

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

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/>.

© ITU 2014

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Supplement	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	General aspects	3
	6.1 Security background.....	3
	6.2 Characteristics of smartphones.....	4
	6.3 Smartphone assets	5
	6.4 Security considerations.....	6
7	Threats to smartphones	7
	7.1 Overview of threats	7
	7.2 Vulnerabilities of smartphones.....	8
	7.3 Attacks to smartphones.....	9
8	Security framework of smartphones.....	12
	8.1 Security objectives.....	12
	8.2 Security framework	12
	8.3 Security considerations.....	14
9	Security solutions for smartphones.....	16
	9.1 Overall aspects.....	16
	9.2 System improvements	17
	9.3 Security tools	19
	9.4 Integration of security solutions	19
	Bibliography.....	21

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.