International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 19

(04/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1120-X.1139 series – Supplement on security aspects of smartphones

ITU-T X-series Recommendations – Supplement 19

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Supplement 19 to ITU-T X-series Recommendations

ITU-T X.1120-X.1139 series – Supplement on security aspects of smartphones

Summary

With the continuous development of functionalities and the expansion of applications, smartphones face many security threats. The objectives of Supplement 19 to ITU-T X.1120 series of Recommendations are to protect the personal privacy of users and to improve information security of smartphones. In order to satisfy these security objectives, this Supplement specifies a hierarchical security framework and relevant security considerations for smartphones. This Supplement identifies smartphone threats, which are categorized into vulnerabilities and attacks. With regard to the security framework, this Supplement provides necessary security solutions through system improvements and security tools.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 19	2013-04-26	17

Keywords

Attack, security, smartphone, threat, vulnerability.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Smartphones are proliferating dramatically and have become an indispensable part of daily life, to keep in touch with family members, to conduct business, and to access the Internet and to perform other activities. Different from traditional mobile phones, smartphones have increasingly powerful general purpose processors, a wide spectrum of peripheral connections, and a rich feature set and advanced operating systems with flexible application programming interfaces (APIs), all of which add to concerns about information security. Furthermore, information security concerns have been exacerbated by the availability of rich, third party applications distributed by online application repositories and side-loaded via removable media. With threats increasing in complexity and quantity, smartphones inevitably have to deal with increasing potential security risks, such as data loss, spyware attacks, virus intrusion, phishing attacks, etc. In order to protect information security of smartphones, significant research and standardization efforts have been made in recent years by a variety of different organizations around the world. These activities generally focus on specific issues, but are insufficient to mitigate security threats to smartphones. Therefore, it is important to standardize smartphone security as a whole, based on existing and potential solutions.

This Supplement can be used as a security guideline for mobile operating system providers, smartphone manufacturers, application developers, security researchers and network operators. This Supplement can also be used for smartphone users. In addition, smartphone security is a combination of solutions and standards from many organizations, such as ITU-T, ETSI, 3GPP, Global Platform, Open Mobile Terminal Platform (OMTP), the Near Field Communication (NFC) Forum and Global System for Mobile communications Association (GSMA).

Supplement 19 to ITU-T X-series Recommendations

ITU-T X.1120-X.1139 series – Supplement on security aspects of smartphones

1 Scope

This Supplement introduces a common architecture, distinct characteristics and main assets of smartphones. Moreover, this Supplement identifies smartphone threats and categorizes them into vulnerabilities and attacks. Based on the common architecture, this Supplement specifies a hierarchical security framework for smartphones, and relevant security considerations are specified. With regard to the security framework, this Supplement provides necessary security solutions, including system improvements and security tools.

This Supplement mainly focuses on smartphone security, and can be used as a security guideline for mobile operating system providers, smartphone manufacturers, application developers, security researchers and network operators.

Subject to agreed upon policies and applicable national and regional laws and regulations, the means of acquiring personally identifiable information as well as the uses made of the information are specifically out of scope of this Supplement. Neither the acquisition, nor the exchange of personally identifiable information is mandated by this Supplement. The prior explicit and informed consent of the user to acquire or exchange any personally identifiable information may be required by some specific national and regional laws, regulations and policies. Some national and regional laws, regulations and policies may further require the implementation of dedicated mechanisms to protect personally identifiable information.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.1252]: A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

3.1.2 attack [b-ITU-T H.235.0]: The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly.

3.1.3 authentication information [b-ITU-T X.800]: Information used to establish the validity of a claimed identity.

3.1.4 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.5 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.6 confidentiality [b-ITU-T X.1521]: A security principle that works to ensure that information is not disclosed to unauthorized subjects.

3.1.7 cryptography [b-ITU-T X.800]: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

3.1.8 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.9 encryption [b-ITU-T X.800]: The cryptographic transformation of data (see cryptography) to produce cipher text.

3.1.10 integrity [b-ITU-T X.1521]: A security principle that makes sure that information and systems are not modified maliciously or accidentally.

3.1.11 physical security [b-ITU-T X.800]: The measures used to provide physical protection of resources against deliberate and accidental threats.

3.1.12 privacy [b-ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.1.13 risk [b-ITU-T X.1521]: The relative impact that an exploited vulnerability would have to a user's environment.

3.1.14 threat [b-ITU-T X.1521]: The likelihood or frequency of a harmful event occurring.

3.1.15 vulnerability [b-ITU-T X.1500]: Any weakness that could be exploited to violate a system or the information it contains.

3.1.16 weakness [b-ITU-T X.1500]: A shortcoming or imperfection that, while not itself being recognized as a vulnerability, could, at some point become a vulnerability, or could contribute to the introduction of other vulnerabilities.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 mobile phone: An electronic device used for making phone calls and sending text messages across a wide geographic area through radio access to public mobile networks, while allowing the user to be mobile.

3.2.2 near field communication: A short range wireless technology that makes use of interacting electromagnetic radio fields instead of the typical direct radio transmissions, and which may be used by smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity.

3.2.3 online application repository: A digital application distribution platform available to users for downloading applications and to developers for uploading applications.

3.2.4 privileged mode: The debugging mode for professionals to modify and examine parameters of smartphones.

3.2.5 smartphone: A mobile phone with powerful computing capability, heterogeneous connectivity and advanced operating system providing a platform for third-party applications.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

API Application Programming Interface

BIOS Basic Input/Output System

CF Compact Flash

CPU	Central Processing Unit
DoS	Denial of Service
GPS	Global Positioning System
HTTPS	Hypertext Transfer Protocol over Transport Layer Security
ID	Identifier
IM	Instant Messaging
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
MMS	Multimedia Messaging Service
NFC	Near Field Communication
OS	Operating System
RAM	Random Access Memory
R-UIM	Removable User Identity Module
SIM	Subscriber Identity Module
SMS	Short Messaging Service
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UIM	User Identifier Module
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
Wi-Fi	Wireless Fidelity

5 Conventions

None.

6 General aspects

6.1 Security background

Smartphones are proliferating dramatically and have become an indispensable part of daily life in recent years. They are used for keeping in touch with family members, conducting business, accessing the Internet and performing other activities. Different from traditional mobile phones, smartphones usually have much more powerful computing capability, heterogeneous connectivity and advanced operating systems. Smartphones can also be installed with rich applications. With these rich applications and powerful functionalities, smartphones are widely used in personal and commercial areas. They enrich and facilitate users' daily lives dramatically. Smartphones are also widely used in corporations with mobile access to corporate resources, which create efficiency gains for both employees and employers. Therefore, it is inevitable for smartphones to contain much valuable personal and corporate information.

Unfortunately, smartphone security has not fulfilled expectations or kept pace with the new functionality being developed for them. Driven by economic benefits, attackers have shifted their focus from personal computers to smartphones. Due to smartphone portability and mobility, users are bound to lose or misplace their smartphones. Whenever this happens, sensitive user information stored in smartphones, such as bank account numbers and passwords, will be compromised if the data is unprotected. More seriously, many malicious codes have been developed based on flexible APIs of smartphones and most look like legitimate applications. Moreover, some legitimate applications collect user information, such as user location, without user awareness. Most applications have a security configuration setting used to control how and when user location data will be transmitted. Many users are unaware that location data is being transmitted and many are even unaware of the existence of a privacy setting used to prevent the transmission of this data. In addition, smartphones can be connected to various subjects directly, such as the Internet, personal computers and other mobile devices. This feature makes smartphones much more useful and popular, but it enables an attacker or software to invade smartphones at various levels. In reality, many users consider smartphone security to be less important than personal computer security, even though the consequences of attacks on smartphones can be more severe.

6.2 Characteristics of smartphones

A smartphone is a combination of a mobile phone and a computing platform, with plentiful connectivity and powerful computing capability. The smartphone has essential components of a computing platform, i.e., an operating system, applications and hardware. Furthermore, as a personal communication device, a smartphone also has powerful communication capabilities with other devices or networks while storing sensitive user data. The common architecture of smartphones is shown in Figure 6-1. The operating system and applications are the controllers of smartphones. The operating system is the system controller and cannot be directly accessed by users. Applications allow users to control smartphones through interaction with the operating system. Users can access user data and control communication interfaces through applications. At the same time, operating systems can directly access user data and communication interfaces.

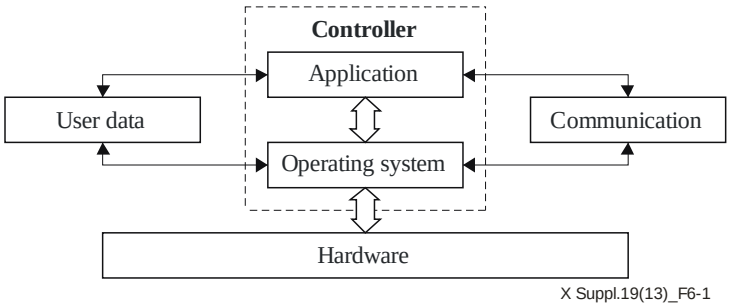

Figure 6-1 – Common architecture of smartphones

Although smartphone features are constantly changing, they have essential features that are different from other mobile devices. In addition to powerful computing capability, heterogeneous connectivity and advanced operating systems with rich APIs, smartphones have the following typical seven characteristics:

1) Overall functions of basic phones

Smartphones are predominantly mobile phones. Therefore, smartphones have at least one radio interface to access mobile networks and overall essential functions of traditional mobile phones, such as voice communications, short messaging service (SMS), etc.

2) Powerful performance

High performance is the foundation of smartphones. Specifically, the speed of built-in processors is getting much faster, while memory storage is getting larger, which allow smartphones to have powerful computing and storage capability. The computing and storage performance of smartphones has nearly kept up with personal computers.

3) Integrated transmission control protocol/internet protocol (TCP/IP) stack

Smartphones are generally integrated with the TCP/IP protocol stack. Based on the TCP/IP protocol stack, smartphones can access the Internet and install applications downloaded from the Internet. Smartphones face a variety of threats from the Internet similar to those encountered by personal computers.

4) Multiple peripheral interfaces

Smartphones usually have various peripheral interfaces, such as wireless fidelity (Wi-Fi), Bluetooth, near field communication (NFC), universal serial bus (USB), etc. These peripheral interfaces not only increase communication capabilities, but also increase security risks.

5) Global positioning capability

Most smartphones can obtain their current location based on satellite positioning, network positioning or hybrid positioning. This location data can be transferred to location-based servicers in order to receive relevant location-based services. User location data is always a primary factor in determining privacy.

6) Synchronization mechanism

Smartphones can generally synchronize local data with other devices such as laptops, personal computers, servers on the Internet and other mobile devices. This synchronization mechanism is implemented by relevant synchronization software or synchronization services.

7) Application supporting

Smartphones are designed to find, download, install and use third-party applications. Smartphone users can install applications according to their needs. Such applications can be classified into the following categories:

- Internet class – web browsing, file downloading, e-mail, etc.
- messaging class – short messaging service (SMS), multimedia messaging service (MMS), instant messaging (IM), etc.
- information class – news, global positioning system (GPS), weather forecast, stock market, etc.
- amusement class – music, movies, games, etc.
- financial class – e-payment, e-wallet, e-banking, etc.

In addition, smartphones are generally associated to online application repositories, which provide applications available for downloading. If neither sufficient security restrictions are placed on smartphone platforms, nor other security limitations are implemented on relevant online application repositories, smartphones will be at risks of compromise.

6.3 Smartphone assets

Smartphones consist of hardware and software, and store a significant amount of user data. All smartphone assets listed in Table 6-1 are attack targets.

Table 6-1 – Smartphone assets

Assets	Description	Importance
user data	Address book, call history, SMS/MMS, e-mail, pictures, audio, banking information, location information, notebook, agenda, etc.	Very important
software	Pre-installed applications, user-installed applications, operating system, etc.	Important
hardware	Central processing unit (CPU), random access memory (RAM), flash, battery, etc.	Important

User data is the most valuable asset of smartphones. As communication devices with multiple connection capabilities, smartphones inevitably connect to other personal computers, laptops, mobile phones, electronic devices and servers on the Internet. Due to these connections, user data stored in smartphones face many threats, such as data interception, identification theft, and location information collection, etc. Any deceit or data accessing without user awareness can be catastrophic. With the boom of mobile e-commerce applications, many attackers are seeking ways to obtain user banking information, such as bank accounts and passwords. User data is accessed and managed by smartphone applications, making them essential entities for data protection.

Smartphone software is the second most important asset of smartphones. Attackers usually retrieve user data through applications infected by malicious code, or some malware with backdoor access. Smartphone applications are responsible for most cases of user data loss. In addition, applications can control smartphone hardware that interacts with the operating system, which means that attackers could also use malicious code to attack smartphone hardware. Furthermore, some pre-installed and user-installed applications can access the Internet, send SMS/MMS or initiate data connections automatically without user awareness, which can cause unpredictable economic loss for smartphone users.

The smartphone hardware itself can also be considered an asset. Smartphones are typically used in a variety of locations. Their mobile nature makes them much more likely to be lost than other fixed devices. Consequently, any physical loss of a device such as misplacement or decommissioning may lead to data leakage and identification theft.

6.4 Security considerations

Increasing functionality, with the exception of security functionality, has serious inverse effects on smartphone security. With increasing functionality, smartphones will inevitably face growing serious security threats. As a rule, smartphones with simple functionality will be more secure than those with advanced functionality. The relationship between functionality and security is monotonically decreasing, which is shown as the solid line in Figure 6-2.

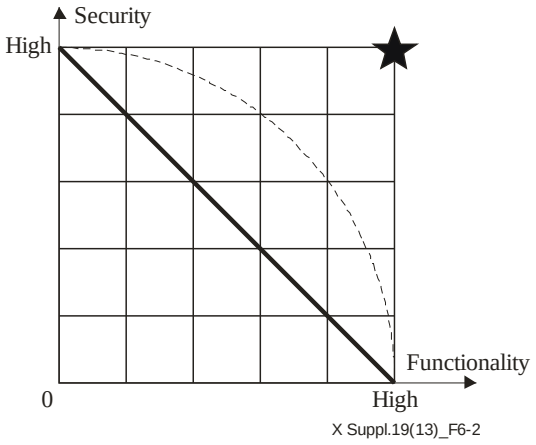

Figure 6-2 – Relationship between functionality and security

The security objective of smartphones is to enhance security while simultaneously increasing the functionality of smartphones. See the dashed curve in Figure 6-2. The ultimate goal is shown as the solid star in Figure 6-2.

In order to enhance smartphone security, security objectives, threats, considerations and solutions should be carefully considered. The relationship among these factors is described in Figure 6-3. To find appropriate security solutions, security threats should be identified as a first step. Once these security threats have been identified, security considerations should be specified in order to reach certain security objectives. Lastly, the security solutions can be obtained. This roadmap is adopted by this Supplement.

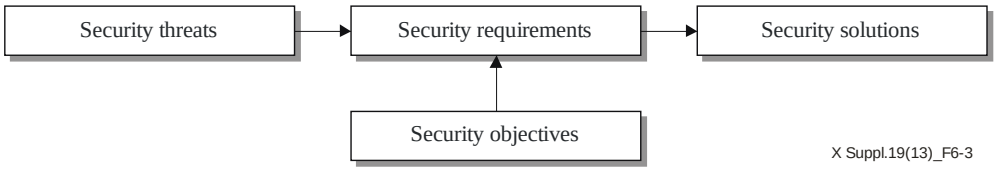

Figure 6-3 – Roadmap of smartphone security

7 Threats to smartphones

7.1 Overview of threats

Distinctive features enrich the applications of smartphones, but also increase the risks to smartphones. Valuable smartphone assets have become the target of attackers. Specifically, advanced operating systems with flexible APIs not only improve the capability and functionality of smartphones, but also increase the security threats (e.g., viruses) to smartphones. Other smartphone features also widen the scope of threats to smartphones: broad bandwidth not only accelerates Internet access, but also speeds up the spread of viruses; multiple peripheral interfaces increase connectivity of smartphones to networks or other devices, but also provide significant avenues for virus injection. Furthermore, in contrast to personal computers, smartphones have always-on and always-connected mobility while storing a wide range of personal information. It is very hard to reinstall the operating system on smartphones; therefore, whenever security is compromised on smartphones, the loss and degree of destruction will be more serious than to personal computers.

Threats, representing potential violations of smartphone security, are grouped into two categories according to their causes: 1) vulnerabilities, and 2) attacks. See Figure 7-1. Vulnerabilities are weakness of smartphones and their inability to withstand the effects of hostile environments. Attacks are attempts to cause intentional damage, perform unauthorized access or malicious modifications of smartphone assets. In other words, vulnerabilities are the internal attributes of smartphones, while attacks are the external offensive activities to smartphones. Most attempts to exploit smartphone vulnerabilities aim to initiate attacks. For example, resident malware can delete important files stored in a smartphone without the awareness of the smartphone user. In this example, malware is the attack and the absence of user awareness is the vulnerability. If the smartphone user was aware of the existence of such an operation, he or she could adopt appropriate ways to prevent the important files from being deleted.

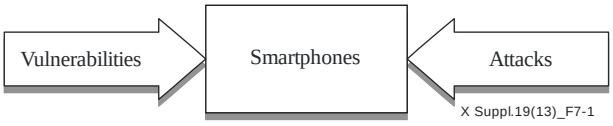

Figure 7-1 – Vulnerabilities and attacks

7.2 Vulnerabilities of smartphones

7.2.1 Classification of vulnerabilities

As comparatively complicated devices, smartphones inevitably have numerous vulnerabilities, and these security threats can be utilized to initiate attacks. These smartphone vulnerabilities can be clustered into 4 classes, as shown in Figure 7-2.

Figure 7-2 – Vulnerabilities of smartphones

7.2.2 System defects

It is impossible for a smartphone to avoid all hardware and software defects. Some non-conformity defects can be observed early on, but many defects remain hidden or latent until triggered by a corner use case. Even when some defects are detected, especially hardware defects, they are difficult to repair. As a result, system defects can cause non-intentional device behaviours. Furthermore, advantage may be taken of a system defect to initiate attacks and compromise smartphone systems.

7.2.3 Insufficient API management

The most distinctive feature of smartphones is its flexible APIs, which are mainly used for application development. However, insufficient API management is responsible for most malicious code infection. API management refers to the process of developing, publishing and managing APIs. Generally, smartphone APIs are classified into open APIs for third-party application development and controlled APIs for remote maintenance. Controlled APIs generally have superuser or particular privileges, which can be used for remote system update, file erasure and information retrieval. If controlled APIs are obtained, negative activities such as backdoor attacks may be initiated. On the other hand, some open APIs have inappropriate privileges that can be utilized to acquire certain privileges to initiate attacks.

7.2.4 Lack of user awareness

Some applications can be installed on smartphones without user confirmation or with limited information. Under these conditions, attackers can spread applications infected by malicious codes with deceptive information. After installation of these applications without accurate or sufficient information, smartphones will be infected by malicious codes. In addition, some sensitive operations, such as sending and receiving messages, deleting important files, activating wireless interfaces, can also be executed secretly. Therefore, smartphone users may become aware of the occurrence of these sensitive operations only after the occurrence of these serious incidents.

7.2.5 Insecure wireless channels

In wireless environments including cellular networks, user data and control signals transmitted between smartphones and network devices can be captured as they are radiated over the air. If these communication channels are left unprotected or unencrypted, the information will be exposed. In reality, most wireless channels do not have sufficient security protections due to the following reasons:

- insufficient security protection of protocol stacks
- cost considerations due to the high costs of security solutions
- government policies that prevent the implementation of security mechanisms.

Even when security mechanisms, such as authentication, encryption, access control, etc., have been implemented, smartphones are vulnerable to some enhanced attacks due to the limited security intensity of the existing security mechanisms.

7.3 Attacks to smartphones

7.3.1 Classification of attacks

As mentioned in clause 6.3, smartphones have valuable assets including software, hardware and user data – especially financial-related information. Driven by economic benefits, many hackers have shifted their focus to smartphones and initiated multifarious attacks, as shown in Figure 7-3.

Figure 7-3 – Attacks to smartphones

7.3.2 Physical control attacks

Due to portability and mobility, smartphones are more likely to be lost than other devices. In this case, sensitive user data stored in smartphones, including address data, bank account information, account passwords, communication records, etc., is always at increased risk of compromise. Without proper protection measures, such information can be accessed and read directly. In addition, the incorrect disposal of old or damaged devices can increase the risk of device compromise. When old or damaged devices are thrown away after a simple disposal, some recycling software can be used to recover erased data from these decommissioned smartphones.

7.3.3 Malware

Malware is an increasing threat to smartphones. Flexible APIs not only enrich application development, but also facilitate development of malicious codes. Heterogeneous connectivity also increases the channels for the spread of malware. Smartphones can be infected by malicious codes during synchronization with personal computers, or during file transmission between virus-infected storage media and the device. Malware can also be spread in a variety of other ways. Users are not always aware of a downloaded application functions. Even if applications have acquired explicit user consent, users may not be aware that an application is behaving maliciously. Malicious code can be spread as follows:

- Internet downloads – A user may download an infected file via an Internet connection. The file could be disguised as a game, security patch, utility, or other useful application posted somewhere as a free or shareware downloadable file. Legitimate applications too, may pose problems if they contain vulnerabilities that can be exploited by malware. Malware is often hidden within pirated legitimate applications that are bundled into packages for free download and are distributed over peer-to-peer services. To install these applications, users would have to defeat side-loading security mechanisms designed to prevent the installation of applications from unknown sources. Social engineering techniques are another way in which users can be duped into changing security settings such that they allow the installation of malware.
- Online application repositories – Online application repositories are digital application distribution platforms for both smartphone users and application developers. Smartphone users can browse and download applications from these platforms. Online application stores can be (and have been) sources for malicious code spreading, which result from both security threats to smartphones and the administration deficiency of some online application repositories.
- Messaging services – Malware attachments can be appended to electronic mail and MMS messages delivered to smartphones. IM services supported on many smartphones are another means of malware delivery. Users have to open an attachment in many cases. In this situation, the smartphones can be infected by malicious codes, especially if the user is socially engineered into changing security settings that allow the installation of such an application.
- Bluetooth communications – Bluetooth is a convenient way to exchange messages or move files between smartphones that are connected with each other using this communication medium. Bluetooth communications can be placed in different modes: discoverable, which allows the smartphone to be seen by other Bluetooth-enabled smartphones; and connectable, which allows the smartphone to respond to messages from connected smartphones. Malware could potentially be delivered by engaging the available connectivity services supported by a smartphone left in discoverable mode where the message sent to the device is convincing enough for a user to be tricked into installing the malware.
- NFC connections – NFC is mainly used in contactless payment systems, such as mobile payment environments. Although the communication range of NFC is limited to a few centimetres, NFC alone does not ensure secure communications. NFC offers no protection against eavesdropping and can be vulnerable to data modifications. Therefore, NFC is also a potential path for malware spreading without sufficient protections. Users could accidentally receive a malicious NFC message by brushing against a well-placed NFC tag.

The range of malware behaviours and subsequent consequences is broad. Malware can be used to eavesdrop on user input, steal sensitive information, destroy stored information or disable a device. Malware can also accumulate wireless communication fees for a subscriber, for example, by sending SMS messages or initiating calls to chargeable toll numbers. Propagation onto other handheld devices or even personal computers can also be attempted by malware to broaden its effect or to perturb the entire communications network. The following distinct high-level categories of malware attacks have been identified:

- Spoofing – Provides the user with falsified (spoofed) information to trigger a decision or action that impacts the security of the smartphone.
- Data interception – Intercept mobile communications or data stored in smartphones.
- Data theft – Collect and send data stored in smartphones.
- Service abuse – Perform actions that cause higher service costs than expected ones for the user, or spread unwanted SMS, MMS, etc.

- Availability – Impacts to availability or integrity of either the smartphone itself, or the data stored in it.
- Network access – Use the smartphone for one or more unauthorized network activities, including port scanning or using the smartphone as a proxy for network communications.

While the range of misbehaviour that malware can exhibit is extensive, outbreaks experienced to data on mobile handheld devices have been mild compared with those encountered by networked desktops and personal computers. However, incidents have been increasing steadily and are expected to grow.

7.3.4 Backdoor attacks

Backdoor attacks mainly result from system bugs and disclosure of controlled APIs. Some smartphone operating systems have security defects such as insufficient authentications and incorrect authorizations. Based on these vulnerabilities, attackers can bypass security policies to access smartphones and initiate attacks. In addition, if attackers have mastered the functioning of controlled APIs, they can also access smartphones and act like legitimate entities.

7.3.5 Wireless attack

A smartphone has at least one wireless network interface for Internet access. This interface can use Wi-Fi, cellular networking, or other wireless communication technologies. Due to the openness of wireless communications, the smartphone is susceptible to eavesdropping. Attacks may also be performed to intercept and modify these wireless communications. According to status influence on wireless communications, attacks can be grouped into two categories: passive attacks (e.g., sniffing, eavesdropping) and active attacks (e.g., spoofing, corruption, blocking or modifying information). Generally, passive attacks are used for active attacks to acquire necessary information of attack targets such as the addresses and vulnerabilities of targets.

7.3.6 Cloning

Authenticating a smartphone to the mobile network securely is a vital function performed via the authentication information residing in the smartphone. This information can also be saved in the removable user identity module (R-UIM), such as the subscriber identity module (SIM), the user identity module (UIM), and the universal subscriber identity module (USIM), etc. Normally, cryptographic key information and algorithms within the smartphone or the R-UIM provide the means for the smartphone to participate in a challenge-response dialogue correctly, without exposing any key materials or other information that could be used to clone the authentication information and gain access to a subscriber's services. Cryptographic key information also supports stream cipher encryption to protect against eavesdropping on the air interface. If somebody obtains the information by cloning R-UIM or by another method, he or she can utilize it to access any services just as a legitimate subscriber would.

7.3.7 Peripheral interface attacks

Smartphones usually have many peripheral interfaces, such as Wi-Fi, Bluetooth, universal serial bus (USB), etc. These peripheral interfaces increase smartphone communication capabilities, but at the same time, they become a popular step-stone for outside attacks. Some smartphones can be infected by malicious codes during synchronization through peripheral interfaces. Some user data is disclosed from smartphones through peripheral interfaces. For example, without user confirmation, Bluetooth may be activated and used to transfer sensitive data without user awareness. In addition, when Bluetooth is activated automatically, it may attract additional viruses. Furthermore, Wi-Fi interfaces of smartphones always face a variety of attacks.

7.3.8 Unauthorized access

Even if security measures are implemented, smartphones and their contents can be accessed through forging or guessing authentication credentials or bypassing the authentication mechanism entirely. Authentication weaknesses are also major avenues that can be exploited. Some security measures are not strong enough against dictionary attacks; others have built-in backdoors for manufacturers that can be used to bypass all or part of the security mechanism. If the security mechanisms are not effective, materials can be accessed without proper authorization. User location is another important component of user data. While cellular carriers have the ability to track smartphone locations with varying degrees of accuracy for internal use, other companies now offer location tracking services for registered smartphones to allow the whereabouts of the user to be known by friends and family. If user location is disclosed, user privacy will be compromised.

7.3.9 Spam

Unwanted SMS, MMS and e-mail from advertisers have begun to appear on smartphones. Other than the inconvenience of having to delete them, charges may apply for inbound activity, such as a per-message charge on each SMS message received or charges for those messages above the monthly limit of a subscriber's service plan. Data download can also result in extra charges – with each image attachment further escalating these charges. Using social engineering techniques, mobile spam is used to persuade users to call or send text messages to chargeable service numbers. Spam is also used for phishing attempts that entice users into revealing passwords, financial details, or other private data via web pages, e-mail or text messages, or downloading malware attached to a message. Instant messaging and multimedia messages are other possible means for malware delivered through spam. Denial-of-service (DoS) is also a possibility using spam techniques.

8 Security framework of smartphones

8.1 Security objectives

To guarantee information security and user privacy, smartphones should typically satisfy multiple essential security objectives as follows:

- Confidentiality – The state where information is not made available or disclosed to unauthorized individuals, entities, or processes. Transmitted and stored data cannot be disclosed to, or read by unauthorized parties.
- Integrity – Transmitted and stored data cannot be altered or destroyed in an unauthorized manner. Smartphones should be able to detect any intentional or unintentional changes to data and resources.
- Availability – Resources can only be accessed and used by legitimate smartphone users. Meanwhile, smartphones should be protected against unauthorized access.

The security objectives of smartphones focus on sensitive transmitted and stored data, rather than on the smartphones themselves. These objectives are accomplished through a combination of security features built into smartphones and security controls applied to smartphones.

8.2 Security framework

To achieve the security objectives described above, smartphones should be secured against a variety of threats caused from any aspect of smartphones. A hierarchical security framework, as shown in Figure 8-1 is specified, which is based on the common architecture of smartphones.

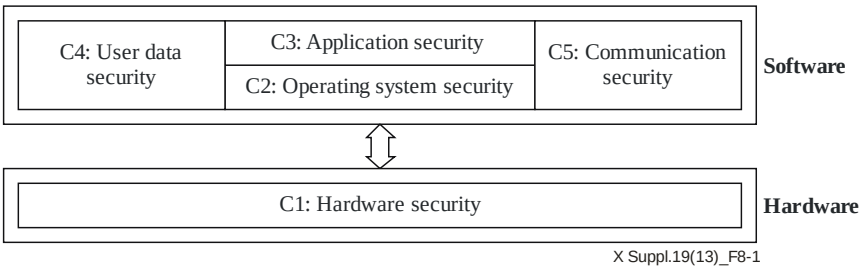

Figure 8-1 – Security framework of smartphones

In this framework, security considerations are grouped into five parts: hardware security (C1), operating system security (C2), application security (C3), user data security (C4) and communication security (C5). Each part has its own specific security considerations. Some smartphones have middleware between the operating system and applications, which provide services to applications beyond those available from the operating system. Regarding security considerations, the middleware does not go beyond applications and operating systems. Therefore, middleware security has not been separated as an independent part.

C1: hardware security

Hardware security is the fundamental base for all upper layer securities. Without the support of secure and reliable hardware, any upper layer security will always suffer from attacks from the lower level hardware. Hardware security should at least support integrity and confidentiality of storage chipsets, non-substitutability of key chipsets, and uniqueness of identification chipsets. In addition, hardware should support necessary security mechanisms for upper layers.

C2: operating system security

The operating system is the heart of the smartphone and acts as the core controller of all other parts. The goal of operating system security is to provide a secure and reliable software environment, including maintaining integrity of system codes, monitoring of data traffics, security services for applications, separation of secure domains and necessary authentication mechanisms. In addition, operating systems should have sufficient security mechanisms for APIs, especially open APIs for third-party developers.

C3: application security

Application security has two parts: inherent security of applications, and security tools. Inherent security of applications includes integrity of application codes, isolation from malicious codes, etc. Security tools are applications used to prevent smartphones from falling victim to security threats such as spamming, virus infections, etc.

C4: user data security

User data is the most important asset of smartphones. The objectives of user data security include confidentiality, integrity and availability of user data stored in smartphones. The user data cannot be accessed without appropriate authentication and authorization. In addition, erased user data cannot be recovered by unauthorized entities, no matter what measures they adopt.

C5: communication security

Communication security is the security mechanism of communication systems, which comprise voice communication, data communication and peripheral interface. The communication security objectives are twofold: confidentiality, integrity and availability of user data transferred between communication systems; and communication interface activation controlled by users.

8.3 Security considerations

8.3.1 Hardware security considerations

- Prevent sensitive IDs from rewriting – Some IDs (i.e., IMEI) are used to identify smartphone user, smartphone device and key chipsets. If these IDs are modified, usage mischarge, function failure, identity theft and other problems may happen. Therefore, smartphones should have a security mechanism to prevent such sensitive IDs from rewriting.
- Support the integrity verification of key chipsets – Any unintended replacement of key chipsets may bring negative influence on smartphones. Therefore, the capability to execute integrity verification at the booting stage should be provided. Integrity verification may also be initiated manually by the user. If the integrity verification is failed, some tools should be provided for further examination.
- Prevent security-related information from modification – If a smartphone has a particular secure storage area for sensitive security-related information, a protection mechanism should be available for the stored information to be accessed. For example, some security keys which are only used for data authentication and data encryption should not be accessed by users directly.

8.3.2 Communication security considerations

- Ensure that smartphones cannot initiate DoS attacks to mobile networks – DoS attacks are serious threats to network resources, which can consume communication bandwidth dramatically and cause serious communication congestion. Smartphones should have a mechanism to detect and stop DoS attacks caused by malicious codes.
- Provide a firewall to filter unwanted access from the Internet – If smartphones are assigned globally routable IP addresses, there will be many accesses to smartphones from the Internet. These accesses include probing and attacking activities to the smartphone. Hence, smartphones should have a mechanism to control accesses from the network.
- Provide a device authentication mechanism – In some situations, only specific smartphones may access particular network services. An additional layer of authentication should be supported that permits only a specific pre-authorized device operated by specific pre-authorized user to access the network. This ensures that, even in the event that a password or token has been compromised, the network is still protected as long as the authorized machine is not used.
- Support user identity confidentiality – The permanent identity of a user to whom a service is delivered cannot be intercepted on a wireless connection.

8.3.3 Operating system security considerations

- Provide a secure and reliable environment – To avoid malicious code and corrupted image files, the operating system should have a mechanism to verify the validity and integrity of OS images and applications. This security mechanism includes integrity verification of system code, monitoring of data traffic and service security of applications.
- Prevent unauthorized OS images and applications installation and update – Smartphones should not allow the installation of unauthorized OS images and applications without the explicit endorsement of the user. Smartphones should check the validity and integrity of OS images and applications before installing or updating.
- Provide integrity check for applications – To avoid malicious codes and corrupted files, the operating system should have a mechanism to verify application integrity by using an attached digital signature.

- Provide integrity check for system-related data – Many rootkit software and malware try to conceal their activities by manipulating log files and other system parameters. Therefore, the operating system should have a mechanism to detect and prevent modification, deletion, creation and replication of various kinds of system-related data including log files.
- Provide secure communication mechanisms between different applications – To prevent data theft in communication systems and man-in-the-middle attacks, the operating systems should provide secure communication mechanisms between different applications.
- Prevent privileged mode for common applications – The privileged mode has high privileges to control OS and applications. Therefore, the privileged mode cannot be accessed by common applications in user-mode.

8.3.4 Application security considerations

- Prevent unknown applications from being installed – Malicious codes are mainly spread through unknown application installations. Therefore, it is very important to enable smartphones to prevent unknown applications from being installed without the explicit endorsement of the user.
- Identify and prevent malicious codes – Smartphones should be able to identify malicious codes by themselves or antivirus software installed on them. Once smartphones identify malicious codes, they should be able to prevent applications with malicious codes from being executed.
- Separate running programs – Smartphones should provide each application with independent space and computing resources. One application should not influence the running of other applications. One such example is the use of virtual machines and sandbox technologies to separate running programs.
- Provide a verification mechanism of installed applications – Because distributed applications can be infected with malicious codes, such as spyware, Trojan horse, etc., the OS should have a security mechanism to verify the application owner and consistency with the original distribution.
- Have the capability to filter spam – Spam messages from SMS and e-mail are unwelcome and cause many problems. The smartphone should have the capability to filter spam messages from mobile networks and the Internet with the explicit endorsement of the user.

8.3.5 User data security considerations

- Support necessary warning mechanism when smartphones are lost – To avoid the unwanted use of smartphones by other persons, the smartphone should have functions that can be controlled remotely by authorized persons. By using this function, when a user loses a smartphone, the user can find the smartphone's location, delete the important data on the smartphone, stop other necessary functions, etc.
- Ensure the integrity and confidentiality of user data – It is possible that malicious codes rewrite or modify important data. Therefore, smartphones should have capability to check the integrity and confidentiality of all types of data stored in the smartphone.
- Provide an access control mechanism for user data – Smartphones store a great deal of information, including much that is related to privacy. Therefore, smartphones should have strict access policies that restrict user data from being accessed.

9 Security solutions for smartphones

9.1 Overall aspects

To solve the threats detailed in clause 7, many security solutions have already been produced. In accordance with the classification of threats, security solutions can be grouped into two classes in terms of realization approaches: system improvements, and security tools, as shown in Table 9-1.

Table 9-1 – Classification of solutions

Objectives	Description
System improvements	Eliminate weaknesses of operating systems and pre-installed applications through system modification, always involving the OS kernel. Enlarge smartphone security abilities through the use of secure hardware, adoption of security mechanisms, addition of user confirmation, etc.
Security tools	Prevent outside attacks through add-on applications such as antivirus software, firewalls, intrusion detection systems, etc.

Security tools, including antivirus software and intrusion detection systems, can prevent external attacks such as malware, but they cannot prevent internal smartphone attacks caused by misuse or user unawareness. Therefore, it is very important to adopt security mechanisms for smartphones, such as user awareness, defect elimination, and so on. These security mechanisms are called security improvements. Both the security improvements and security tools have advantages and disadvantages:

- Security tools – are easier to use but also run risks, such as system incompatibility, internal malicious code, etc. In addition, security tools do not ensure a security improvement.
- System improvements – they ensure security enforcement, but this can be rather expensive due to kernel configuration or adoption of new hardware.

Security mechanisms are the fundament security bases for smartphones and no one absolute secure smartphone exists. System improvements always take a long time; therefore, the combination of system improvements and security tools is the practical security solution for smartphones. The relationship between security solutions and security framework is shown in Table 9-2.

Table 9-2 – Relationship between security solutions and security considerations

Solutions	Considerations
Secure boot	C1, C2
User confirmation	C1, C2, C3, C4, C5
Secure APIs	C3
Isolation of applications	C3
Unrecoverable data erasure	C4
Firewall	C2, C3, C5
Automatic locking	C2
Encryption for sensitive user data	C4
Digital signatures	C3
Access control	C2, C3, C4, C5
Authentication	C2, C3, C4, C5
Remote data protection	C4

Table 9-2 – Relationship between security solutions and security considerations

Solutions	Considerations
Network access security	C5
Anti-spam software	C3
Anti-virus software	C1, C2, C3, C4, C5
Intrusion detection system	C1, C2, C3, C4, C5
Backup software	C4

9.2 System improvements

9.2.1 Secure boot

To avoid the unintended replacement of key chipsets, the corruption of the operating system and the unintended modification of system files, integrity verification should be executed at the booting stage. This is done by comparing the calculated hash values of system modules in smartphones with the authentic ones. If the hash values are completely the same, the key chipsets, the operating system and the system files are proved secure without any changes. Otherwise, users should be cautious and use security tools to find potential security problems. Secure boot can also be initiated manually.

9.2.2 User confirmation

To avoid the infection of malicious codes and disclosure of sensitive information, user confirmation should be put into effect before the installation and execution of applications. There are some steps that need to be followed before the installation and operation of user confirmation. Therefore, a balance between usability with a simple operation and security of user confirmation should be considered.

All installations should have user confirmation while only sensitive operations need user confirmation. The sensitive operations include, but are not limited to:

- making phone calls
- sending SMSs/MMSs
- sending e-mails
- opening/closing cellular data connections
- opening/closing WiFi connections
- opening/closing Bluetooth connections
- opening/closing NFC connections
- connecting USB
- inserting a memory such as a compact flash (CF)
- initiating a positioning function
- recording a local voice or online voice
- initiating a camera
- reading/writing/modifying/deleting sensitive personal data, such as address books, communication records, SMSs, MMSs, e-mails, pictures, videos, etc.

In addition, some status information should be shown on smartphone screens, including cellular data connection, Wi-Fi connection, Bluetooth connection, NFC connection, USB connection, location positioning, voice recording, video recording, etc. All of the above considerations can only

be met at the operating system level, especially system APIs. Meanwhile, all the information provided by the operating system should be sufficient and reliable.

9.2.3 Secure APIs

Smartphones should provide customized built-in authentication and encryption mechanisms, which can be customized secure schemes, and also open source schemes such as secure socket layer/transport layer security (SSL/TLS). Secure APIs should be provided for the application developer to implement secure functionality. For instance, hypertext transfer protocol over transport layer security (HTTPS) can be used in application functions to access the network.

9.2.4 Isolation of applications

Smartphones should endow each application independent space and computing resources. An application cannot access other running applications except when the application explicitly requests permission to use certain features such as user location. One such example is the use of virtual machine and sandbox technologies to separate running programs.

9.2.5 Non-recoverable data erasure

To avoid the recycling of data of decommissioned smartphones, an application or a function should be provided to overwrite all electronic data, residing on the hard disk drive or other digital media, with random meaningless data. Unrecoverable data erasure goes beyond basic file deletion commands, which only remove direct pointers to data disk sectors and make data recovery possible with common software tools.

9.2.6 Firewall

The operating system should support firewall functions. Firewalls can audit and block unauthorized connections from/to smartphones based on blacklists or other features, thus preventing security threats from untrusted sources.

9.2.7 Automatic locking

Automatic locking protection should be adopted by smartphones. If the idle time between operations exceeds the predefined time threshold, automatic locking should be executed. In addition, users can enable the locking mechanism manually.

9.2.8 Encryption for sensitive personal data

Encryption software or encryption mechanisms provided by operating systems is recommended. Sensitive personal data such as bank account numbers, credit card numbers, account passwords, user-defined data, etc., should be encrypted.

9.2.9 Digital signatures to trusted applications

An authentication system should be established to deliver digital signatures to trusted applications while users can select software with valid digital signature for their smartphones. Based on such a mechanism, users can install and use trusted applications with valid digital signatures.

9.2.10 Access control

Access control limits the access of processes and users to resources and/or services. Access control can limit the risk of malicious/exploited applications.

9.2.11 Authentication

Users should be authenticated in order to access smartphone resources or use smartphones, thus preventing the unauthorized use of the device and unauthorized access to smartphone resources.

9.2.12 Remote data protection

To avoid security threats from smartphone loss or disposal, smartphones should be able to recognize and execute remote commands for erasure, locking, etc. In order to realize these functions, daemon processes need to be running in smartphones, which can monitor commands in real-time. When remote commands contained in SMS/MMS are received, the content in the smartphone will be erased or the smartphone will be locked.

9.2.13 Network access security

To avoid electronic eavesdropping and resist other threats, smartphones should support complete security-related protocols in the terminal side, including entity authentication, confidentiality, data integrity and mobile equipment identification. However, these security features also need the support of the network devices.

9.3 Security tools

9.3.1 Anti-spam software

Anti-spam software is needed for countering SMS/MMS/e-mail spam. With increased use of computing and storage capacity, anti-spam software is provided and enables full management of filtering rules and filtering of SMS/MMS/e-mail.

The management of filtering rules includes:

- loading/unloading pre-defined filtering rules
- adding/deleting/querying blacklist items and whitelist items
- maintaining keyword-based or time-based filtering rules.

The management of filtering SMS/MMS/e-mail includes:

- summarizing/viewing/querying/restoring/deleting filtered SMS/MMS/e-mail.

9.3.2 Anti-virus software

Anti-virus software should be used to detect, prevent and remove malware, including but not limited to viruses, worms, Trojan horses, spyware and adware. In addition, a variety of strategies especially for smartphones are typically employed. Signature-based detection involves searching for known patterns of data within executable code. However, it is possible for smartphones to be infected with new malware for which no signature is known.

9.3.3 Backup software

Desktop software should be provided to backup sensitive personal data including address book information, communication records, SMSs, MMSs, e-mails, pictures, videos and system configurations, etc.

9.4 Integration of security solutions

There are no distinct boundaries between system improvements and security tools. Most security solutions cannot be implemented as security improvements, but only implemented as security tools. However, different solutions will have different effects and performance. For example, it is better to implement a firewall as a security improvement because the TCP/IP stack is a part of the operating system and the firewall always works on the TCP/IP layers. Therefore, security solutions should be considered on the basis of the real environment.

In addition, smartphone security is a trade-off between security, functionality and performance. Rich functionality not only decreases performance, but also increases security risks. Therefore, smartphone functionality should be minimized according to user requirements. In addition, security solutions should keep up with smartphone functionality. As part of the operating system, system improvements should be implemented all the time. Particularly, based on secure boot, a trust chain including key chipsets, the operating system and applications can be established. In addition, security tools are always flexible, but should support digital signatures, also which can be implemented as system improvements.

Bibliography

[b-ITU-T H.235.0] Recommendation ITU-T H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014