DuD
Datenschutz und Datensicherheit

Trusted Computing in Mobile Platforms

Players, Usage Scenarios, and Interests

Evgenia Pisko, Kai Rannenberg, Heiko Roßnagel

Trusted Computing for mobile platforms is considered important, and the approach of the TCG Mobile Phone Work Group is often seen as the most prominent one. However there are more initiatives, approaches, and players, especially in the mobile communications industry. We give an overview on the players and their interests as well as on the options trusted computing can offer and match both with each other.

Evgenia Pisko writes her Ph.D. thesis on security applications for mobile platforms at the Chair of Mobile Commerce & Multilateral Security and holds a scholarship of Deutsche Telekom Stiftung.
E-Mail: evgenia.pisko@m-lehrstuhl.de

Prof. Dr. Kai Rannenberg holds the T-Mobile Chair of Mobile Commerce & Multilateral Security at Goethe University Frankfurt (www.whatismobile.de).
E-Mail: kai.rannenberg@m-lehrstuhl.de

Heiko Roßnagel is Research Assistant at the Chair of Mobile Commerce & Multilateral Security. His research interests are in the area of security, with a focus on electronic signatures.
E-Mail: heiko.rossnagel@m-lehrstuhl.de

Introduction

Extending Trusted Computing towards mobile platforms is being discussed for quite a while. In the Trusted Computing community the approach of the TCG Mobile Phone Work Group lead by Nokia is most prominent. However, there are several other initiatives working on related topics. While this on first sight might look as the usual “War of Standardization Committees” a closer examination shows, that there are some reasons for the existence of the different groups. These reasons stem from the fact, that quite a few different players are involved when it comes to securing mobile platforms. These players have different interests and security requirements, some of them are converging and overlapping, others are diverging and in opposite to each other.

Therefore this text focuses on analysing the different players and their interests and highlights issues for further research. It begins with a section on the security of current mobile platforms; then Section 2 describes the most relevant standardization activities. Section 3 introduces the different players, whose interests are relevant for designing and marketing mobile platforms. Section 4 describes five “Usage scenarios” for trusted mobile platforms before Section 5 discusses which of these scenarios are most relevant for which players. Section 6 then gives a conclusion and an outlook.

1 Security of current Mobile Platforms

A few years ago mobile phones were closed platforms that contained only software provided by the device manufacturer. This has changed dramatically during the last couple of years. Nowadays mobile phones are used as MP3 players, digital cameras, organizers and gaming devices. In addition, users can customize their mobile device, by downloading ring tones, logos and wallpapers. Mobile devices have become open platforms that enable the users to install all kinds of software from all kinds of different sources. In order to increase the attractiveness of their platforms, Symbian and Microsoft are even offering the software development kits for their mobile phone platforms (Windows Mobile and Symbian OS) free of charge.

Another important development of the last couple of years is that almost all mobile phones now offer Personal Area Network connectivity by supporting protocols such as Bluetooth. In this new and open environment, where software for these mobile devices can easily be developed and installed, and in which these devices can easily communicate with each other, there will naturally arise some security risks, that are quite common within the current PC market. It is only a matter of time until threats like worms, viruses and Trojan Horses will emerge in a large scale on mobile devices, unless some counter measures will be applied by device manufactures or mobile operators. But as was shown in [3, 4] the security of current mobile operating systems has been neglected or sacrificed during the last couple of years. Most of the current devices are for example not even offering memory protection.

While vendors of antivirus products may welcome these developments as a basis for new business and revenue, other players within the mobile market are quite concerned. Worms that are distributed over the mobile network can cause a huge amount of traffic that has to be paid by someone. Mobile phones that refuse to work because of a security failure will not increase the users’ confidence in future products of the respective device manufacturer and don’t produce revenue for the mobile operator. Application

service providers, like for example financial institutions, are probably not looking forward to doing business with a customer using a phone compromised by a Trojan Horse.

Therefore, most market players have a vital interest in trusted computing and its promise of open and secure systems. This interest can bee seen by their active participation in standardization groups and projects regarding trusted computing.

2 Standardization Activities

Several players in the mobile market are working on mobile security enhancement techniques and standards in different associations and alliances. Some companies participate in different organizations in parallel. In this section we will present the most important work groups and projects.

Under the leadership of Nokia the **Mobile Phone Work Group** within the Trusted Computing Group (TCG) [9] comprises wireless vendors, component manufacturers and mobile service or content providers. It aims at adapting existing IT security standards, especially the TCG specifications, to mobile device platforms to achieve a trusted mobile platform and also works on a specification for application access to this platform.

The **Trusted Mobile Platform** project [11] pursued by IBM, Intel and NTT DoCoMo in 2003 and 2004 issued specifications [12, 14] defining a set of hardware and software components that can be constructed to build devices offering different levels of security. As TCG members the project participants set the TCG Trusted Platform Module as the basis for their specification. In addition, the Trusted Mobile Platform project defined a protocol that allows secure network communication with other devices. Its specification [13] offers an example ticket purchasing protocol with various enterprise and consumer scenarios.

The **Open Mobile Terminal Platform** group [8] was founded in 2004 by mobile operators mmO$_2$, NTT DoCoMo, Orange, SMART Communications, Telefónica Móviles, Telecom Italia Mobile, T-Mobile and Vodafone to define the platform requirements necessary for mobile devices to deliver openly available standardised application interfaces that will provide customers with a more consistent and improved user experience across different devices, whilst also enabling individual operators and manufacturers to customise and differentiate their offering. Currently the OMTP group is pursuing two projects on device security, one on “Application Security“ and one named “Trusted Environment”.

The goal of the project **“Application Security”** is “to provide security requirements to enable protection of the user and network from rogue applications and external attack” [7]. Mobile operators and equipment manufacturers work within this project on an Application Security Framework Specification. This work is based on the output of the project **“Mobile Application Security”** of the **GSM Association (GSMA)** [1]. The GSMA project developed the “Mobile Application Security Concept” [2] based on a terminal policy and underlying certification programme. As a part of this concept the draft of a Mobile Application Security Framework defines a mobile application domain model and corresponding device requirements. The recommended domains are shown in Fig.1. The OMTP “Application Security” project continues the work on this framework.

The project **“Trusted Environment”** aims at specifying:

- hardware requirements for security-critical functions such as SIM locking or terminal identification via IMEI (International Mobile Equipment Identity),
- hardware-based mechanisms preventing physical attacks over debug ports,
- device security enhancing facilities such as secure booting and secure flashing.

The **Open Mobile Alliance** (OMA) [5] was founded by nearly 200 mobile operators, mobile equipment manufacturers, application and content providers developing mobile service enabler specifications. Among other activities the Open Mobile Alliance specifies a digital rights management infrastructure. The specifications are continuously updated. Within the OMA the **Security Working Group** [6] specifies

- protocols for secure communication between mobile clients and servers,
- security and trust services provided by and to mobile clients and servers,
- interactions with entities, such as secure hardware tokens.

A short overview of the main standardization activities and results is presented in Table 1.

3 Mobile Market Players and their Interests

Different players in the mobile market have different interests with regard to trusted computing. The following list gives an overview on them.

Mobile equipment manufacturers

In the past the main manufacturers of mobile equipment were mobile phone manufacturers like Nokia and Motorola, who were producing both hardware and software for the devices they were marketing under their own name. Meanwhile the value chain for mobile equipment has become more complex. Parts of the hardware or even complete devices may come from manufacturers who don’t show up in the mobile phone market under their own name, such as Infineon or HTC. Parts of the software or

DOMAINS	Certification Process	Description	Access Rights (Promptings at execution)
Untrusted	None	LOW Security → High Risk ✓ Helps Developers	- No access to very sensitive functionalities - Regular user promptings for all other sensitive functional groups
Trusted	3rd party certification e.g. UTI/Java Verified	MEDIUM Security → Limited Risk through certification programmes	- Access to most sensitive functionalities - User prompting with options to switch off
Operator/ High Trust	e.g. operator managed certification programme	HIGH Security → Very low Risk through enhanced cert prog, contractual relationship with developer	- Access to all functionalities - No user promptings
Manufacturer	OEM	HIGH Security → Very low Risk through enhanced cert prog, contractual relationship with developer	- Access to all functionalities - No user promptings

Figure 1: Mobile Application Domains as proposed by the GSMA [2]

Organization/ Project	Participants	Goals	Results
Mobile Phone Work Group of the TCG	Nokia and a "large number of wireless vendors, component manufacturers and mobile service or content providers" [10]	Adaptation of TCG specifications to mobile device requirements	Not yet published
Trusted Mobile Platform project	Intel, IBM, NTT DoCoMo	Architecture definition of a trusted execution environment at different trust levels	Hardware and Software Architecture Description, Protocol Specification
GSM Association / Mobile Application Security	Mobile Operators (Vodafone, Orange, T-Mobile, France Telecom)	Definition and promotion of a Mobile Application Security Framework for open operation system platforms	Application Security Terminal Requirements based on domain model and terminal security policies, Application Certification Program
OMTP group Application Security Project Trusted Environment Project	Mobile Operators, Equipment Manufacturers, Service Providers	Recommendation for open mobile platforms establishing an open framework for mobile device manufacturers and associated software and hardware suppliers Development of the Mobile Application Security Framework Requirement definition for hardware-based security functions	Not yet published
Security Working Group of the OMA	Mobile Operators, Equipment Manufacturers, Service Providers	Specification of the operation of security mechanisms, features and services for mobile clients, servers and related entities	Specifications of Wireless Transport Layer Security, Wireless Identity Module, Wireless Public Key Infrastructure, SmartCard Web Server, and other requirements for application layer and transport layer security

Table 1: Overview of the standardization of trusted mobile platforms

even its architecture come from specific software developers or from major players such as Microsoft or Sun, who design mobile phone architectures as extensions of their PDA operating system (Pocket PC) or as a version of their runtime system (Java Virtual Machine). Marketing of mobile equipment is not only done by the "classic manufacturer brands" but also by some mobile operators.

The risks of mobile platforms described in Section 1 are affecting the equipment manufacturers the more, the more they are perceived as the providers of the respective product. A security flaw in a "Nokia" phone would be attributed to Nokia, a problem in a Pocket PC PhoneEdition device that is branded by T-Mobile (e.g. the MDA) would be attributed to Microsoft as the platform architect of the Pocket PC PhoneEdition and to T-Mobile as both names show up on the device. Only insiders would see a relation to HTC as the equipment manufacturer.

Mobile operators

In most cases mobile operators have at least four functions that relate to trusted computing in mobile devices. They operate networks, provide services, maintain direct customer relationships and provide mobile devices to customers, very often by heavily subsidizing their costs. Therefore one can see them as the most powerful players in the mobile market, and they have quite some influence on the design and the features of mobile equipment as they are in many cases the directly paying customers of the equipment manufacturers. According to their functions mobile operators have several reasons to be interested in trusted computing. First, non-functioning devices cannot be used and therefore don't generate revenue. Then compromised devices can generate an extra (maybe useless) traffic load that may heavily impact the network and reduce the service quality even to users not using a compromised device. Further on users might refuse to pay for traffic caused by compromised devices, claiming that the mobile operator should be responsible for keeping the network clean, and – if they got the mobile device through the operator – that the operator should provide devices that allow for peace of mind when using the operator's services. Also, since the mobile operator has the most prominent contact with the customer, it is very likely that the customer will seek support for compromised devices from the mobile operator such causing extra service costs that the mobile operator might not be willing to spend.

Content providers

Content providers are producing and/or distributing digital content like games, ring tones, music and other software for mobile devices. They have an interest in securing their intellectual property rights on the provided content. They are also concerned with on the one hand attracting more users to their distribution channels and on the other hand promoting facilities securing payment flow. Hence, they are interested in possibilities for Digital Rights Management that would be enabled through the use of trusted computing.

Application service providers

Application service providers are providing mobile services, such as location based services, news services, or mobile payment services. Also mobile operators can act as application service providers. Some application service providers such as financial institutions may have a high interest in ensuring that the devices their customers use

for authenticating transactions are not compromised.

Private customers

Private customers are usually not concerned about the security of their mobile devices. They rather purchase them for functionality, usability and design properties. However, once security failures have occurred, private users will perceive them as a mistake made by the manufacturer or mobile operator. Some mobile users would like to set the security levels of the devices they use in a more flexible manner.

Corporate buyers

Corporate buyers are IT managers, technical staff and system administrators concerned with providing information and communication technology for their company. They can be seen as the most security-conscious customers on the mobile market, as they are concerned about mobile devices and mobile access causing security holes in their enterprise systems, e.g. by access via mobile clients that cannot support user authentication on the same security level as other clients can. To reduce this and other risks corporate buyers often base their purchase decisions on the security of the products as they perceive it.

Corporate users

Corporate users are using mobile infrastructures predominantly for business needs. Their devices are usually not bought by themselves but rather provided by their employers. Corporate users are often not much more concerned about the security of their mobile devices than private customers, but they have to cope with the usage restrictions that their employers imposed for security purposes.

4 Usage Scenarios for Trusted Mobile Platforms

Trusted mobile platforms advance security in several aspects, but not all aspects are in the primary interest of all players, and therefore it is useful to list the several features separately.

Secure OS

Trusted mobile platforms can help to protect the operating system from manipulations. By using features such as secure booting, the integrity of the system can be observed by the user or a remote party. In addition, the operating system could accomplish a domain separation between a secure kernel or nexus, in which only trusted applications are allowed to run and an insecure application domain for all other kinds of applications. These mechanisms can help to prevent the manipulation of the system software and applications.

Digital Right Management (DRM)

Over the last years mobile phones have become multimedia devices often used to play music, mobile games etc. The implementation of a DRM infrastructure can help the respective content providers. A trusted mobile device could provide a facility that can be integrated within a DRM infrastructure, providing e.g. device authentication, cryptographic functions, and certificate management support.

Device misuse prevention

Frequently mobile devices contain private or confidential information, such as personal contacts or access credentials. Most mobile devices provide device access protection via PIN or password input. However, many mobile users don't use this functionality because it usually reduces the convenience of using the device. This can lead to information or service misuse if the unprotected device gets in the wrong hands. The mobile device could provide protection mechanisms such as strong user authorization, data access management and data encryption.

Storage of additional credentials on the mobile device

Today the SIM card is used as secure storage for mobile operator credentials. If mobile devices can offer secure storage based on trusted computing these credentials could be moved to the device. Also, trusted security features can enable mobile devices to additionally store sensitive data like passwords, authentication credentials, payment information etc. and enhance mobile devices towards personal digital wallets. To support secure storage functions a trusted platform needs to provide cryptographic functions and key management support as well as dependable user authorization and secure data access.

Secure corporate network interaction

When users retrieve data from corporate servers or synchronize their e-mails with their mobile devices, a violation of the corporation's perimeter security can occur. This type of external mobile access is normally secured by corporate access policies and corporate network security mechanisms. However, often there are no protection mechanisms for securing the internal data exchange between mobile devices and desktop computers. Usually staff members can easily copy confidential information to the mobile device and carry it out of the secured perimeter. A trusted mobile device could facilitate secure device identification in the corporate network and provide reliable mechanisms for secure data exchange. Those responsible for corporate IT systems could regain the control over the internal and external data exchange.

5 Matching Usage Scenarios and Players

Security options enabled by trusted platform features and the respective usage scenarios correspond to different interests of the different players within the mobile market. Therefore in the following this matching is being discussed.

The security of mobile platforms is valued as especially important by equipment manufacturers, mobile operators and corporate buyers, as loss of money or reputation can pose a significant problem for them. They, being the most security conscious groups, have a high interest in the security of the operating system. Corporate and private customers would welcome more reliable and trustworthy devices as well as malware protection, but they often undervalue possible security threats. A balance between usability and security restrictions has to be provided to meet the needs of both of these groups. Mobile platform security is also relevant for application providers, especially for those that offer services dealing with sensitive or monetary information.

Equipment manufacturers and content providers have the most interest in the development of a DRM infrastructure. If traffic would be increased significantly by digital content download through DRM systems, this would make a DRM system also attractive for mobile operators. Furthermore as infrastructure providers mobile operators aim at offering optimal support for their business partners, such as content and service providers. This could include support to launch a DRM infrastructure.

Loss of a mobile device, very likely containing confidential information, can be very damaging for a company. Information protection against unauthorized misuse is important to corporate buyers and users. The misuse of a stolen or lost device can

also be of concern to private customers. However, only a few of them are aware of the possible risks.

The possibility to store additional credentials on mobile devices improves the market position of equipment manufacturers. Identifying the device in the network even without a SIM and storing of payment and personal credentials on the device could extend the offerings of application providers and the options of corporate buyers. Private customers would welcome the ability to store banking credentials on the device or to have a secure PIN management application.

Secure corporate network interaction primarily affects corporate buyers and corporate users. Corporate users can feel being restricted by security limitations, but corporate buyers will feel more comfortable if access to their systems is secured. Application providers can extend their offerings to business customers relying on this feature. Also mobile operators could provide additional services to business customers and open new sources of revenue, e.g. by offering the integration of complete information system solutions.

Usage Scenarios\ Players	Equipm. manufacturers	Mobile operators	Content providers	Appl. service provid.	Private customers	Corp. buyers	Corp. users
Secure operating systems	++	++		+	+	++	+
Digital Right Management	++	+	++				
Device misuse prevention					+	++	++
Storage of additional credentials	+			+	+	+	
Secure corporate network interaction		+		+		++	+

Table 2: Players and security features they are especially interested in

6 Conclusion and Outlook

Mobile platforms have good chances to migrate into trusted platforms. To a greater or lesser extent all mobile market players are interested in device security enhancements, and the most important players are actively engaged in the standardization and development process.

Based on a trustworthy platform new mobile devices can facilitate the development of security-critical mobile commerce and mobile business application and services such as mobile payment or mobile signatures. Of course applications working with sensitive data require security functions implemented within mobile devices. To expand the market of security sensitive mobile applications the use of these functions in a trusted device should not be limited to device manufacturers or mobile operators. The possibility to share the security mechanisms and infrastructures with mobile market players such as users and application developers would enable users to make full use of the devices they acquired and paid for. It would also enable the market of mobile application services such as mobile banking to grow.

However the different players have sometimes different expectations when it comes to the security and trustworthiness of mobile devices. This can be seen not only by the different standardization consortia and their overlapping constituencies but also from the analysis of the respective interests performed in Sections 3 and 5.

What is missing at the moment is:

- An architecture combining the features the different parties are interested in;
- An entity to drive this architecture, e.g. the one consortium comprising all the players and interests.
- The availability of all standardization results for public review

One may doubt that the universal group driving the universal solution will come up. In the absence of this group one can expect developments driven by mobile operators to be more influential than others, at least as long as most mobile devices are being used for mobile communication, subsidized by mobile operators and equipped with a SIM. Developments by the TCG and its sections working on mobile devices have to cope with this perspective, at least until any other mobile application such as mobile music consumption or mobile banking gets as popular as mobile communication.

References

[1] GSM Association: Mobile Application Security Project; *www.gsmworld.com/using/secrity/mobile_application.shtml*

[2] GSM Association: Summary report of the Mobile Application Security Project *www.gsmworld.com/using/security/gsma_mas_final_summary_v1.pdf*

[3] Kingpin; Mudge (2001): *Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats.* Proceedings of the 10th USENIX Security Symposium (pp. 135-151), Washington D.C; www.usenix.org/events/sec01/full_papers/kingpin/kingpin.pdf.

[4] Murmann, T. and Rossnagel, H. (2005): How Secure Are Current Mobile Operating Systems? Pp. 47-58 in D. Chadwick and B. Preneel (Ed.): *Communications and Multimedia Security*, New York: Springer

[5] Open Mobile Alliance: Introduction. *www.openmobilealliance.org*

[6] Open Mobile Alliance, Security Working Group: Introduction; *www.openmobilealliance.org/tech/wg_committees/sec.html*

[7] Open Mobile Terminal Platform group: Current Projects; *www.omtp.org/projects.php*

[8] Open Mobile Terminal Platform group: Introduction; *www.omtp.org*

[9] Trusted Computing Group: Introduction; https://www.trustedcomputing-group.org/home

[10] Trusted Computing Group: White Paper "*Security in Mobile Phones";* https://www.trustedcomputing-group.org/downloads/whitepapers/TCG-SP-mobile-sec_final_10-14-03_V2.pdf

[11] Trusted Mobile Platform Project: Introduction; *www.trusted-mobile.org*

[12] Trusted Mobile Platform Project: Hardware Architecture Description; *www.trusted-mobile.org/TMP_HWAD_rev1_00.pdf*

[13] Trusted Mobile Platform Project: Protocol Specification; *www.trusted-mobile.org/TMP_Protocol_rev1_00.pdf*

[14] Trusted Mobile Platform Project: Software Architecture Description; *www.trusted-mobile.org/TMP_SWAD_rev1_00.pdf*