Balancing Security and Usability of Local Security Mechanisms for Mobile Devices

Shuzhe Yang and Gökhan Bal

Chair of Mobile Business and Multilateral Security
Goethe University Frankfurt am Main, Germany
{shuzhe.yang,goekhan.bal}@m-chair.net
http://www.m-chair.net

Abstract. The loss of control over a new-generation mobile device (e.g. loss of device or short time of inattention) can have negative impacts on the owner's privacy due to the increasing number of privacy-sensitive data stored on such devices. Current mobile platforms either lack the required protection mechanisms or the implementations lack a balance between the level of security and usability. In order to fill this gap, we propose a design for a local security mechanism for mobile devices by using an reasonable combination of existing technologies.

Keywords: Privacy, Biometrics, Usable Security, Mobile Platform Security, Trustworthy User Devices.

1 Introduction

Recent developments in the domain of mobile technology caused a significant change in the prominence of mobile devices in peoples' daily lives. Users not only trust their devices to provide them with classical communication capabilities such as phone calls or short messaging. Instead, they trust new-generation devices to store and managed a significant amount of privacy-sensitive data such as photos, location information, browser credentials, or the media library. Furthermore, one property of these platforms is their openness for third-party applications. In order to enable innovative personalized services, these applications are provided with access to those data. The success of application stores for mobile platforms substantiate the perceived usefulness of these applications by users. Thus, mobile devices have turned into personal assistants in daily life and are capable of revealing a lot about the habits and activities of their users.

The downside of this development is the increased risk for misuse. A loss of a mobile device would not only cause financial losses (e.g. through unauthorized phone calls), it could furthermore lead to a critical invasion into users' privacy since an attacker would have access to a significant amount of privacy-sensitive information. Thus, two relevant attack scenarios to protect users from are (1) the loss of the device (e.g. through theft) and (2) short period of inattention that could be exploited by an attacker. As countermeasures for these attack scenarios, device and platform manufacturers introduced a series of mechanisms such as

D. Gritzalis, S. Furnell, and M. Theoharidou (Eds.): SEC 2012, IFIP AICT 376, pp. 327–338, 2012.

PIN-protected access to the device user interface. But with the increasing functionality of mobile devices grows the complexity of their usage. This necessitates the consideration of user's capabilities to use such a device. Current mobile platforms either lack the required protection mechanisms or the implementations lack a balance between the level of security and usability. Moreover, there are still deficits in existing approaches concerning the integration of technologies to achieve a balance between usability and security. In this paper, we bridge this gap by presenting a conceptual design of a local security mechanism. As a first step, we establish a set of evaluation criteria based on the global goals of security and usability. These criteria lead to a set of design decisions that will serve as the basis for the design.

The structure of the paper is as follows. Chapter 2 will provide an overview on related work in practice and research. Chapter 3 first defines the two relevant attack scenarios in more detail and classifies them according to existing classification schemes for mobile security attacks. Furthermore, frameworks for security and usability evaluation will be established. Chapter 4 first presents the set of design decisions and then introduces our proposed design for a local security mechanism. Chapter 5 summarizes this work and concludes with limitations of this research and gives hints for potential future work directions.

2 Related Work

Research in the field of mobile security experienced a significant growth in the last years. This is due to new manifold challenges that new-generation mobile technology poses to research and development. In order to expedite advancements in this field, several efforts to substantiate this research domain have been performed. In a survey paper, Becher et al. (2011) provide a classification framework for the different aspects of mobile security vulnerabilities [16]. This framework comprises of the categories of *hardware-centric attacks*, *device-independent attacks*, *software-centric attacks*, and *user layer attacks*. One prominent attack scenario related to hardware-centric attacks they present is *Forensics Analysis*. In this attack scenario the attacker's target is to break the confidentiality of the stored data. As countermeasures the authors propose encryption of the non-volatile memory of the device and to use a secure store for secure keys (e.g. using a Trusted Platform Module (TPM)). Another taxonomy for security threats to mobile computing is presented by Friedman and Hoffman (2008) [17]. Security threats are grouped into the categories 1. Malware, 2. Phishing and Social Engineering, 3. Direct Attack by hackers, 4. Data communications interception and spoofing, 5. Loss and theft of devices, 6. malicious insider actions, and 7. user policy violations. As countermeasure, the authors propose data encryption, backup and recovery mechanisms, and device control.

Several countermeasures have been developed in research and practice to cover different aspects of mobile security and especially for the considered attack scenarios. In Nicholson et al. (2006), the authors propose a solution for the device loss scenario by introducing the concept of *Transient Authentication*. Transient

authentication lifts the burden of authentication from the user by using a wearable token that constantly attests to the user's presence [18]. When the user departs, the token and device lose contact and the device secures itself. The main drawback of this multi-factor authentication approach is the dependence on a second device. If the user loses or forgets that token, access to his data cannot be granted or can only be granted with additional efforts. Another feature that is included in some of the new-generation mobile platforms is *Remote Wipe* which allows users to delete data remotely. This solution depends on the ability to locate the device via the Global Positioning System (GPS) or the mobile cellular network. Thus, an attacker could simply disconnect positioning features. Further approaches use *implicit authentication* mechanisms to enhance the usability of security. In this approach, different behavioural patterns of humans are exploited to identify the user [20]. Other approaches use biometric data or the combination of different biometric data to authorize the user [7].

3 Requirements and Evaluation Framework

This section first describes the attack scenarios that are in focus of this research. Furthermore, it derives relevant requirements to protection mechanisms that will serve as the basis for the development of our proposed design. Based on these requirements, we set-up an evaluation framework, considering both usability and security aspects.

3.1 Attack Scenarios and Impact

The two relevant attack scenarios that we tackle are: *loss of mobile device* and *short time of inattention*. The common ground of these two attack scenarios is the mobile device owner's loss of physical control over the device. Thus, these attack scenarios can be categorized under the class of *hardware-centric attacks* according to the classification scheme of Becher et al. (2011) [16]. Regarding the taxonomy of Friedman and Hoffmann (2008), the threat category covering our attack scenarios is *loss and theft of device* [17]. The relevance of these two scenarios is strongly related to the unique property of mobility. In consequence of the small size of mobile devices, the risk of device theft or loss is high. Without proper protection mechanisms, an attacker can easily communicate in the name of the device owner or manipulate data on the mobile device. The main distinction point between the two scenarios is the available time for an attack. If the mobile device is stolen, the attacker has an unlimited amount of time to break the security mechanism. In the case of inattention, the attacker has a limited time frame to break the system. The main goal of a security system that protects the user in these two scenarios is to keep the confidentiality of the user. Thus, unauthorized access to the data and manipulation of data must be prevented. Another important protection goal is related to accountability. The attacker must not be able to transmit data or to use the communication capabilities of the device.

3.2 Evaluation Criteria

Based on our primary goal to achieve a balance between security and usability, we developed a set of evaluation criteria. This evaluation framework comprises of the two parts *security* and *usability*. Each of those parts is further divided into several aspects. This evaluation framework can be used to evaluate existing and future security mechanisms to protect against the two attack scenarios. In the following, the evaluation criteria are presented in detail. Table 1 further maps each criterion to the IT security protection goals that are affected.

Security Evaluation

- *User Interface Access Control.* A simple security mechanism that authenticates the user to unlock the user interface.
- *Access over Application Programming Interface (API).* The security mechanism must consider the possibility that an attacker can install third-party applications, which use bugs to access data stored on the mobile device.
- *Self-Security.* The security mechanism itself must be protected, which means that an unauthorized deactivation should not be possible.
- *Direct Storage Access.* This attack requires to open the mobile device. If another device mounts the storage of the mobile device, security mechanisms are not loaded. In consequence, the attacker can extract stored data (only relevant to *loss of device* scenario, because this attack requires much time).
- *Recovery.* The possibility to find the mobile device after a loss to cut the financial loss (only relevant to *loss of device* scenario).

Usability Evaluation

- *Simplicity of Setup.* If the setup is too complex or the purchase price is too high, it might deter users from using it or leads to misconfiguration.
- *Efforts for Maintenance.* The aspect *maintenance* contains for example additional infrastructure, which needs administration effort.

Table 1. Evaluation Framework for Security

Scenario	Aspects of Security Mechanism	IT Protection Goals
Loss of Mobile Device	User Interface Access Control	Confidentiality, Authenticity, Integrity
	Access over API	
	Direct Storage Access	
	Recovery	Accountability
	Self-Security	-
Inattention	User Interface Access Control	Confidentiality, Authenticity, Integrity
	Access over API	
	Self-Security	-

Table 2. Evaluation Framework for Usability

Usability		Aspects of Usability
Comfort	Simplicity of Setup	Efficiency
	Maintenance	Efficiency, Satisfaction
	Frequency & Effort of Credential Request	
	Frequency of Decision Request	
	User Comfort after an attack	Efficiency, Effectiveness
Cost	One-time costs	Efficiency
	Running costs	Efficiency, Satisfaction
	Transaction-based costs	Efficiency, Effectiveness

- *Frequency & Effort of Credential Request.* Evaluates how often the user has to enter credentials and how many resources – physical or mental load, time, monetary or material costs [2] – are required to perform this task (e.g. entering a complex but secure password vs. entering a PIN).
- *Frequency of Decision Request.* Some security applications let the user decide which data should be stored securely. This decreases the usability.
- *User comfort after an attack.* Evaluates the complexity and number of steps to activate the security mechanism after an attack.
- *One-time costs.* E.g. price for purchasing software.
- *Running costs.* E.g. monthly fee for software usage.
- *Transaction-based costs.* E.g. fees for activating the security mechanism.

According to the International Organization for Standardization (ISO) Norm 9241-11 [2] a security mechanism is usable, if it fulfils the aspects of *efficiency*, *effectiveness* and *satisfaction*. Table 2 maps each evaluation criteria to these aspects of usability.

4 Design of a Security Mechanism

This chapter presents the proposed design for a security and usability-balanced protection mechanism for mobile devices. Based on the evaluation criteria presented in Section 3 we first make a set of design decisions that will affect the shaping of our design.

4.1 Design Decisions

Design Decision 1: One level of protection for both types of privacy-sensitive data.

Two protection levels decreases the usability because either the user would have to categorize each data item or a policy-based mechanism would have to be introduced to automate the categorization of the data items on the device. A level of protection that is appropriate for direct identifiable data will also be suitable for indirect identifiable data.

Design Decision 2: Fingerprint recognition as authentication method

Due to the common limitations of mobile devices (small size, etc.), biometric authentication will provide the highest usability on mobile devices. Fingerprint, iris and face recognition are appropriate mobile authentication methods (cf. [6,7,8,9,10]). Fingerprint recognition has the best efficiency/price ratio and is therefore the best candidate for mobile devices. Token-based authentication as proposed in [8] is possible but unsuitable since the user must carry the token and that involves the risk of losing it.

Design Decision 3: Hardware-based full disk encryption

Encryption technologies are used to prevent the possibility of installing third-party applications and extracting data with *direct storage access* attacks. A solution should implement a hardware-based full disk encryption because of several reasons. A hardware-based encryption enables higher performance than software solutions, which increases the usability and user's workflow is not affect and stronger encryption algorithm can be used to enhance security.

Design Decision 4: Separate hardware storage for credentials

A separate and secure credential storage is needed because credentials stored in the local memory can be attacked by malware using bugs in the operating system or in applications. Using a hardware credential storage enhances the protection of credentials and increases the trustworthiness.

Design Decision 5: Secure boot process

Another attack possibility is compromising the Master Boot Record by installing malware [11]. Thus, the proposed design should implement countermeasures to prevent this attack.

4.2 Entities and Used Technologies

Considering the design guidelines and the design decisions presented in the previous sections, this section presents the entities of our proposed design. Furthermore, in order to support implementations, we present existing technologies and mechanisms that can be adopted to implement the respective entities.

MTM. The Mobile Trusted Module (MTM) is a aligned version of the TPM for mobile devices [19]. In our design the MTM serves as secure credential storage and is used for platform integrity verification (e.g. for a secure boot process). The MTM could also be used as encryption module, but for performance reasons we do not make use of this capability [13,14].

Encryption Module. For encryption purposes, an encryption module such as implemented in Apple's iPhone 3GS, is required [1]. Today's mobile devices' processors usually do not have encryption accelerating instruction sets. As mentioned earlier, using an MTM would not meet our performance requirements.

Fuzzy Cryptography. Fingerprint-based authentication requires the creation and storage of a fingerprint template on the device, more specifically on the MTM. We recommend to use fuzzy cryptography which introduces a biometric cryptographic system, which verifies the fingerprint with error-redundant functions and corrects potential disturbances [4]. Fuzzy cryptography makes brute-force attacks [3,4,5] and duplication of credentials difficult. Trivedi and Seshadri (2011) present a method to generate and derive the encryption key from biometric data (e.g. fingerprint) [15].

Capacitive Touch Screen and Optical Sensors for Fingerprint Recognition. Capacitive touch screens, which are mostly built in mobile devices, can be used for scanning fingerprints in combination with optical sensors [10]. It uses fourier enhancement algorithms and rank-order transformation to increase the quality of the scanned fingerprint.

RIM Certificates . As countermeasure for attacks that compromize the Master Boot Record, Dietrich and Winter (2008) present a solution that uses Reference-Integrity-Metric (RIM) certificates to measure the integrity of the boot software [12]. RIM certificates store reference integrity values of boot-relevant services in an uncompromised state (e.g. delivery state). During the boot process, software integrity is measured and compared to the RIM certificates. The boot process will be stopped, if the integrity is compromised. By using RIM certificates and integrity verification of all unencrypted components within a mobile device, the trustworthiness can be ensured.

4.3 Process Description

In this section we describe how the used technologies and entities can be combined in order to provide the user with an effective local security mechanism. Figure 1 depicts a component diagram with the used components. The essential processes are described in the following.

Setup. The setup process is depicted in Figure 2. The process begins with the user putting his finger on the touch screen for the initial fingerprint scan. Two credentials will be derived from the scanned data. First, a hash value will be created using fuzzy cryptography, second an encryption key will be generated that will be encrypted with the Storage Root Key (SRK) and stored in the key storage of the MTM. The hash value will then be stored in the Platform Configuration Register (PCR) of the MTM.

Encryption. After the hash value and encryption key have been created, the encryption process starts (Figure 3). The first step is decrypting the encryption key with SRK. After that, two encryption processes are needed. First, data that is already on the device (e.g. mobile operating system) will be encrypted in-place

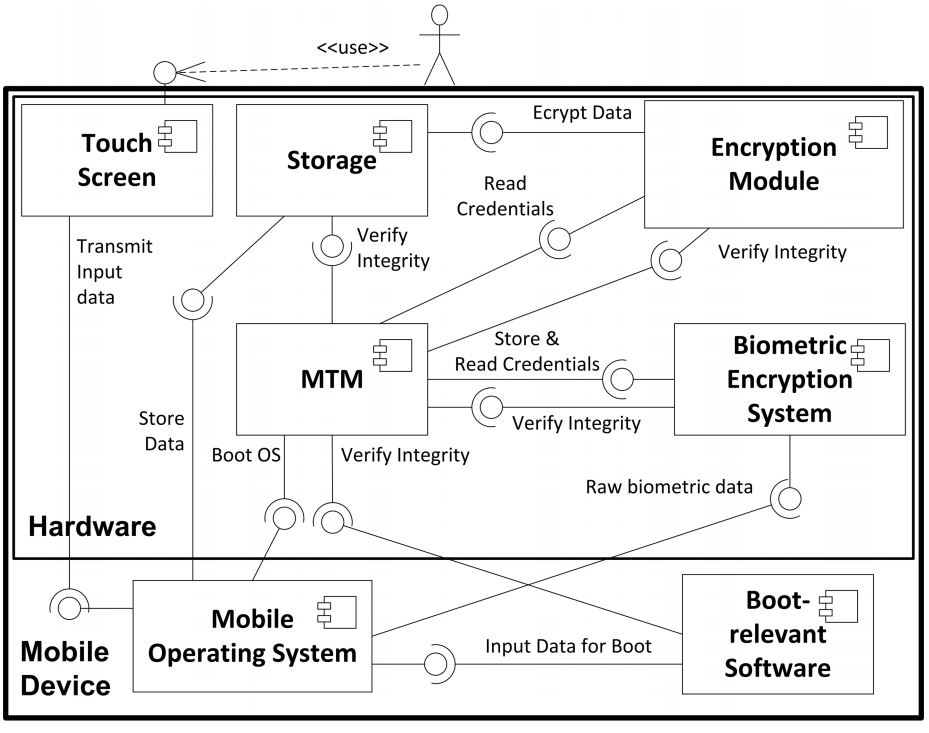

Fig. 1. Component Diagram of the Design

in the background. Second, the empty space on the storage must be encrypted in order to prepare it for future usage and to prevent unauthorized installation of third-party applications. In both processes the file system is also encrypted, which means that the encryption layer is between file system and the physical storage. In consequence, if the storage is connected to another device, the file system will not be visible to the platform.

Boot and Authentication. As stated before, the mobile device contains the required hardware hash values and RIM certificates for the secure boot process. When the user starts the mobile device, the biometric encryption system immediately verifies the integrity of the hardware and boot-relevant services with the

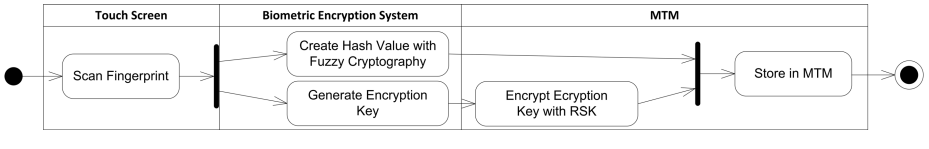

Fig. 2. Setup Process

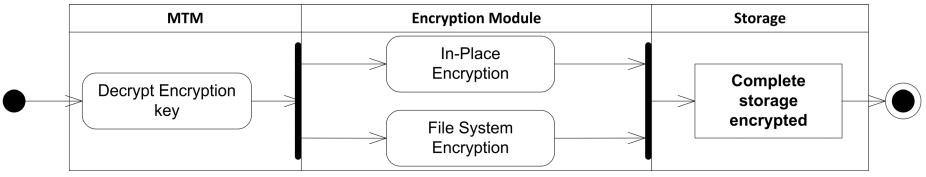

Fig. 3. Encryption Process

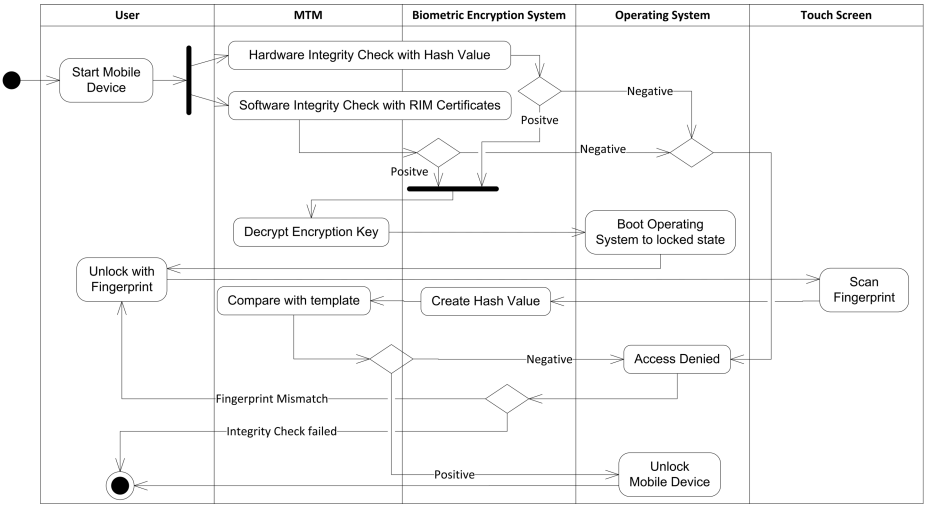

Fig. 4. Boot and Authentication Process

hash values and RIM certificates stored in MTM. Only in case of a mismatch between the measured values and the stored values, the operating system stops the boot process. Otherwise, the boot process will continue. After the boot process, the user interface to the mobile operating system is locked. To unlock the device, the user needs to put his finger on the touch screen for fingerprint-based identity verification. The touch screen scans the fingerprint and transfers the data to the biometric encryption system which then generates a hash value of the scan. In the next step, this hash value is compared with the stored hash value template in the PCR of the MTM. If the hash value does not match, the access is denied. If they match, the mobile device will be unlocked and the user has access to the interface and data. This process is depicted in Figure 4.

4.4 Evaluation

This section provides a security and usability evaluation of the proposed system based on the evaluation framework presented Chapter 3.

Security

- *User Interface Access Control.* Based on the low EER, the acceptance of an unauthorized person's fingerprint is unlikely [10]. A fake of the fingerprint is difficult because capacitive touch screens recognize the electronic charge of the finger which avoids attacks based on fingerprint imitations.
- *Access over API.* These attacks are prevented by the RIM certificate-based integrity checks. Hardware modification and/or installing malware in boot-relevant software is difficult with this system.
- *Direct Storage Access.* This class of attacks is prevented by the full disk encryption.
- *Self-Security.* A deactivation of the security mechanism is difficult due to the components being implemented as hardware.
- *Recovery.* Our proposed system does not support recovery. Thus, other solutions must be used in parallel for supporting recovery.

These evaluation results hold for the device loss scenario as well as for the inattention scenario.

Usability

- *Simplicity of Setup.* Compared to current implementations, our setup process requires a little bit more effort. But since this task has to be performed only once, it still is in an acceptable level.
- *Maintenance.* The design does not require any significant maintenance efforts after setup.
- *Freqency & Effort of Credential Request.* Compared to current unlock mechanisms based on passwords or gestures, our approach is more comfortable in daily usage. On the one hand, the user does not need to remember passwords and on the other hand today's fingerprint-based identity verification technologies are fast and reliable.
- *Frequency of Decision Request.* After setup, the user does not need to make any decisions. The services run in the background.
- *User Comfort after an Attack.* The comfort is on a high level because all data stored on the mobile device is safe and do not need the user to interfere.
- *Costs.* We propose to implement the security mechanism into the mobile operating system and the mobile device, which means it is cost neutral for the user.

5 Conclusion

The growing privacy-sensitivity of smartphones pose high requirements to protection mechanisms. To this day, several concepts and technologies have been developed to enhance users' trust into these devices. Nevertheless, they failed to provide appropriate concepts that on the one hand provides protection and on the other hand considers users' habits for using new-generation devices. In

this paper, by exploiting the capabilities of existing security technologies, we presented a new design for a holistic security mechanism to protect the user from two prominent security attacks on mobile devices: device loss and inattention. The goal was to provide a design that explicitly can be implemented with today's existing technology and to consider users' usability experiences with new-generation smartphone. The novelty lies in the combination of those technologies to a holistic design. Our design is based on a requirements analysis regarding the aspects of security and usability. We derived a set of design decisions that we considered essential to achieve the expected level of security and usability.

The main limitation of our work is that we do not provide an practical evaluation of the proposed design. An evaluation of an implementation of the system in terms of performance and usability should be the next steps to prove the effectivity of the system. Another limitation is that it partly builds on technology which is not widespread (e.g. only a little number of devices with an MTM exists). Thus, even if we build only on existing technology, due to the limited diffusion of MTMs an implementation of our system may not be possible yet. Still, the proposed solution shows the direction to which mobile security research and development should go. It is essential for mobile security technologies to keep up with the developments in the usability of new-generation smartphones. Thus, research has to figure out how to provide existing technologies to the users in a way that does not disturb the user experience.

References

1. Morrissey, S., Campbell, T.: IOS forensic analysis. Apress, Berkeley (2010)
2. ISO: ISO 9241-11:1998-03, Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability 35.180; 13.180(9241-11:1998-03). ISO, Geneva (1998)
3. Buhan, I., Kelkboom, E., Simoens, K.: A Survey of the Security and Privacy Measures for Anonymous Biometric Authentication Systems. In: International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2010), pp. 346–351. IEEE Press, New York (2010)
4. Merkle, J.: Biometrie-Daten-Schutz. Funktionsprinzip und Chancen biometrischer Kryptosysteme. In: KES 2008, vol. 6, p. 52. SecuMedia-Verlag, Ingelheim (2008)
5. Cavoukian, A., Stoianov, A.: Biometric Encryption. Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy. Discussion paper of the Office of the Information and Privacy Commissioner of Ontario (2007)
6. Park, K.R., Park, H., Kang, B.J., Lee, E.C., Jeong, D.S.: A study on iris localization and recognition on mobile phones. EURASIP Journal on Advances in Signal Processing, vol. 2008 (2008)
7. Tao, Q., Veldhuis, R.N.J.: Biometric Authentication for a Mobile Personal Device. In: Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, pp. 1–3. IEEE Press, New York (2006)
8. Furnell, S., Clarke, N., Karatzouni, S.: Beyond the PIN – Enhancing user authentication for mobile devices. In: Computer Fraud & Security 2008, vol. 8, pp. 12–17. Elsevier Science Inc., New York (2008)

9. Abileah A., Green P.: Optical sensors embedded within AMLCD panel: design and applications. In: Association for Computing Machinery (ACM) (eds.) Images and Beyond: the Future of Displays and Interaction, article no. 27. ACM, New York (2007)
10. Marcialis, G.L., Roli, F.: Fingerprint verification by fusion of optical and capacitive sensors. Pattern Recognition Letters 25(11), 1315–1322 (2004)
11. Schmidt, J.: Krypto für Jedermann. Richtig verschlüsseln mit Linux. Verschlüsselung unter Linux. In: c't - Magazin für Computertechnik, vol. 11, pp. 192–195. Heise Verlag, Hannover (2011)
12. Dietrich, K., Winter, J.: Secure Boot Revisited. In: Wang, G. (ed.) The 9th International Conference for Young Computer Scientists, pp. 2360–2365. IEEE Press, New York (2008)
13. Cesena, E., Löhr, H., Ramunno, G., Sadeghi, A., Vernizzi, D.: Anonymous Authentication with TLS and DAA. In: Acquisti, A., Smith, S.W., Sadeghi, A.-R. (eds.) TRUST 2010. LNCS, vol. 6101, pp. 47–62. Springer, Heidelberg (2010)
14. Kursawe, K., Schellekens, D., Preneel, B.: Analyzing trusted platform communication. In: ECRYPT Workshop, CRASH – Cryptographic Advances in Secure Hardware (2005)
15. Raghav Trivedi, T., Seshadri, R.: Efficient Cryptographic Key Generation using Biometrics. International Journal of Computer Technology and Applications 2(1), 183–187 (2011)
16. Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S., Wolf, C.: Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In: Proceedings of the IEEE Symposium on Security and Privacy, pp. 96–111. IEEE Press, New York (2011)
17. Friedman, J., Hoffman, D.V.: Protecting Data on Mobile Devices: A Taxonomy of security threats to mobile computing and review of applicable defences. Information Knowledge Systems Management 7(1,2), 159–180 (2008)
18. Nicholson, A.J., Corner, M.D., Noble, B.D.: Mobile Device Security Using Transient Authentication. IEEE Transactions on Mobile Computing 5(11), 1489–1502 (2006)
19. Trusted Computing Group: TCG Mobile Trusted Module Specification. Specification Version 1.0 Revision 7.02 (2010)
20. Shi, E., Niu, Y., Jakobsson, M., Chow, R.: Implicit Authentication through Learning User Behavior. In: Burmester, M., Tsudik, G., Magliveras, S., Ilić, I. (eds.) ISC 2010. LNCS, vol. 6531, pp. 99–113. Springer, Heidelberg (2011)