International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1249

(01/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Technical framework for countering mobile in-application advertising spam

Recommendation ITU-T X.1249

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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.

Recommendation ITU-T X.1249

Technical framework for countering mobile in-application advertising spam

Summary

Recommendation ITU-T X.1249 provides a technical framework for countering mobile in-application advertising spam. Mobile in-application advertising spam is the sending of unsolicited advertisements, which are displayed within a mobile phone application. This unsolicited advertising can appear on the display screen of a mobile device as a banner at the top or bottom of the screen, a mobile interstitial or an overlay. Along with the rapidly increasing development of mobile applications, there has been a dramatic surge in mobile in-application advertisements and the filtering of malicious advertisements may improve user experience and even security. Therefore, it may be beneficial to establish a practical framework for countering mobile in-application advertising spam, which can reasonably integrate the advantages of all countermeasures.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1249	2019-01-30	17	11.1002/1000/13605

Keywords

Mobile in-application advertisement, spam.

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation 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 Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation 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 Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. 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

Recommendation ITU-T X.1249

Technical framework for countering mobile in-application advertising spam

1 Scope

This Recommendation provides a technical framework for countering mobile in-application advertising spam. In this framework, functional components, filtering rules and workflows are specified. In addition, this Recommendation proposes a feedback platform for countering mobile in-application advertising spam.

This Recommendation is applicable for application providers and mobile Internet service providers.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 mobile phone [b-ITU-T X-Sup.19]: 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.

3.1.2 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.

3.1.3 spam [b-ITU-T X.1242]: The electronic information delivered from senders to recipients by terminals such as computers, mobile phones, telephones, etc., which is usually unsolicited, unwanted, and harmful for recipients.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 asynchronous filtering: A file processing technique for identifying spam advertisements (ads), that makes it possible to process to several identifications simultaneously.

3.2.2 mobile application: A software application designed to run on mobile devices such as smartphones and tablet computers.

3.2.3 mobile in-application advertising: An advertisement displayed within a mobile application. It can be displayed on the mobile device's screen as a banner at the top or bottom of the screen, mobile interstitial or as an overlay, etc.

3.2.4 mobile in-application advertising spam: Mobile in-application advertising which is usually unsolicited, unwanted and harmful for recipients.

NOTE 1 – "unsolicited" herein means "user not asked for" and "unwanted" means that users have done something to clearly express their rejection, such as turning off the option of receiving some kinds of advertising.

NOTE 2 – Mobile in-application advertising spam is usually sent indiscriminately, in bulk and repetitively. Examples of actual and tangible harm include fraud or conveyance of malicious code.

3.2.5 synchronous filtering: A file processing technique for identifying spam advertisements (ads), which waits for one to complete before the next begins.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AD Advertisement

API Application Program Interface

ID Identity

IP Internet Protocol

URL Uniform Resource Locator

5 Conventions

None.

6 General aspects

Due to the rapid development of mobile Internet and the open nature of mobile operating systems, mobile in-application advertisements have also been developing rapidly. Usually, a mobile application invokes an application program interface (API) provided by the service platform to deliver advertisements (ads). Because ads delivered by mobile applications are free or almost free, mobile in-application advertisements have become very popular. Most of them are legitimate ads, which are suitable for users, while some of them are spam. Many measures such as opt-in or opt-out have been adopted for blocking advertisement spam.

Although many countermeasures have been implemented to counter mobile in-application advertising spam, a technical framework in fighting such mobile-in application advertising is still missing. Mobile in-application advertising spam may cause many negative influences to applications and service providers. Mobile in-application advertising spam may consume a large volume of data bandwidth or may cause data-traffic jams, and can even convey mobile fraud. No single measure has proved to be a totally adequate solution to countering spam. We seek here to establish a practical framework for countering mobile in-application advertising spam, which can reasonably integrate all the advantages of countering mobile in-application spam countermeasures.

7 Technical framework

Filtering systems for countering mobile in-application advertising spam (i.e., the spam-filtering system) are mainly implemented in service platforms providing service APIs for apps. The apps can invoke these APIs to deliver ads and other messages. The technical framework for countering mobile in-application advertising spam is shown as Figure 1.

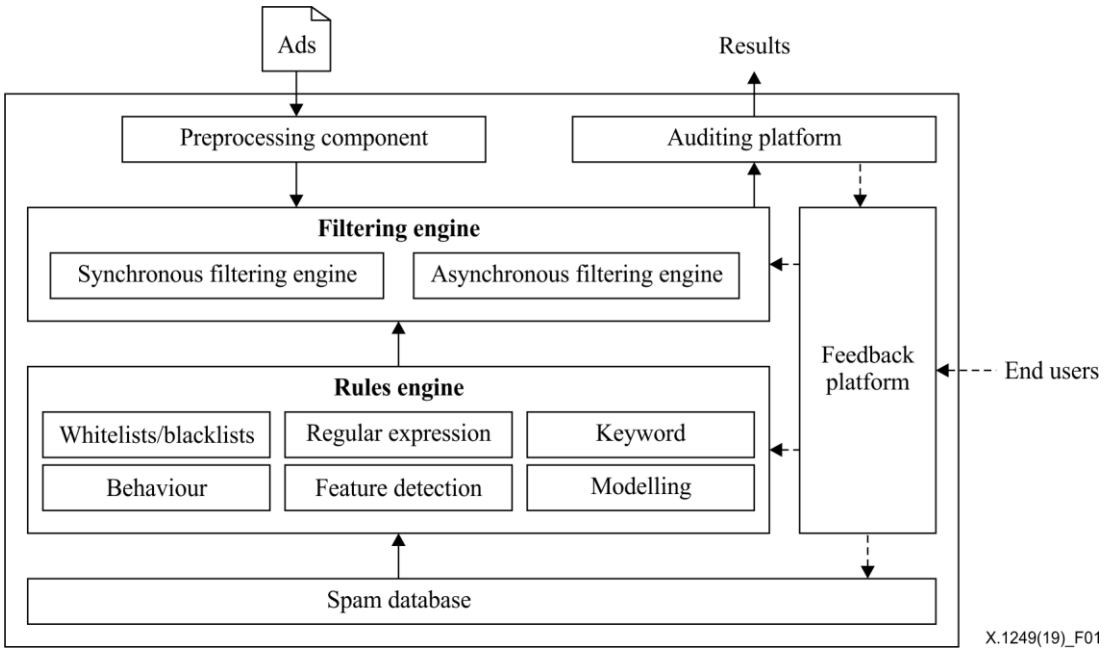

Figure 1 – Technical framework for countering mobile in-application advertising spam

8 Functional components

8.1 Preprocessing component

The preprocessing component is used to preprocess the original ad files to convert them to the format required by the filtering engines, such as separating the contents of text, image, uniform resource locator (URL), audio and video, etc.

8.2 Filtering engines

Filtering engines are the most important components of a mobile in-application advertising spam-filtering system. The main objective of filtering engines is to identify actual mobile in-application advertising spam or the possibility of such spam. According to the various ways of identifying mobile in-application advertising spam, filtering engines could be classified as synchronous or asynchronous filtering. In terms of time efficiency, an asynchronous filtering engine is usually better than synchronous filtering engine.

8.2.1 Synchronous filtering engine

Synchronous filtering waits for one filtering rule to complete before the next begins. Synchronous filtering refers to online filtering due to its lower complexity, and the filtering results would take a very short time to produce. Normally, the results of synchronous filtering can be known immediately, which means the decision will be made as soon as the filtering completes. If the results of a filtering rule have an impact on the execution of the subsequent filtering rules, then synchronous filtering is suggested. Synchronous filtering could include filtering using whitelists\blacklists, regular expressions, behaviour modelling, feature detection, etc.

8.2.2 Asynchronous filtering engine

Asynchronous filtering enables various workflow processes to run at the same time; that is, various workflows do not depend on each other's outcomes. Asynchronous filtering refers to offline filtering due to the higher complexity of mobile in-application advertising spam filtering, and usually the filtering results take a long time to produce. Asynchronous filtering usually includes audio recognition, video recognition, keywords matching, deep modelling, etc.

8.3 Rules engines

Rules engines provide filtering rules, including all rules which can be used for filtering engines. Filtering rules have several sources: operator configurations, spam databases and third-party rules sharing. The rules engine provides decision rules for identifying mobile in-application advertising spam. Some decision rules will be based on the sum of the weighted values of the various tests for spam if the filtering results are not determinate. The rules engine will provide a threshold (i.e., fixed) value. If the sum is over the threshold value, the filtering engine will decide whether the ad is spam. In addition, the rules engine can integrate different detection factors from the filtering engine together to determine whether an ad is mobile in-application advertising spam.

8.4 Auditing platform

Not all mobile in-application advertising spam can be detected by filtering engines. Therefore, manual methods should be used for mobile in-application advertising spam evaluation and an auditing platform is introduced. Via the auditing platform, the auditor can find unknown mobile in-application advertising spam which filtering engines cannot recognize. The accuracy of the auditing platform is usually higher than that of the filtering engines. Therefore, the results from the auditing platform can be deposited into a mobile in-application advertising spam database for future utilization.

8.5 Mobile in-application advertising spam database

This database is used for storing mobile in-application advertising spam characteristics. It is a logical database and could be maintained by each service provider or shared by several service providers. Mobile in-application advertising spam characteristics from the database can be used for comparing and filtering. Enriching the mobile in-application advertising spam database can help to improve the performance of the rules engine. The mobile in-application advertising spam database can be enriched by the feedback platform extracting characteristics from newly identified mobile in-application advertising spam.

8.6 Feedback platform

End users are targets, victims and receivers of mobile in-application advertising spam. Along with results from the auditing platform, the participation of end users is helpful to effectively and efficiently counter mobile in-application advertising spam. Therefore, the feedback platform should also take end users' responses into account. Mechanisms need to be established to support this aim, including providing feedback to the spam ads database. Such feedback-handling procedures need to be transparent, efficient and effective. In addition, it is necessary for feedback platforms to record feedback in a standard format. This will allow different operators and entities to share the feedback. Spammers' main addresses can be obtained from the shared feedback, and these addresses can be added and used in the blacklists.

9 Filtering rules

9.1 Keywords

Keywords are used to determine whether the content (i.e. words) of an ad matches the samples found in the mobile in-application advertising spam database. Keywords are derived from the following sources: operator configuration, external channels, the feedback platform and machine learning from spam databases. Keywords can accurately identify high-risk malicious ads, in a short period of time at a low cost; therefore, they are often used for synchronous filtering. To improve the effect of keywords, it is necessary to consider a preprocess of the original text to filter some intentionally confused characters, and some different encoding types of the keywords especially in URLs' filtering.

9.2 Blacklists/whitelists

Blacklists are based on the principle of maintaining Internet protocol (IP) addresses or domains that are suspected of sending mobile in-application advertising spam. These lists can also include device identity (ID), URLs or sender accounts in the service platform. They can be implemented by an entity for shared use, or introduced and maintained by the service platform using it for its own requirements. Whitelists are based on the principle of listing sources/entities of approved or recognized ads. These lists can include device ID or sender accounts in service platforms. Similar to keywords, although blacklists and whitelists inevitably contain inaccuracies and blacklists can possibly prevent some legitimate ads from getting through filtering engines, both blacklists and whitelists are an effective solution for filtering mobile in-application advertising spam.

9.3 Regular expression

Regular expressions are usually used to exactly match and filter malicious ads in text form with some specific patterns. They are flexible, logical and functional, and usually lead to a final result which does not need additional judgment or modifications. Unlike a keyword or a blacklist/whitelist, a regular expression can be used to match a series of ads that differ in content but with a particular form. Regular expressions are also widely used in synchronous filtering for high efficiency. They are also widely used in synchronous filtering with the fact that a well-designed regular expression would bring a high accuracy. To avoid unpredictable resource consumption, the regular expressions should be fully tested including performance and accuracy before use.

9.4 Feature detection

Feature detection is a common application of computer vision usually based on pattern recognition and machine learning. The most representative use of feature detection is to recognize malicious ads from thousands of pictures. Feature detection needs to compute, extract and store features from known mobile in-application advertising spam into the mobile in-application advertising spam database. When receiving a suspected image, feature detection computes the abstraction information of the image and makes a decision to see whether there it contains a malicious ad at that point. Feature extraction algorithms and corresponding matching algorithms, determine whether it can quickly and accurately find malicious advertising images. Feature detection usually provides a fuzzy conclusion, and needs to combine an additional decision-making process to determine the final results. Due to the complexity of calculations and comparing of the entire file, feature detection is more often used for asynchronous filtering.

9.5 Behaviour

Mobile in-application advertising spam are typically sent in bulk, indiscriminately or repetitively, and also have some other particular characteristics. Filtering engines can record mobile ads' behaviours and calculate the relationships between them. When the received ad's behaviour is consistent with characteristics already stored in the spam database, it is possible to determine that the file is likely to be a malicious ad. Since behaviours of ads are uncertain in terms of time, behaviour detection could be utilized to identify the unknown malicious ads, and is more suitable for asynchronous filtering.

9.6 Model checking

Model checking is an important approach that has emerged for verifying requirements. For example, the similarity model and decision tree model are effective in detecting mobile in-application advertising spam. Sometimes single models cannot determine whether ads are malicious, while a combination of several models, such as model stacking, can be used for comprehensive detection. Model checking can be used for both synchronous and asynchronous filtering.

10 Workflows

Mobile in-application advertising spam filtering usually follows the serial process shown in Figure 2. In some cases, synchronous filtering engines and asynchronous filtering engines can also be in parallel.

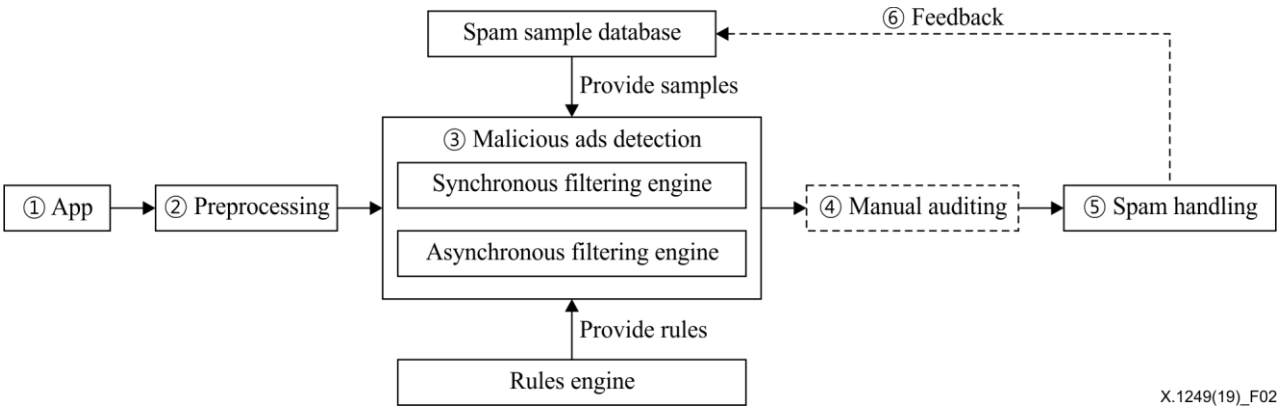

Figure 2 – Workflows for spam ad filtering

The general steps are as follows:

1) Ads are provided and delivered to mobile phone applications.

2) Ads should be preprocessed in advance. For example, the various types of ad media will be separated into URLs, text, audio, video, etc.

3) According to the threats and complexity of filtering, the content will be delivered to the synchronous filtering engine or the asynchronous filtering engine, which are preconfigured but can be adjusted as needed. For comprehensive detection, it is sometimes necessary to load the same content into both the synchronous and asynchronous filtering engines. Combined together with the rules and samples provided by the rules engine and the mobile in-application advertising spam database, ads are checked to determine if filtering is necessary.

   a) The synchronous filtering engine will detect mobile in-application advertising spam after step 2 based on the filtering rules from the rules engine. If the synchronous filtering module finds mobile in-application advertising spam, the spam filtering will complete, the ad will be blocked immediately and it will proceed to step 6. If the URLs or accounts in apps belong to whitelists in the synchronous filtering engine, the ad will be delivered directly. If the ads cannot be evaluated, then proceed to step 4.

   b) The asynchronous filtering engine will detect spam in ads after step 2 based on the filtering rules from the rules engine. If the asynchronous filtering module finds spam, the spam filtering will complete, the ad will be blocked immediately and it will proceed to step 6. If the ads cannot be evaluated, then proceed to step 4.

4) Ads sometimes need to be tested and evaluated manually. If spam is detected and confirmed, then proceed to step 5.

5) According to the pre-configuration, spam ads are dealt with, such as recording, replacing, etc.

6) Mobile in-application advertising spam ads are stored in the mobile in-application advertising spam database. In addition, mobile in-application advertising spam from the spam database can be extracted as new rules and loaded into the rules engine, or utilized for optimizing the rules engine.

11 Performance requirements

The accuracy of mobile in-application advertising spam detection should be measured by the combination of false positive and false negative rates, which should be considered to be balanced.

11.1 Accuracy requirements

False positive rates are calculated as the ratio between the number of valid ads that are misidentified as spam or malicious, and the total number of valid ads. If the false positive rate is high, it means some valid advertising of mobile apps has been blocked. Therefore, false positive rates should be decreased as much as possible.

False negative rates are calculated as the ratio between the number of mobile in-application advertising spam advertisements that are misidentified as valid, and the total number of mobile in-application advertising spam advertisements. If the false negative rate is high, it means users would be more easily subjected to mobile in-application advertising spam. Therefore, false negative rates should also be decreased as much as possible.

11.2 Efficiency requirements

Efficiency of a mobile in-application advertising spam filtering algorithm can be measured by its time and space complexity in the filtering engine. Time complexity refers to the time needed for a filtering ad's process to run, while space complexity refers to the space needed (memory). These two indicators have an important impact on the application type of the filtering rule. Lower time and space complexity filtering rules can be applied in the synchronous filtering engines while higher ones could be applied in the asynchronous filtering engines.

Bibliography

[b-ITU-T X.509] Recommendation ITU-T X.509 (2016), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

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

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam.*

[b-ITU-T X.1242] Recommendation ITU-T X.1242 (2009), *Short message service (SMS) spam filtering system based on user-specified rules*.

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

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

[b-ITU-T X-Sup.24] ITU-T X-series Recommendations – Supplement 24 (2014), *Supplement on a secure application distribution framework for communication devices*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019