Towards a Flexible, Multi-Level Security Framework for Mobile Devices

N.L.Clarke, S.Karatzouni and S.M.Furnell

Centre for Information Security & Network Research,
School of Computing, Communications & Electronics, University of Plymouth, Plymouth, United Kingdom

Email: nrg@plymouth.ac.uk

Abstract

The mobile device has become a ubiquitous technology that is capable of supporting an increasingly large array of services, applications and information. Given their increasing importance, it is imperative to ensure that such devices are not misused or abused. Unfortunately, a key enabling control to prevent this, user authentication, has not kept up with the advances in device technology. Although frequently reported as weak and insufficient, Personal Identification Numbers (PINs) are still the predominant form of authentication. Moreover, this form of authentication is point-of-entry only; thus failing to re-establish the authenticity of the user beyond power-on. This paper proposes the use of transparent, continuous biometric authentication of the user: providing more secure identity verification; minimising user inconvenience; and providing security throughout the period of use. It is also recognised that not all services, applications and information have the same security requirements and the paper proposes an approach for establishing what level of security to provide based upon individual services and applications. The *Personal Security Model (PSM)*, *Simple Risk Assessment Model (SRAM)* and *Organisational Risk Assessment Model (ORAM)* are three techniques for establishing the security requirements for individual services and applications based upon the responsible stakeholder (i.e. end-user or organisation) and their associated level of knowledge.

1. Introduction

The mobile networking landscape has changed significantly over the last decade, with a transition from large form factor telephony devices to small multi-purpose multimedia communications devices. The recent introduction of Third Generation (3G) technologies has provided the underlying mechanism for a wide variety of innovative data orientated services, with approximately one million users every day adopting these new features (Best, 2006).

By providing functionality that extends beyond telephony, the mobile device has evolved from being a simple telephone to become a necessity that people utilise every day, for a variety of applications. This level of functionality can be seen to be significantly expanding, with devices today having similar processing and memory capabilities to PCs of a few years ago. Indeed, their combination of portability and capability means that handsets such as smartphones and PDAs are likely to have an increasingly significant role as mobile computing and network access devices.

This transition poses serious security considerations for mobile users. With the ability to access and store a wide variety of more sensitive information, the need to ensure this information is not misused or abused is imperative. Whereas the replacement cost arising from loss or theft might previously have been the principal risk associated with mobile devices, unauthorised access to

its data could now be a far more significant problem (introducing threats ranging from personal identity theft to serious corporate loss and increasingly liability).

Given the changing nature of the mobile device and network, it is necessary to consider whether the current authentication on mobile handsets is capable of providing the level of security that is necessary to meet these requirements. Interestingly, it can be seen that although devices have undergone several generations of improvements in technology and functionality, the mechanism used for providing identity verification has not changed or even been modified. Even with increasingly large amounts of literature suggesting secret-knowledge techniques are ineffective (Lemos, 2002; Denning, 1999), the Personal Identification Number (PIN) is still the most widely used approach on mobile devices.

Looking beyond secret-knowledge, two other forms of authentication are available, namely tokens and biometrics. However, only the latter are able to realistically provide more secure mechanisms for user authentication. Tokens rarely authenticate the user, but rather authenticate the presence of the token; with the assumption being the legitimate user is in possession of the token. However, given the evolving nature of mobile devices, simply replacing one authentication mechanism with another is arguably not sufficient. Rather, only through an analysis of the requirements can an effective solution be proposed. This paper establishes the need for flexible and multi-level security for mobile devices, to meet the demands for all stakeholders (end-users, network operators, system administrators). Section 2 provides an overview of the existing security provision of mobile devices and section 3 introduces the need for multi-level and continuous identity verification. Section 4 proceeds to propose a series of mechanisms for establishing the level of security that should be attributed to different services – moving authentication away from the device and point-of-entry towards continuous verification tied to service and application usage.

2. Current security provision for Mobile Devices

As the range of data and services expands, it is increasingly desirable for users to protect their devices via appropriate authentication methods. The dominant method for achieving this on current devices is the use of 4-8 digit PINs, which can be applied to both the device and the user's Subscriber Identity Module (SIM) - a removable token containing the cryptographic keys required for network authentication.

The PIN is a secret-knowledge authentication approach, and thus relies upon some knowledge that the authorised user has. Unfortunately, such techniques have long-established drawbacks, with weaknesses often being introduced as a result of the authorised users themselves. These are most clearly documented in relation to passwords, with bad practices including the selection of weak (guessable) strings, as well as sharing details with other people, writing them down and never changing them (Lemos, 2002; Morris and Thompson, 1979). A survey assessing authentication and security practices on mobile handsets found that 34% of the 297 respondents did not use any PIN security (Clarke & Furnell, 2005). In addition, even for those respondents who did use the PIN at switch-on only, 85% would leave their handset on for more than 10 hours a day, thereby undermining any security the PIN might provide. Interestingly, however, it would appear that users do have an appreciation of security, with 85% of respondents in favour of additional security for their device. The increasing requirement for protection is further evidenced by a survey of 230 business professionals, which found that 81% considered the information on their PDA was either somewhat or extremely valuable. As a result, 70% were interested in having a security system for their PDA, with 69% willing to pay more for a PDA with security than one without (Shaw, 2004).

With the aforementioned evolution of mobile device functionality and access, the requirement for additional and/or advanced authentication mechanisms is becoming more apparent. The original specifications for security in third generation (3G) networks identified the importance of authenticating users in the more advanced environment that would be provided. Specifically, it was stated that *"It shall be possible for service providers to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorised access to 3G services by masquerade or misuse of priorities"* (3GPP, 2001). The reference to performing the authentication *during* service delivery is particularly interesting, and a potential interpretation is to use more advanced techniques that would enable periodic or continuous re-verification of the user. However, it is notable that the introduction of 3G handsets to date has not witnessed any large-scale advancement over previous authentication approaches. Having said this, a small number of operators and handset manufacturers have identified the need to provide alternative authentication mechanisms. For instance, NTT DoCoMo's F505i handset comes equipped with a built-in fingerprint sensor (NTT DoCoMo, 2004). However, although fingerprint technology increases the level of security, the technique remains point-of-entry only and intrusive from the perspective of the user.

3. An Analysis of the Security Requirements on Mobile Devices

Another observation in relation to the current point-of-entry authentication is that it tends to assume that all services, applications and information accessible on the device are of equal value, and do not require any further access control restrictions. However, it can be argued that different services and data require different security provision.
For example, the protection required by a text message is substantially different to that required by a bank account. Figure 1shows a representation of how current authentication schemes deal with security, keeping a single level of security for all services. Figure 2**Error! Reference source not found.** shows how the threat derived from each service could add another dimension to the way in which the security level is defined. Each service carries a certain risk of misuse, and this ought to be a factor in deciding the appropriate level of security.

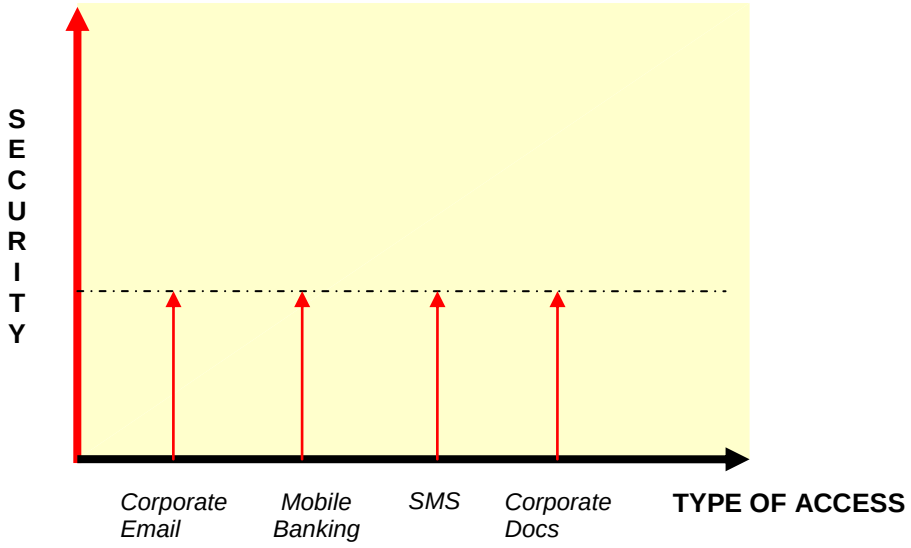


Figure 1: Current Security Assessment

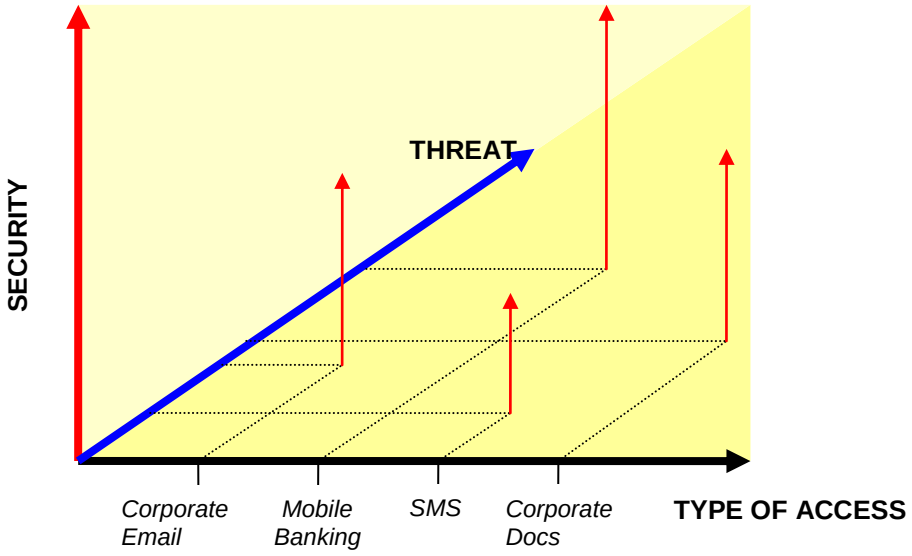
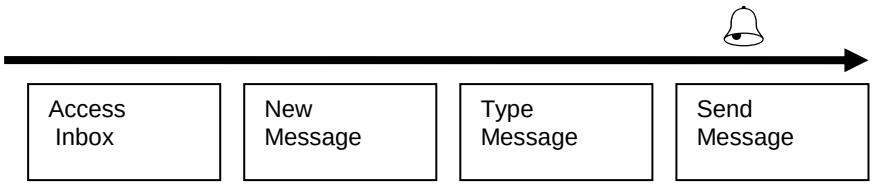


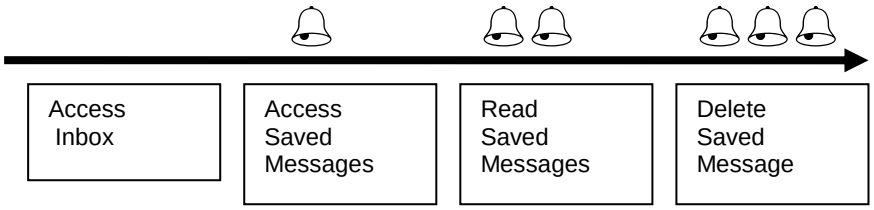
Figure 2: Proposed Security Assessment

The level of security is more appropriately assigned to each service, so that each service or function can independently require a certain level of authentication (and consequently trust in the legitimacy of the user) in order to grant access to the specific service. In this way, more critical operations can be assigned greater protection, leaving less risky operations to a lower level of trust.

It can also be argued that the level of security within a service or application is likely to change during the process, as key stages will have a greater risk associated to them than others. In order to carry out a specific task, a number of discrete steps are involved, which may not carry the same level of sensitivity (i.e. some processes are more critical, whereas others are simply operational steps that assist in the completion of the desired task). A simple example that illustrates this notion is the procedure of accessing an email inbox. The user access the inbox and at that instance there is not a real threat involved as the operation cannot lead to any misuse in its own right (see Figure 3 (a)). Even if the next step is to create a new message and start typing the content, no additional risk exists. However, the security implications actually start when the user is pressing *'Send'* as it is at this point that the adverse impacts from impostor actions would actually begin. By contrast, in Figure 3 (b), the user again accesses the inbox, but tries to access the saved messages instead. This time the requirement for greater protection occurs earlier in the process, as accessing the saved messages could affect confidentiality if an impostor reads them.



(a) Sending a Text Message



(b) Reading & Deleting Text Messages

Figure 3: Variation of the security requirements during utilisation of a service

It can be foreseen that each operation has different sensitivities and as such each step of the process changes the threat and therefore the risk level. However, within the context of this paper only the issue of *inter-process security* is addressed, establishing appropriate levels of security for each service and application rather than the device as a whole. *Intra-process security* will be addressed as part of further research.

In order to apply individual security levels to applications and services there is a need for threat assessment to classify the security risks associated with them, from both organisational and individual perspectives. From this classification, a security level could be attributed to each type of service, and subsequently to the level of trust required in the legitimacy of the user.

Within this research a number of usage scenarios were identified based upon current and potential future usage of mobile devices. These scenarios assist in the design of a threat assessment template, examining the security risk that each service encompasses and an associated severity level. A criterion used to classify the different usage scenarios is the way that each service utilises network connectivity. As such the services and functions can be split into those requiring the network, those requiring traditional cellular services, and those that operate locally on the device. This separation also assists in understanding what forms of authentication can be subsequently applied; device-centric or network centric techniques. Table 1 presents a listing of potential services and functions that can be accessed via a mobile device.

Cellular	Non-Network	Network
Voice Call	Contacts	E-mail
SMS	Calendar	Instant Messaging
MMS	Tasks	Data Synchronization
Video Call	Word Processing	Browsing Information
Voice Mail	Camera use	Downloading Web

		Content
Fax	Multimedia access	Ticketing
Push-to-Talk	Data synchronization	Location-based services (Pull)
Conferencing	Control of devices	Video-on-Demand
Value-added services	Business Applications	TV streaming
	Identification Documents	Micro-payments
		E-learning
		E-health
		Business Applications
		Information Services (Pull)
		Adult services
		Gaming
		Gambling
		Electronic Currency
		Voting

Table 1: Examples of Usage Scenarios

The classification of risk for each service and application would change to fit the requirements of each party, whether it is an organisation or an individual. However, it is important to remember that this research is looking for an approach that is usable for all stakeholders – organisations of all sizes and individuals. The complexity of the risk assessment process therefore needs to change depending upon whether it is being completed by a professional within an organisation or a normal member of the public.

4. Risk Analysis for Mobile Devices

In order to determine the level of authentication required for each service, it is appropriate to consider the implications arising from misuse. This in turn requires a means of assessing the risk in a particular context. Risk analysis techniques have been developed and widely utilised by organisations to ensure they take account of the threats and vulnerabilities against their systems. However, rather than consider the full range of risks associated with mobile assets, this paper presents a method for establishing the level of trust required in the identity of the user wishing to access the application or service. It is recognised that mobile devices are often owned by individuals and used to store business data (or vice versa). With this in mind, the required security can be defined by responsibility in one of three ways:

1. The organisation is wholly responsible for the device and all applications, services and business processes that operate on it.
2. The end-user is wholly responsible for the device and all applications and services that operate on it.
3. Both organisation and end-user take partial responsibility for particular applications, services and business processes that operate on it. No specific apportioning of responsibility is assumed.

Similarly to risk assessment, it is the responsibility of the appropriate party (or parties) to define the trust level required for each application, service or business process. What actually needs to be assessed will largely depend upon whether the device is being used for business or personal purposes. For example, it is envisaged that, for personal purposes, the user is likely to utilise the applications and services that are available and provided on the device by the network operator. The range of applications and services will largely depend upon the device, and therefore be fairly static. For business purposes, the range of applications and services operating on the device will include all of the default functionality (similarly to personal users), but also operate a wider range of third party and bespoke applications. It is therefore important to ensure an organisation has the ability to add applications and services.

The level of trust can be established in several ways. Recognising the different requirements of a personal user versus an organisation, the following alternative models are proposed:

- *Personal Security Model (PSM)* to be undertaken by a personal user.
- *Simple Risk Assessment Model (SRAM),* to be undertaken by either the personal user, the organisation, or a combination of both.
- *Organisational Risk Assessment Model (ORAM)*, to be undertaken by organisations incorporating the mobile device functionality into their current risk assessment methodology and tools.

Figure 4 illustrates the 3 models, with an increasing reliance upon formal risk assessment methodologies as one moves towards organisational use.

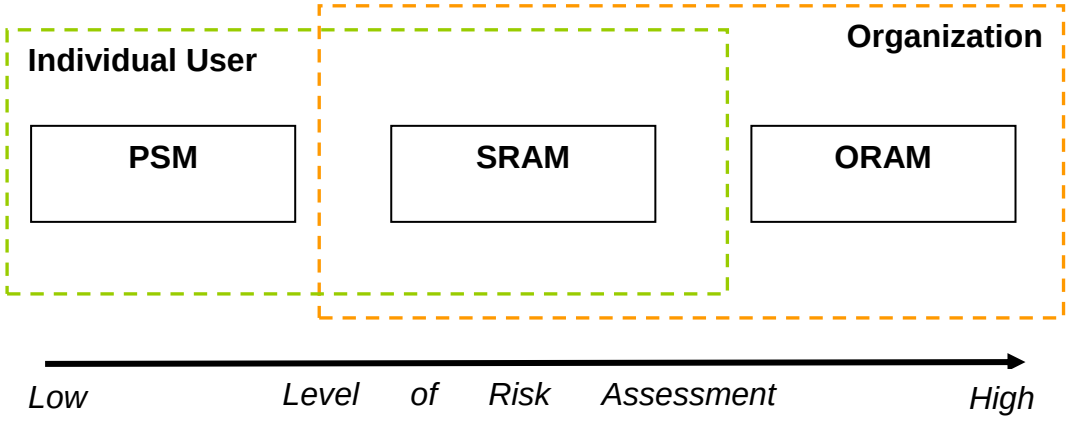


Figure 4: Risk Assessment Models

***Personal Security Model (PSM)*:** Although risk assessment methodologies are traditional tools used by businesses to identify the level of risks, such an approach is not so viable for the end-user. It would place a significant burden upon novice users, as specialist knowledge and procedures are required. The PSM approach offers a simple means of assigning risk to a service or application. Based on the knowledge and also the personal use of the device, an individual user will simply set a risk/security level to each service or application, without any further analytical view of impact. Figure 5 illustrates an example of the PSM model using a low/medium/high rating for attributing the security to each service.

	Security Level		
Service	**Low**	**Medium**	**High**
SMS	✓		
Voice Call	✓		
Video Call		✓	
Email		✓	
Electronic Currency			✓
⋮			

Figure 5: Example of PSM

The type of value that is attributed to each of the services is also left flexible, with further research required to evaluate different approaches. However, as an illustration, potential solutions could include:

- Numeric scale (e.g. 1 (low) to 10 (high))
- Likert scale (e.g. Strongly disagree – Strongly agree)
- Boolean response (e.g. Yes – No)

Recognising that many end-users may not even be willing to go this far in terms of explicitly assessing their own needs, it is also conceivable that a default profile could be established for the standard services on a device, which the user could then tune if inclined to do so (i.e. in a similar manner to aspects such as the security settings in other contexts, such as web browsers).

Simple Risk Assessment Model (SRAM): This model can operate in one of three ways depending upon where the responsibility resides for undertaking the assessment (.i.e. with the personal user, the organisation, or both).

SRAM represents a more focused risk analysis tool than the PSM, useful for more security-aware mobile device users. It follows a risk analysis process, but focuses only upon mobile devices. Personal users who feel PSM does not provide the granularity required in the process will be able to utilise this model and follow a simplified risk analysis process. Organisations not versed in risk analysis, or lacking related expertise, will also be able to follow this model. In addition, taking into account that the responsibility of the device might reside with more than one party, this model also permits the choice of which stakeholder has the responsibility of assigning risk to each service or application.

In order to determine the sensitivity levels, each service can be analysed in terms of the typical consequence that would potentially result from breaches of confidentiality, integrity and availability in each usage context. The consequences considered have been adopted from a standard risk analysis methodology, namely CRAMM (Barber and Davey,1992), and are classified as follows:

- Disruption
- Breach of personal privacy
- Embarrassment
- Financial loss
- Legal liability
- Threat to personal safety

- Breach of commercial confidentiality

Figure 6 illustrates the application of the SRAM model. As with the PSM model, the values to be attributed to the services can vary depending upon what is most appropriate to the circumstance.

Service	Commercial confidentiality	Personal privacy	Disruption	Embarrassment	Financial loss	Legal liability	Personal safety
SMS	Low	Low	Low	Low	Low	Low	Low
Voice Call	Low	Low	High	Low	Low	Low	Medium
Video Call	Low	Low	Medium	Low	Medium	Low	Low
Email	High	Medium	High	Medium	Low	Medium	Low
Business Applications	Medium	Low	High	High	Medium	High	Low
Calendar	Low	Medium	Medium	Low	Low	Low	Low
Data synchronization	High	Low	Medium	Medium	Medium	High	Low
⋮							

Figure 6: Example of SRAM

***Organisational Risk Assessment Model (ORAM)*:** Many organisations already have formal risk assessment strategies in place, with relevant expertise to conduct them. As such, this final model simply permits them to integrate mobile devices, and the applications and services accessed by them, into their existing risk analysis processes.

The three models can be used independently and assist in providing the flexibility required when dealing with differing stakeholder responsibilities. The rating of each service is completed irrespective of the risk assessment process and therefore each party can use the process that best matches their requirements and ability. As such, even in the case of both the business and the user having a responsibility for the contents of the device, each one will be able to attribute security levels to the services that refer to them.

Although the use of any of these methods introduces a degree of subjectivity into the process (particularly with larger ranges of options) this method is widely utilised and accepted in risk assessment techniques. Therefore, as long as an informed person within the organisation is undertaking the assessment, it will be as good as any other form of risk assessment. This assumption however cannot be made for the personal user, who is likely to have little (if any) experience of risk assessment. It is therefore important that we more carefully define how the end-user will assign values. In order to minimise the subjectivity of responses, it seems prudent to minimise the number of options available to the user, with more clearly defined meanings for each option. Given each personal user will experience a standard list of applications/services on

their device, this additional information regarding the impact of each choice can be built-in to the process by the network operator.

5. Conclusions and Future Work

Enhanced identity verification is imperative to protect today's ubiquitous and powerful mobile devices. Although many advances have been made in handset technology and the networks that support them, little has changed in the way we verify the user's using them. Moreover, it is no longer a matter of simply replacing one point-of-entry authentication approach with a more powerful approach. Instead, a more fundamental understanding of what we use the mobile device for is required so that effective controls can be put in place to protect the assets appropriately.

This paper has argued the need to adopt continuous, multi-level authentication of the user, tied specifically to the services and applications that are used. Possible approaches for establishing the required level of protection (considering both the services and the skills of the stakeholders) have been proposed. This work forms an integral part of on-going research into developing a non-intrusive and continuous authentication architecture for mobile devices. Future work will involve implementing the risk assessment mechanisms and developing an open-source architecture for integrating the enhanced authentication technologies.

Acknowledgement

This research was support by a two year grant from the Eduserv Foundation.

References

3GPP. (2001). "3G security; Security threats and requirements". 3GPP TS 21.133, 3rd Generation Partnership Project. http://www.3gpp.org/ftp/Specs/html-info/21133.htm.

Barber, B. and Davey, J. (1992): "The use of the CCTA risk analysis and management methodology CRAMM", Proceedings of MEDINFO92, North Holland, pp. 1589 –1593.

Best, J. (2006). "3G reaches 50 million users worldwide", http://news.cnet.co.uk/mobiles/0,39029678,49251672,00.htm

Clarke NL, Furnell SM. (2005). "Authentication of users on mobile telephones - A survey of attitudes and practices". Computers & Security, vol. 24, no. 7, pp519-527, 2005

Denning, D. (1999) : "Information Warfare and Security", Addison – Wesley, US

Lemos, R. (2002): "Passwords: The Weakest Link? Hackers can crack most in less than a minute". http://news.com.com/2009-1001-916719.html

Morris, R. and Thompson, K. (1979). "Password Security: A Case History". *Communications of the ACM*, vol. 22, no. 11, pp. 594-597.

NTT DoCoMo. (2004). “Latest Handsets – 505i Range”. http://www.nttdocomo.com/corebiz/foma/try/900i/index.html. NTT DoCoMo.

Shaw, K. 2004. “Data on PDAs mostly Unprotected”. Network World Fusion. http://www.nwfusion.com/