing methodologies are not appropriate. The methodology must be fast in execution, options must be limited and yet comprehensive [11].

3 Categorisation

To individually risk assess mobile applications would be a time consuming and never-ending task. For example, the number of applications in Apple's App Store has increased more than fivefold within one year (207,639 – May 2010) [12]. Moreover, this fails to take into account bespoke organizational applications that might exist. Therefore, in order to support end-users, reduce the loading yet provide a meaningful assessment, the approach has proposed a categorization (which can also be referred to as assets in RA nomenclature). Based on the identified mobile phone usage trends and the market offer (Blackberry App World, Apple App Store, Android Market, Nokia Ovi Store and HTC Apps) the following asset categories have been developed:

Table 1. Asset categories

Network access - communication:	
Voice communication	Messaging
Network access - data network:	
E-mail	Web access
Personal information (online synchronized)	Bluetooth/IR
Network access - data network - applications:	
Maps & Navigation	Social networking
News & Information	E-banking
E-learning	E-health
Remote access	Ticketing/Shopping
Utilities, Personalization, Games, Entertainment	Books and libraries
Business applications (3rd party applications)	Business applications – in-house developments
Music/Audio/Video, Photography	
(Control) of device/Stored data:	
Physical device	Offline applications/Utilities
Data synchronization with PC	Documents
Multimedia data stored on device	Configurations and other
Password storage	Personal information

The determination of risk within the methodology is based upon the standard formula; risk is calculated from the multiplication of the asset value, threats and vulnerability. The worth of an asset can result from various dimensions. It can be estimated in terms of money, but also as impact in terms of CIA. Derived from previous RA methodologies, seven dimensions for the estimation of the value of an asset are defined. These asset value categories **Error! Reference source not found.**are the same, whether a mobile device is used in a private or a corporate environment; however, the terminology has been modified to ensure it is appropriate for the particular audience.

Table 2. Asset value categories

Private context	**Corporate context**
Impact of Disruption	Loss of availability
Impact on personal privacy	Breach of commercial confidentiality
Impact of data corruption	Loss of data integrity
Impact of embarrassment	Loss of reputation
Financial loss	Financial loss
Legal liability	Legal liability
Impact on personal safety	Impact on personal safety

Compared to the traditional computer environment (servers, clients, network components, etc.) little research and real world data exists concerning the likelihood of threats and the severity of vulnerabilities within a mobile context. Therefore a set of generic threats categories was developed. The proposed categorization of threats was generated based [2], [9],[13], [14]:

Table 3. Threat categories

Unauthorized information access	Denial-of-service
Unauthorised use of a service, an application	Malicious content Unauthorized collection of user data
Communications Technical failure of device	Theft/Loss/Damage by insiders/outsiders
Unsolicited information	Repudiation
Communications interception (including active and passive interception)	

The level of vulnerability is determined in terms of the thoroughness of the design process itself. To identify those, a list of questions were developed (see Annex A) based on the SANS top software errors (http://www.sans.org/top25-software-errors/) was developed. An except is illustrated in Table 4.

Table 4. Excerpt of vulnerability questions

TRUE	Are credentials transmitted via an encrypted channel?
TRUE	Is 3rd party encryption used for storage of data on the device?
FALSE	Are there any encryption algorithms used which are no longer considered as secure?
TRUE	Is there a procedure in place to ensure regular updates of the application?
FALSE	Claims the application per default access to data stored on the phone, which are not necessary (e.g. Game - access to call history)

4 Risk Calculation Scheme

Based on the developed categories, which are the input parameters for the proposed RA method, the risk calculation scheme, which consists of the following 6 steps works in the following way.

- RA_Step 1 – Evaluation of asset value categories
- RA_Step 2 – Calculation of a single asset value
- RA_Step 3 – Evaluation of threats
- RA_Step 4 – Calculation of a single threat value
- RA_Step 5 – Answer vulnerability questions.
- RA_Step 6 – Calculation of risk level

During the first step the asset value categories for an asset are evaluated in terms of potential consequences using a scale from 0 – not applicable, to 8 – critical. These values are used in the second step to calculate a single asset value. The procedure is the same for the threats in step three and four. The threat categories are evaluated (0 – not applicable to 5 – almost certain). To determine the vulnerability level the questions listed in Annex A are answered. Taking the asset value and the threat rating a temporary risk level is calculated using the matrix provided in Table 5.

Table 5. Temporary Risk Matrix

		Asset value							
		1	2	3	4	5	6	7	8
Threat level	1	1	1	2	3	4	5	6	7
	2	1	1	2	3	4	5	6	7
	3	1	2	3	4	5	6	7	8
	4	2	3	4	5	6	7	8	8
	5	2	3	4	5	6	7	8	8

The outcome can be in-, decreased or stay unaltered based on the determined vulnerability level. As little data about vulnerabilities and threats are available, the asset value has the highest impact on the resulting risk level. To show the performance an exemplary RA result is provided in Table 6, combining the output of RA-Step 2, RA-Step 4 and RA-Step5 to a single risk level per asset.

Table 6. RA-Step 6 -Risk Assessment Results

Asset category	Asset value	Threat level	Risk temp	Vulnerability level	Risk level
E-Mail (corporate)	8	4	8	2	8
E-banking	7	5	8	1	7

Table 6. (*continued*)

E-health	**8**	**4**	**8**	**2**	**8**
Remote access (corporate)	*7*	*5*	*8*	**1**	*7*
Remote access (private)	**6**	**5**	**7**	**1**	**6**
Voice communication	**6**	**3**	**6**	**1**	**5**
Stored business documents	**6**	**3**	**6**	**3**	**7**
Physical device	**6**	**2**	**5**	**0**	**5**
Personal information (online synchronized)	**4**	**3**	**4**	**2**	**4**
E-Mail (private)	**4**	**3**	**4**	**2**	**4**
Social networking	**4**	**3**	**4**	**1**	**3**
Messaging	**3**	**3**	**3**	**2**	**4**
Personal information	**4**	**2**	**3**	**2**	**3**
Web access (browser)	**2**	**4**	**3**	**3**	**4**
Stored documents	**3**	**1**	**2**	**2**	**2**
Maps & Navigation	**2**	**1**	**1**	**3**	**2**
News client	**1**	**1**	**1**	**1**	**1**
Utilities	**1**	**1**	**1**	**2**	**1**

5 Mobile Device Risk Assessment (MDRA)

The process consists of three main stages, which are shown in Fig 1. MDRA is designed to operate in the following contexts:

- Private User
- Corporate User
- Hybrid mode of private and corporate usage

It is envisaged these contexts incorporate the principal stakeholders that interact with mobile devices. This distinction is important as there may be different security requirements and threat levels in the different contexts. An example to illustrate this is that the confidentiality requirement with regard to a private e-mail account is likely to be lower than compared to a corporate e-mail account. It is also important to ensure corporate IT administrators have the ability to control the risks associated to company information and this responsibility is not left to the user.

Various stakeholders exist within this process. End-users and corporate organisations have an obvious requirement for the system. Network operators also have an important role to play. Misuse of services on mobile networks cost operators a tremendous amount of money (i.e. telephony fraud).

The first stage of the process relies upon the network operator to undertake the RA process for each category and define default risk scores. This alleviates the workload from the individual user and also provides a mechanism for informed and educated responses to be given. The default values for all asset categories are then set (O_Phase 1). Should a finer level of assessment need to be made for a particular asset (rather than asset category) this can also be established (O_Phase 2). The second stage is executed by the organization, should the device been used to access or store company information. If it is simply a personal device, this stage is not necessary. Under the C_Phases, the company has the opportunity for defining which applications it has control of and undertaking the necessary RA process. (C_Phase 1). After the company has conducted their RA they can store their RA settings.

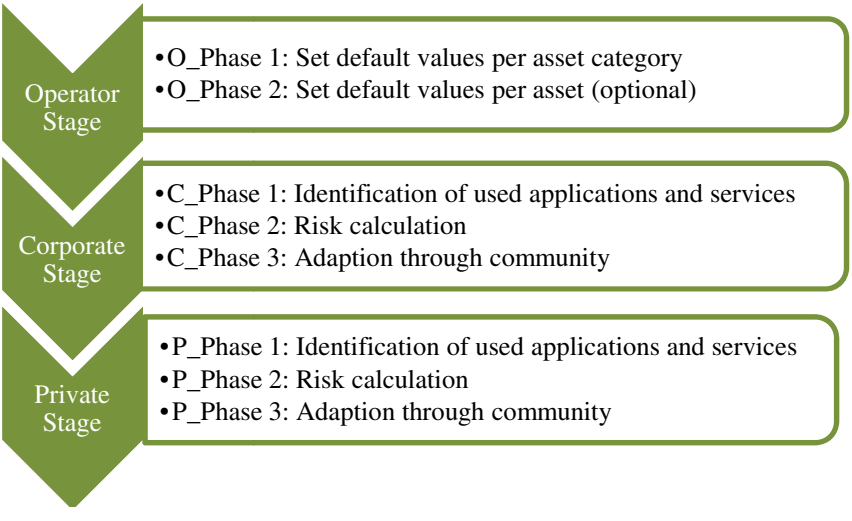

Fig. 1. Stage overview

The user of the device executes the last stage. Similar to the corporate stage, the installed applications and services are determined automatically and the risk level is calculated. In situations where the smart phone is used in a mixed (personal and corporate) context, only the applications that do not belong to the organization can be modified by the user. A private end-user starting the MDRA for the first time only has to choose his knowledge level – all other steps are automated.

P_Phase 3 is an essential phase. In order to keep the system up to date over time, the default values must be updated regularly. In order to integrate and automate the update a relative majority-voting scheme is proposed; where any alteration or modification of risk, made by a user, is transmitted to central storage by the network operator. Based on the knowledge level, chosen by the private end-user, different types of values, as shown in Table 7, can be edited. As soon as sufficient risk scores for a particular asset/application are available, the default value is replaced by the majority decision. The priority of the risk scores, assigned by the different parties involved, is shown in Table 8. It is also necessary with majority voting that a

separation between private and corporate context exists. As such data is also stored centrally, the network operator has oversight and control if necessary to mitigate against any attacks against majority-voting systems. With wide adoption, risk estimation is moved away from the default values towards a community decision system.

Table 7. Community decision - editable RA input parameters

Knowledge level	Input paramters		
	Asset value	Threat	Vulnerability
Novice user	✓	⃠	⃠
Average user	✓	✓	⃠
Security expert	✓	✓	✓

Table 8. Priority of risk scores

Priority	Private context	Corporate context
1	Settings of user	Imported corporate settings
2	Community decision (majority voting data)	
3	Settings assigned through operator – O_Phase 2	
4	Default values inherited from corresponding asset category	

6 Evaluation

In order to evaluate the performance of the proposed methodology and to gather feedback a proof of concept prototype was developed. The prototype screens, which are shown in Figure 2 and 3, are a subset that was used to conduct a preliminary physical trial with thirteen participants. The participants were grouped into “novice user” (4 participants), “average user” (5 participants) and “security expert” (4 participants). Most participants were extensive application users, (based upon their own assessment), but few of them had ever considered installing applications to improve their security level.

This first screen shows the default view. It provides a list of installed applications and the automatically calculated risk level. The applications are assorted descending based on their risk level. In order to have a look on the input parameters, which were used for the risk calculation, the user simply selects the desired applications by touching it on the screen.

On the second screen the user can chose to have a closer look at the e-banking application “Money Transfer”. On the resulting screen the values, which are assigned to the seven asset value categories, are shown in descending order. If the user wants to, this can be altered here. Furthermore, the asset value categories descriptions of threats, which may come with this application, are listed. But they cannot be changed. In order to change the threat rating, it is assumed that a certain level of information security knowledge is required. Therefore this can only be done in the advanced view.

Fig. 2. MDRA Prototype (a) Default Screen (b) Individual Application

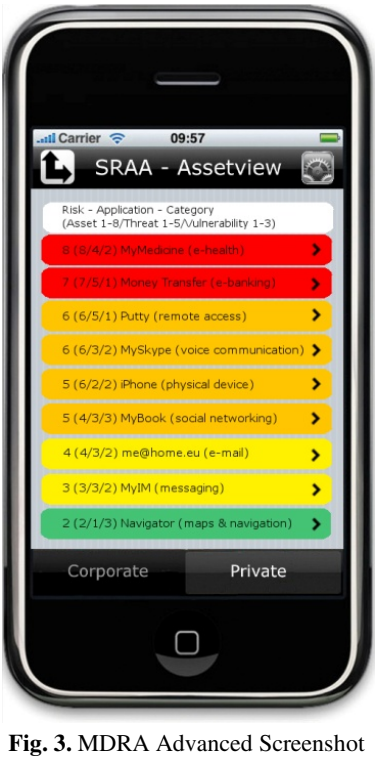

Fig. 3. MDRA Advanced Screenshot

The user can change the view to “advanced”. Compared to the base view from the first screen all input parameter values (asset value, threat and vulnerability rating) are shown on this screen. In order to change these values, the same procedure as before can be executed. Select the desired application by touching it on the screen. In contrary to the base view the user can change all values (asset value categories, threat and vulnerability rating)

After the walkthrough most participants, also the novice users, agreed that there is valuable information stored upon their mobile devices. Not all of the participants understood the way the risk was calculated the first time. The whole risk calculation process and the combination of asset, threat and vulnerability rating was especially challenging for novice users. Keeping that in mind the limitation of assessment options is an important concept. A novice user stated that too many options would prevent him from using such an application; however, the participants categorized as security experts preferred the more detailed view.

The walkthrough showed that novice users tend to use such an application in a passive way, which means they would use it as an information source without changing values. With an increasing knowledge level (average user and security experts) the participants tend to want to use such an application in an active way. This is important, as the automated update of the assigned values through adaption by the users is a vital concept of the proposed methodology.

Some participants identified that it would be a helpful feature to integrate the rating directly in the various application stores in order to have a look at the rating prior the installation of a particular application.

Providing information like security guidelines for a secure smart phone and application usage would also be appreciated. Taking this further one of the participants, who belonged to the group “security expert”, stated that it would be an interesting feature to directly provide company guidelines and policies about mobile phone usage on the smart phone. Providing information directly where it is needed is supportive with regard to secure handling and can raise the user’s awareness.

The walkthrough showed that people are interested in learning more about the risks they are facing. Half of the participants stated that they would use such a system, whereby the novice users tended to use the system in a passive way (as an information source). The average users and especially the security experts tend more towards an active usage (changing values). A further evaluation, using a larger group of participants is imperative, including a comparison between the risk estimation outcome of novice users and experts.

7 Conclusions

The main goal of this research was to develop a methodology, which enables mobile device users with differing knowledge levels to assess and understand their level of risk connected to their handset behavior. The second objective was to devise an approach that understood the risks associated with various actions and applications. Through those risk outputs, further research can be conducted on developing security countermeasures that do not simply provide a one-fits-all approach but tailors the response with the associated risk.

The largest assumption of this research is the focus upon the network operator and their need to undertaken the in the first instance RA, in order to establish the default values. Whilst there are some strong reasons for them to do so, other options do exist – security vendors themselves could be interested stakeholders that would provide the application and associated risk scores.

Future work needs to focus on the usability of such an approach and a wider comparison of novice user and security experts concerning the risk estimation with a fully operational prototype and full end-user evaluation. Whilst much discussion can be placed on the subjectivity of risk scores, MDRA provides the robustness and flexibility to suit a wide population basis in a user-friendly manner.

References

1. ITU Key Global Telecom Indicators for the World Telecommunication Service Sector, http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html
2. Dagon, D., Martin, T., Starner, T.: Mobile phones as computing devices: the viruses are coming! IEEE Pervasive Computing 3(4), 11–15 (2004)
3. Ziemann, F.: http://www.pcwelt.de/news/Trojanische-Spiele-Mobile-Malware-in-sechs-Monaten-verdoppelt-351574.html
4. Richardson, R.: CSI Computer Crime and Security Survey. Computer Security Institute (2009), http://www.gocsi.com
5. Verkasalo, H.: Analysis of Smartphone User Behavior. In: 2010 Ninth International Conference on Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR), pp. 258–263 (2010)
6. Clarke, N.L., Furnell, S.M.: Advanced User Authentication for Mobile Devices. Computers & Security 26(2), 109–119 (2007)
7. Clarke, N.L.: Advanced User Authentication for Mobile Devices. PhD Thesis. University of Plymouth, United Kingdom (2004)
8. Carnegie Mellon University, http://www.cert.org/octave/download/intro.html
9. Insight Consulting, http://dtps.unipi.gr/files/notes/2009-2010/eksamino_5/politikes_kai_diaxeirish_asfaleias/egxeiridio_cramm.pdf
10. Clusif, http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Overview.pdf
11. Clarke, N.L., Karatzouni, S., Furnell, S.M.: Towards a Flexible, Multi-Level Security Framework for Mobile Devices. In: Proceedings of The 10th Security Conference, Las Vegas (2010)
12. Statista, http://de.statista.com/statistik/daten/studie/157934/umfrage/anzahl-der-apps-im-itunes-app-store-seit-2008/
13. Microsoft, http://msdn.microsoft.com/en-us/library/ee823878%28CS.20%29.aspx
14. Fried, S.: Mobile Device Security - A Comprehensive Guide to Securing Your Information in a Moving World. Auerbach Publications, Boca Raton (2010)

Annex A

TRUE	Are credentials transmitted via an encrypted channel?
TRUE	Is there a mechanism in place, so that the user can be sure to talk with the correct server (X.509 certificates for example)?
TRUE	Are all sensitive data transmitted via an encrypted channel?
TRUE	Is 3rd party encryption used for storage of data on the device?
FALSE	Are there any encryption algorithms used which are no longer considered as secure?
FALSE	Are there any encryption keys used which key length is too short?
FALSE	Are there any hashing algorithms used which are no longer considered as secure?
FALSE	Are there any hashing algorithms used which output length is too short?
FALSE	Are there any signing algorithms used which are no longer considered as secure?
FALSE	Are there any signing keys used which key length is too short?
FALSE	Are there any user data collected (and sent to a central server), without noticing the user in advance or at all?
TRUE	Is an authentication mechanism in place, to prevent unauthorized usage?
TRUE	Is an authorization mechanism in place, to prevent unauthorized usage of particular features?
TRUE	Is a bug reporting procedure in place, enabling user to report bugs and security issues?
TRUE	Is there a procedure in place to ensure regular updates of the application?
FALSE	Claims the application per default access to data stored on the phone, which are obviously not necessary (Game - access to personal data (phone numbers, calendar, etc.))?
FALSE	Are any input data processed without prior sanitation?
TRUE	Is the Up/Download of files with dangerous type restricted?
	Are any internal software information leaked through error messages?
TRUE	Implements the application handling of unusual/error conditions?
FALSE	Are any updates installed without integrity checks?
FALSE	Are there any known vulnerabilities/exploits, which are not fixed by now?
TRUE	Are the privileges of the application set to the minimum required per default?
TRUE	Are there any indications for a secure software development process like: security requirements, internal/external review, automated code review, abuses cases, risk analysis, penetration testing?
TRUE	Does the application logging (e. g. login, security events), in order to provide data for post incident analysis?