International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1214

(03/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

Security assessment techniques in telecommunication/information and communication technology networks

Recommendation ITU-T X.1214

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
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.1214

Security assessment techniques in telecommunication/information and communication technology networks

Summary

Recommendation ITU-T X.1214 describes a security assessment methodology for software-based telecommunication/information and communication technology (ICT) network elements and best practices for developers, manufacturers, operators and individual security experts in the telecommunication domain to address the security of their software-based elements. Both traditional circuit-switched networks and packet-based networks are exposed to different threats and attacks – from external as well as internal sources – that target the various parts of the telecommunication/ICT network. In telecommunication/ICT networks, this Recommendation covers:

– detection of vulnerabilities;

– methodology of security assessment.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1214	2018-03-29	17	11.1002/1000/13404

Keywords

Binary analysis, fuzzing, penetration testing, security assessment, security test, source code review, vulnerability scanning.

---

* 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

Introduction

Telecommunication/ICT networks play a critical role in the economic growth of most countries. This has led to government regulation of the telecom industry, which includes requirements to ensure the security of the telecom equipment and networks. Telecom operators should adopt a robust and managed security programme to ensure that software-based elements of their networks are protected against malicious attacks, both external and internal, while also ensuring compliance with the local regulatory environment. This requires that a very effective security assessment mechanism be in place for these software-based elements founded on globally accepted security standards and best practices.

Maintaining a consistent security posture across an organization's network in the face of the ever-changing nature of the threat landscape is a complex and time consuming task. Organizations may have to incur heavy expenditure while recovering from a security breach. These costs are related to remediation efforts, customer protection and retention programs, legal activities, discouraged business partners, lowered employee productivity and reduced revenue. An effective security evaluation approach helps them to avoid these financial pitfalls by proactively identifying and addressing risks to their software-based assets and capabilities before attacks or security breaches occur. An independent evaluation from a security point of view is increasingly demanded by markets such as government, the financial sector and telecommunications.

This Recommendation mainly highlights the security assessment techniques to be adopted by telecom/ICT network operators and service providers for proactive identification and assessment of vulnerabilities in their software-based elements.

Recommendation ITU-T X.1214

Security assessment techniques in telecommunication/information and communication technology networks

1 Scope

This Recommendation discusses security assessment techniques that can be used on software-based elements in telecommunication/information and communication technology (ICT) networks. Both traditional circuit-switched networks and packet-based next generation networks are exposed to different threats and attacks – from external as well as internal sources – that target the various parts of software-based elements of a telecommunications/ICT network. Security assessment of software-based components before deployment in these networks can help operators and service providers to enhance the reliability of networks to a considerable extent. Hence, there is a requirement for standardization in this area, so that global security assessment standards and best practices for software-based elements can be made available to developers, manufacturers, operators and individual security experts.

These techniques can be used individually or in combination, as desired or felt appropriate.

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.

[ITU-T X.1520] Recommendation ITU-T X.1520 (2014), *Common vulnerabilities and exposures*.

[ITU-T X.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration*.

[ITU-T X.1544] Recommendation ITU-T X.1544 (2013), *Common attack pattern enumeration and classification.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 repository [ITU-T X.1524]: An implicit or explicit collection of security-related software weakness elements that supports a capability, e.g., a database of security weaknesses, the set of patterns in a code analyser, or a website.

3.1.2 vulnerability [ITU-T X.1520]: Any weakness in software that could be exploited to violate a system or the information it contains.

3.1.3 weakness [ITU-T X.1524]: A shortcoming or imperfection in the software code, design, architecture, or deployment that, could, at some point become a vulnerability, or contribute to the introduction of other vulnerabilities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 binary analysis: A technique of identification of weaknesses in machine language executable files.

3.2.2 fuzzing: A technique for discovering unknown or zero day vulnerabilities in a software by providing unexpected inputs towards it and monitoring it for exceptions.

3.2.3 mutation: Mangling individual bytes, words or strings within an input data packet.

3.2.4 penetration testing: A technique for evaluating the impact of exploitation of identified vulnerabilities.

3.2.5 security assessment: An explicit study to locate security vulnerabilities and risks.

3.2.6 signature-based scanning: A scanning technique that compares the contents of a target to its database of known signatures to identify vulnerabilities.

If a particular signature is matched, then the scanner identifies the vulnerability and suggests the remedial action also.

3.2.7 source code review: A technique of identification of weaknesses in software code segments written in high level languages.

3.2.8 tool: A software application or device that examines a host, network, a piece of software, binary, a software application or device or other artefact and produces information that is related to vulnerabilities, weaknesses or exposures, e.g., a vulnerability scanner, fuzzer, a source code review tool, binary analyser or a penetration testing tool.

3.2.9 vulnerability scanning: A technique of identification of known or published vulnerabilities within a target.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CAPEC Common Attack Pattern Enumeration and Classification

CVE Common Vulnerabilities and Exposures

CWE Common Weakness Enumeration

DUT Device Under Test

ICT Information and Communication Technology

OS Operating System

SQL Structured Query Language

5 Conventions

None.

6 Basic concept – Security testing

Telecommunication/ICT networks are likely to have a heterogeneous mix of equipment from various suppliers. A highly credible, trusted third party certification programme must be in place to conduct an assessment to identify and evaluate security weaknesses and vulnerabilities contained in equipment software, firmware and hardware implementations. The security evaluation of a product

mainly revolves around detection and validation of vulnerabilities present therein. Detection of vulnerabilities can be divided into two major categories (see clauses 6.1 and 6.2).

6.1 Detection of known or published vulnerabilities

Software vulnerabilities are found in commonly used software products on a daily basis. These vulnerabilities, e.g., common vulnerabilities and exposures (CVE), have been published by the National Vulnerability Database and several other databases. Efficient management of published vulnerabilities is thus an important activity in the security efforts of modern enterprises. To manually keep track of all vulnerabilities present in systems and remedy them appropriately is a daunting task. There are automated tools available that perform signature-based scanning to detect these vulnerabilities and identify them with reference to [b-CVE].

6.2 Detection of unknown or zero day vulnerabilities

This type of detection involves the discovery of vulnerabilities that have not been published so far. There are a variety of approaches to this, each with its own advantages and disadvantages. No one approach is complete and no single method can uncover all possible vulnerabilities for a given target. Tools and techniques used for unknown or zero day vulnerability detection include fuzzers, source code review tools and binary analysis tools. Details of these tools are given in clauses 7.2 to 7.5.

7 Security testing techniques

As mentioned above, there is a variety of approaches to detecting vulnerabilities in software-based elements, each with its own advantages and disadvantages. No single method can uncover all possible vulnerabilities for a given target. Hence, an effective assessment mechanism would certainly believe in adopting multiple approaches, which are discussed in clauses 7.1 to 7.5.

7.1 Vulnerability scanning

A network vulnerability scanner is an appliance or software that is used to scan the architecture of a network and report any identified vulnerabilities in software-based elements of the network. During the vulnerability scan, a database of vulnerability signatures is compared to the information obtained from a network scan to produce a list of vulnerabilities that are presumably present in the network. Sometimes, it also has an embedded penetration testing tool to provide the possibility of actually exploiting the identified vulnerabilities to fully verify their presence. Vulnerability analysis is the process of evaluating the severity of identified vulnerabilities. Organizations typically have a large number of vulnerabilities in their operational environment and some of which lead to higher security risks than others. For instance, some software vulnerabilities have dire consequences if they are exploited. It is thus important to assess the most significant problems and remedy these first.

Vulnerability scanning can typically be performed on systems that are connected to the Internet, as well as on internal networks that are not connected to the Internet in order to assess software vulnerabilities.

The tools, repositories and services used for vulnerability scanning shall be CVE compatible with the requirements and functionalities specified in [ITU-T X.1520].

7.2 Fuzzing

Fuzzing is defined as a method for discovering unknown or zero day vulnerabilities in software by providing unexpected inputs and monitoring it for exceptions. It is typically an automated or semi-automated process that involves repeatedly manipulating and supplying data to target software for processing. The target software may be a protocol stack, an application or files, depending upon which the fuzzer may be a protocol fuzzer, application fuzzer or file fuzzer. The researcher or tester requires

no knowledge about the internal working of the target and that is why this approach is also sometimes referred to as a black box testing approach.

There are mainly two types of approaches for fuzzing, i.e., generation-based fuzzing and mutation-based fuzzing, as described in clauses 7.2.1 and 7.2.2, respectively.

7.2.1 Generation-based fuzzing

In this approach, development of test cases begins with studying a particular specification to understand all supported data structures and the acceptable value ranges for each. Inputs for the targets are then generated that test boundary conditions or violate the specification altogether. Creating test cases may require a considerable amount of preliminary work, but has the advantage of being able to be reused for testing multiple implementations of the same protocol or file format.

7.2.2 Mutation-based fuzzing

Mutation-based fuzzers apply mutation to existing data samples in the form of packet capture related to the target to create test cases. Every individual byte, word or string within those samples is mangled and sent towards the target. This approach requires very little preliminary research and it can be developed in a short period of time. However, this is not a very efficient approach, as it may require collection of numerous data samples to get good coverage of a target protocol.

Fuzzers work best for problems that can cause a program to crash, such as buffer overflow, cross-site scripting, denial of service attacks, format bugs and structured query language (SQL) injection. Fuzz testing is less effective for dealing with security threats that do not cause program crashes, such as spyware, some viruses, worms, Trojans and keyloggers.

The tools, repositories and services used for fuzzing shall be common weakness enumeration (CWE) compatible with the requirements and functionalities specified in [ITU-T X.1524].

7.3 Source code review

Source code review is a common approach used by software developers to find weaknesses or flaws and is also known as white box testing. It can be accomplished either manually or with the assistance of automation tools. Given that software programs commonly comprise millions of lines of code, a pure manual review is generally impractical. Automated tools are an invaluable resource that make the task easier, but can only identify potentially vulnerable or suspicious code segments. Sometimes human analysis is required to determine whether detected issues are indeed valid, because this tool also yields false positive results. Reluctance from vendors or manufacturers towards sharing of source code is the biggest limitation of this approach.

The tools, repositories and services used for source code review shall be CWE compatible with the requirements and functionalities specified in [ITU-T X.1524].

7.4 Binary analysis

Security evaluation using machine language instructions instead of source code is typically referred to as binary analysis. Binary analysis creates a behavioural model by analysing the control and data flow of an application through executable machine code – the way an attacker sees it. Unlike source code tools, this approach accurately detects issues in the core application and extends coverage to vulnerabilities found in third party libraries, pre-packaged components and code introduced by a compiler or platform specific interpretations.

Software development is a multi-tier process where growing types of threats – such as those coming from malicious code and backdoors – are impossible to spot with source code review tools, because they are not visible in source code. These threats can be detected by using static binary analysis on the application in its final form.

The tools, repositories and services used for binary analysis shall be CWE compatible with the requirements and functionalities specified in [ITU-T X.1524].

7.5 Penetration testing

A penetration test is a proactive and authorized attempt to evaluate the security of an infrastructure by safely attempting to exploit system vulnerabilities, including operating system (OS), protocol and application flaws, improper configurations, and even risky end-user behaviour. The fundamental purpose of penetration testing is to measure the feasibility of systems or end-user compromise and to evaluate any related consequences such incidents may have on the resources or operations involved. Tests are typically performed using manual or automated technologies to systematically compromise servers, endpoints, web applications, wireless networks, network devices, mobile devices and other potential points of exposure. A penetration test target may be a white box (which provides background and system information) or a black box (which provides only basic or no information).

By performing a penetration test, vulnerabilities that are most critical, less significant or false positives can be proactively identified. This allows an organization to more intelligently prioritize remediation activities and apply needed security patches.

The tools, repositories and services used for penetration testing shall be common attack pattern enumeration and classification (CAPEC) compatible with the requirements and functionalities specified in [ITU-T X.1544].

Appendix I

Flow chart

(This appendix does not form an integral part of this Recommendation.)

Organizing security assessment techniques in a flowchart would be a good start to a security assessment process. In order to establish this, a model may be considered where the assessment begins from the most elementary part of the network and extends to the integrated systems deployed within it. Security is first provided to the source code of the software elements, then to applications and libraries in the system, proceeding to systems in the network and finally to the overall deployed network.

Hence, the entire security assessment can be organized in two major stages.

i. The first is the pre-deployment stage at which the target can be thoroughly checked using all the security assessment techniques discussed and the findings of this assessment should be used to mitigate the vulnerabilities found.

ii. The second could be the post-deployment stage at which the target is already operational in the network. At this stage it may not be practical to subject the target to all the assessment techniques. Therefore, security analysers may resort to periodical vulnerability scanning to ensure that the vulnerabilities identified after the deployment of the product are being fixed regularly by installing patches, etc.

In the pre-deployment stage, as a first step, source codes of the software elements may be analysed and flaws detected may be corrected. Later, applications and libraries used by these applications are processed in a binary analysis. After the binary analysis, comes the fuzz testing and then the final stage is the vulnerability scanning and penetration test of the systems. Findings and observations of the overall assessment should be passed on to the respective developers, so that they may take corrective measures to mitigate all the detected vulnerabilities.

In the post-deployment stage, the whole network may be subjected to a periodic vulnerability scan. As and when any vulnerability is detected, it must be fixed.

A flowchart depicting the process is Figure I.1.

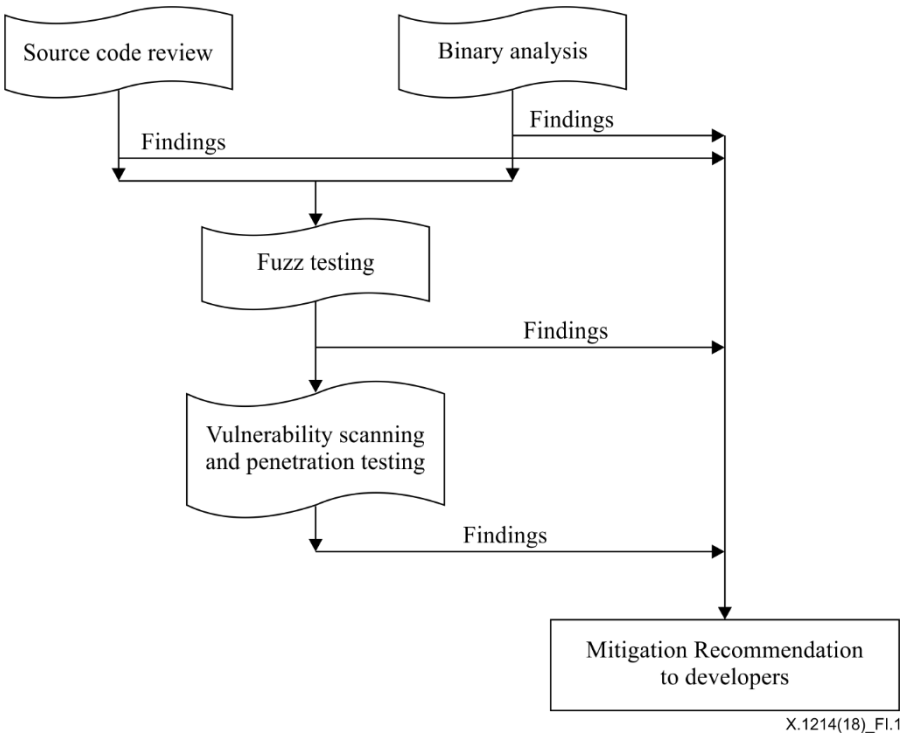

Figure I.1 – Flow chart for security assessment techniques

Appendix II

Other supplementary techniques for enhancing the security of an ICT network

(This appendix does not form an integral part of this Recommendation.)

This appendix provides some techniques for further enhancement of security of a telecom/ICT network.

II.1 Password strength assessment

Password-based authentication is widely used in telecommunication/ICT networks for purposes such as configuration, management, operation and maintenance and service provisioning. The robustness of these passwords should be assessed by system administrators to ensure that they may not be easily hacked. For this purpose, password cracking can be performed. There are various mechanisms available for password cracking, such as dictionary attack, brute force attack and rainbow tables.

II.2 Social confidentiality assessment

In some cases, psychological manipulation can be used on employees within organizations to cause them to divulge confidential information. It is a type of confidence trick for the purpose of information gathering, fraud or system access. Social engineering may be performed to assess the credibility of such individuals or groups within an organization. Specific targets may be identified when the organization knows of an existing threat or feels that the loss of information from a person or specific group of persons could have a significant impact.

II.3 Functional security assessment

Even though no specific tool(s) may be involved in functional security testing, the approach supplements the vulnerabilities detection techniques already discussed in clauses II.1 and II.2.

Security functional requirements for any device or network element used in telecommunication/ICT networks are:

i. local authentication of a user for configuration and management of a device;

ii. remote authentication of a user for configuration and management of a device;

iii. secure password storage in a device;

iv. secure crypto key management verification;

v. device protection mechanism against illegal software patching;

vi. remote management traffic protection of a device;

vii. classification of management users of devices according to privileges or permissions;

viii. secure time synchronization;

ix. audit (logs) event generation by the device under test (DUT);

x. secure audit logs export by the DUT.

II.4 Wireless scanning

Wireless scans can help organizations to take corrective measures to mitigate security risks posed by wireless-enabled technologies. A wireless scanning tool should be capable of scanning all IEEE 802.11 wireless devices [b-IEEE Std. 8802-11], whether domestic or international. Wireless scanning can identify unauthorized wireless devices within the range of the scanners, discover wireless signals outside an organization's perimeter, and detect potential backdoor and security violations.

II.5 Use of secure cryptographic module and algorithm implementations

Cryptographic algorithms are used for encryption and decryption of authentication data or user data for secure data transfer through telecommunication/ICT networks. Although cryptographic algorithms are well designed, implementation errors are common. If insecure algorithms having implementation flaws are deployed in telecommunication/ICT networks, they can be exploited by an attacker, leading to potential heavy data loss and fraudulent intrusion activities. Hence, highly secure cryptographic modules and algorithms may be used in telecommunication/ICT networks.

II.6 Network sniffing

Network sniffing is a passive technique that monitors network communication, decodes protocols, and examines headers to flag information of interest. It is also referred to as a network monitor or network analyser and can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic.

Using the information captured by the network sniffer, an administrator or a security expert can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain secure and efficient network data transmission.

Bibliography

[b-IEEE Std. 8802-11] ISO/IEC/IEEE 8802-11:2018(E) – *ISO/IEC/IEEE – International Standard – Information technology –Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*

[b-CVE] CVE Numbering Authorities (1999-2018*). Common vulnerabilities and exposures list.* Mitre Corporation.
https://cve.mitre.org/cve/

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, 2018