International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 24

(09/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1120-X.1139 series – Supplement on a secure application distribution framework for communication devices

ITU-T X-series Recommendations – Supplement 24

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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Supplement 24 to ITU-T X-series Recommendations

ITU-T X.1120-X.1139 series – Supplement on a secure application distribution framework for communication devices

Summary

Supplement 24 to ITU-T X.1120-X.1139 series provides a secure application distribution framework for communication devices and security requirements for application distribution sites to enhance the safety of the communication environment for users.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 24	2014-09-26	17	11.1002/1000/12333

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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

Supplement 24 to ITU-T X-series Recommendations

ITU-T X.1120-X.1139 series – Supplement on a secure application distribution framework for communication devices

1 Scope

Supplement 24 to ITU-T X.1120-X.1139 series provides a secure application distribution framework for communication devices. The communication devices include smartphones, tablet personal computers (PCs), set-top boxes (STBs), and similar devices that have the capability to download applications from managed application distribution sites and execute the downloaded applications. This Supplement also includes security requirements for application distribution sites.

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.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

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

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

3.1.4 data origin authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.5 digital signature [b-ITU-T X.800]: Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g., by the recipient.

3.1.6 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.

NOTE – Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

3.1.7 smartphone [b-ITU-T X-Sup.19]: A mobile phone with powerful computing capability, heterogeneous connectivity and advanced operating system providing a platform for third-party applications.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 application distribution site: An application distribution platform on which users can buy and sell applications online. It is also referred to as an application market. Such sites are usually operated by the owners of operating systems, the manufacturers of communication devices, and telecommunication service providers.

3.2.2 communication device: A computing device that has the capability to download applications from managed application distribution sites and execute the downloaded applications. They include smartphones, tablet personal computers (PCs) and set-top boxes (STBs). A communication device can be distinguished from a feature phone that cannot download and use the applications that users prefer.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

API Application Programming Interface

CVE Common Vulnerabilities and Exposures

OS Operating System

PC Personal Computer

STB Set-Top Box

TTP Trusted Third Party

URL Uniform Resource Locator

5 Conventions

In this Supplement:

The phrase "**is required to**" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Supplement is to be claimed.

The phrase "**is recommended**" indicates a feature or action that is preferred, but which is not absolutely required. Thus, this preference need not be present to claim conformance.

The phrase "**is prohibited from**" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Supplement is to be claimed.

The phrase "**can optionally**" indicates a feature or action on which choice is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator or service provider. Rather, it means the vendor may optionally not provide the feature and still claim conformance with this Supplement.

6 Introduction

Many communication devices, such as smartphones, personal computers (PCs), set-top boxes (STBs), have capabilities to execute applications. Users can install their favourite applications on their own devices, which add new functions to those devices. However, there are problematic applications that steal personal information or execute malicious activities. Because most applications are installed from application distribution sites, secure distribution of applications from such sites is one of the most important elements to manage. This Supplement presents the phases of application deployment and the framework for secure application distribution. In addition, security requirements of the application distribution sites are provided to secure the use of communication devices.

7 Application deployment

7.1 Life cycle of application deployment

Figure 1 shows the life cycle of application deployment. This consists of five phases: design/development, evaluation, deployment, and update or removal.

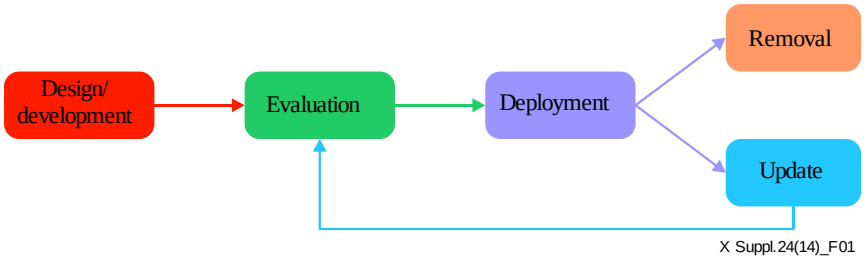

Figure 1 – Life cycle of application deployment

7.2 General security considerations

This clause specifies security considerations for each phase in the life cycle of the application.

7.2.1 Design/development

This phase is where developers design and develop their applications. In this phase, developers need to design applications taking into consideration the security aspects, and in particular secure coding. To achieve this, application distribution sites need to ask developers to think about security and to develop secure applications.

7.2.2 Evaluation

Evaluation is the phase where applications are examined by reviewers at distribution sites. The submitted applications are evaluated to determine whether they are secure before being posted on distribution sites. In this process, application distribution sites need to verify the developer's identity and review the submitted application from a security perspective. After the evaluation, if the application reviewer judges that the application is secure, it is posted on the distribution site. If the application is judged not to be secure, the application distribution site needs to give feedback to the developer. The operators of distribution sites need to have testing and evaluation capabilities to perform security checks of applications. In some cases, the operators can entrust a third-party testing institution to perform security checks of applications.

7.2.3 Deployment

Deployment is the phase where applications are distributed and utilized by users. As some application distribution sites review application security with minimum scrutiny, a large number of applications may not be secure. Therefore, users using these applications need to be very careful when they download and use insecure applications. Application distribution sites can apply a reputation mechanism that collects evaluations of applications from users, and need to educate users about how to download and use applications carefully.

7.2.4 Update

This phase is where developers update their applications. After update, a reviewer needs to re-examine the applications at the distribution site.

7.2.5 Removal

This phase is where applications are removed from distribution sites. If an application is identified as harmful or malicious, distribution sites need to remove it. Additionally, distribution sites need to recommend that its users remove the application from their communication devices. Distribution sites may apply a remote system that enables them to remove the harmful application, depending on user consent.

8 Secure application distribution framework for communication devices

Figure 2 shows a secure application distribution framework for communication devices. This clause defines the processes for each element in this framework.

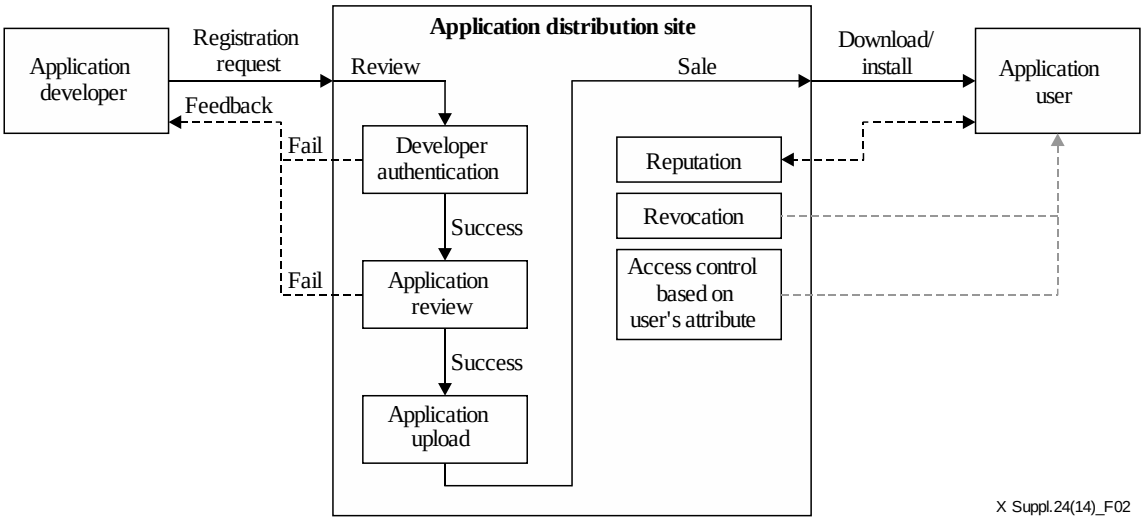

Figure 2 – Secure application distribution framework for communication devices

8.1 Developer authentication

Application distribution sites authenticate the existence and identity of developers, regardless of the company or individuals involved. Authentication of the developer's existence can prevent malicious attacks at an early stage for secure application distribution. Furthermore, the developer should be clearly identified to reassure application users as well as distribution sites.

8.2 Application review

Distribution sites review the applications received from developers before accepting them. This enables sites to reject malware, spyware, and insecure applications. The sites can check applications with automatic (static or dynamic) analysis tools. Manual (human) review can also be used. The procedure of checking applications is advantageous for users because it enables secure and proper execution. This mechanism can be processed by the application distribution site.

8.3 Reputation

Application distribution sites manage a reputation system to enable users to choose secure applications. The reputation is produced by users who utilize the application. The reputation mechanism is used to collect users' comments and evaluations, and is useful for identifying problematic applications. On distribution of the application, sites can give overall reputation information to users. The reputation system can be relevant to users when purchasing an application. Therefore, application distribution sites should rigorously manage the reputation system.

8.4 Revocation

Distribution sites have an application revocation mechanism for malware and insecure applications. The revocation system for rejecting harmful applications can protect users from malicious attacks. A harmful application can be active on the user's smartphone; as a result, by using the revocation process, the application user can maintain the security of the smartphone.

8.5 Access control based on users' attributes

Applications that are not appropriate for children and young people require careful distribution. Therefore, distribution sites have a mechanism to control access to applications based on the user's attributes. This mechanism allows sites to distribute an application appropriate to a particular user.

8.6 Secure payment system

For a paid application, distribution sites use a secure payment system that provides safe management of the user's information and a quick response in case of problems. Sites are typically interested in generating profit from distributing tpaid applications to users. In this process, the secure payment system should be designed to ensure the protection of the user's payment information and all other related transactions (e.g., credit card).

9 Requirements for secure application distribution

9.1 Developer authentication

Distribution sites are recommended to authenticate application developers and their real existence. The developer is authenticated at an early stage, and this can be achieved by various identification mechanisms. Authentication can be achieved by the following two elements:

1) Application distribution sites provide a developer registration mechanism. During the registration phase, they need to check the real existence of the developer. They can use several kinds of information to identify developers, such as credit card authentication, and a certificate issued by a trusted third party (TTP).
2) Application distribution sites provide a mechanism to identify the developer. Normally, developers generate digital signatures for their applications, and distribution sites as well as users can verify these signatures to check who developed applications.

9.2 Application review

Distribution sites are recommended to check applications before distributing them. The purpose of this check is to prevent users of distribution sites from using these harmful or dangerous applications. Harmful or dangerous applications may include malware, collection of privacy information, and transfer of sensitive information without encryption. The criteria for harmful and dangerous applications are defined on application distribution sites. The criteria can also be classified in detail, such as no excessive use of network bandwidth, supporting secure transfer of sensitive data, and no collection of unnecessary information in service scenario. Appendix I provides examples of check items for the application review.

9.3 Reputation

Sites can optionally provide a mechanism whereby users can check the reputation of applications distributed. Information on reputation is gathered from application users. In order to increase the reliability of the evaluation of reputation, distribution sites need to authenticate users who submit their comments on applications. It is advisable for distribution sites to collect various opinions on reputation from application users.

9.4 Revocation

Application distribution sites are recommended to provide a revocation mechanism. As an improper revocation can be harmful for communication devices, application distribution sites are recommended to provide online revocation securely. The following are examples of revocation mechanisms, if a problematic or malicious application is detected, distribution sites will:

- remove it from their sites;

- send this information to the communication devices, which in turn will remove it, with the user's consent;
- send a request to remove it from the users' devices.

9.5 Access control based on users' attributes

Sites are recommended to provide an access control mechanism for applications based on the user's attributes. It is also recommended that a secure access control mechanism be applied for application distribution sites. This mechanism is composed of three elements:

- Attribution setting based on several kinds of information, such as the user's information and preference, as well as accessing country or region.
- Access control setting for each application. Both developer and distribution sites can assign such settings.
- Access control to applications based on the user's attributes.

Appendix I

Application review

I.1 Examples of checking items

Table I.1 lists examples of checking items for the application review.

Table I.1 – Examples of checking items for application review

Classification	Examples of criteria
Network aspect	Excessive network load should not be caused by frequent network access attempts. Network capacity should not be used excessively, or excessive loads should not be applied to the device, using the alarm service.
Data aspect	Important information should not be displayed directly. Important information, such as a password or financial information, should be displayed as "●●●●●●" or "********". All packets should be encrypted when important information is transferred. All important information should be saved in an encrypted terminal.
Virus and malicious code infection aspect	The application should not be infected with malicious code.
Log-in security	The application should be logged out automatically if the service is not used for a certain period of time. The user should not be allowed to log in more than one time.
Rights management	The user's right for the screen that handles important information should be assigned properly. A use of the right that is not notified to the user in advance should be prohibited. The application should not be able to use the unauthorized rights according to the service scenario.
Device damage	The application should not consume the charge in the device battery excessively or generate excessive heat.
Push alarm service	The application should not send sensitive personal information or confidential information using the push alarm service. The application should not send an unsolicited message, phishing or spam e-mail, using the push alarm service.
Miscellaneous	The application should not provide an unspecified false or fake function. The application should not be used for illegal file sharing. The application should not be able to identify the user's password or personal information, using an illegal method.

I.2 Testing and evaluation mechanism

Testing and evaluation capabilities can be included but are not limited to those listed in Table I.2.

Table I.2 – Testing and evaluation mechanism

Classification	Examples of criteria
Specification examination	The examination that is performed to identify the functions of the software, the application programming interface (API) used, and the qualification of developers, etc. If the examination has failed, the applications will not be accepted by the online application store.
Static analysis	The analysis of software that is performed without actually executing programs built from that software. In most cases, the analysis is performed on the object code by an automated tool, which is also called program understanding, program comprehension or code review. Usually, static analysis is used for scanning malicious uniform resource locators (URLs) and viruses based on specific signatures. In addition, some APIs can only be used by the operating system (OS) owners. Therefore, misused APIs can also be detected by the static analysis.
Dynamic analysis	The analysis of software that is performed by executing programs built from that software system on a real or virtual processor. For the dynamic program analysis to be effective, the target program must be executed with sufficient test inputs to produce interesting behaviour. Use of software testing techniques such as code coverage helps ensure that an adequate slice of the program's set of possible behaviours has been observed. Also, care must be taken to minimize the effect that instrumentation has on the execution of the target program.
Vulnerability scanning	Performed by scanning based on common vulnerabilities and exposures (CVE) database, to find the potential vulnerabilities in applications.
Manual check	The real practice with software on smartphones, which can be used for malware based on human engineering and other malware which could not be detected by the above automatic analysis.
Security support database	Include sample database of malicious codes, signature database of malicious behaviours, vulnerability database of applications, etc.

Bibliography

[b-ITU-T X-Sup.19] Recommendations ITU-T X-series – Supplement 19 (2013), *ITU-T X.1120-X.1139 series – Supplement on security aspects of smartphones*.

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

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, 2015