ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1219 (04/2023)

SERIES X: Data networks, open system communications and security

Cyberspace security – Cybersecurity

Functional requirements for a secured process to evaluate technical vulnerabilities

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	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (1)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
Cybersecurity	**X.1200-X.1229**
Countering spam	X.1230-X.1249
Identity management	X.1250-X.1279
SECURE APPLICATIONS AND SERVICES (2)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
IMT-2020 SECURITY	X.1800-X.1819

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

Recommendation ITU-T X.1219

Functional requirements for a secured process to evaluate technical vulnerabilities

Summary

Recommendation ITU-T X.1219 provides the functional requirements for a secured process to evaluate technical vulnerabilities.

Vulnerability evaluation by crowdsourcing is an effective approach for famous online systems to identify technical vulnerabilities. However, many problems and challenges remain such as when the shell scripts that are uploaded by members of security teams are not deleted after evaluation, which results in backdoors in the system.

The functional requirements provided in this Recommendation, and the corresponding security mechanisms, would help increase trust in the crowdsourcing approach by ensuring that vulnerability evaluations performed by security teams are reliable, auditable, traceable and controllable.

History [*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1219	2023-04-29	17	11.1002/1000/15542

Keywords

Audit, evaluation, reliable, vulnerability.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T X.1219

Functional requirements for a secured process to evaluate technical vulnerabilities

1 Scope

This Recommendation provides functional requirements for evaluating technical vulnerabilities. It analyses the advantages, problems and challenges of the common practice of vulnerability evaluation using crowdsourcing, and provides functional security requirements for a technical evaluation process. The features of the secured process, such as specified targets, behaviour audit, network traffic recovery, information sharing, etc., can build trust between security teams and organizations, secure the evaluation process, and enhance the potency of the evaluation.

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 crowdsourcing [b-ITU-T P.912]: Obtaining the needed service by a large group of people, most probably an online community.

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 automated vulnerability scanner: A program or software that can automatically identify and collect potentially suspicious technical vulnerabilities of a target through the Internet or intranet by matching responses from the target against a vulnerability library.

NOTE – The results of an automatic vulnerability scanner are mostly suggestions and may not be accurate.

3.2.2 technical vulnerability: A vulnerability that could be exploited by using technical measures.

4 Abbreviations and acronyms

None.

5 Conventions

None.

6 Security requirements analysis

6.1 Common practice in the industry

In recent years, many organizations have been willing to work directly with external (and internal) security volunteers or experts to discover technical vulnerabilities in their networks and online systems, as an important complement to automated vulnerability scanners.

A generic process of evaluating vulnerabilities by security volunteers or experts is shown in Figure 1. The organization publishes the targets needed to be evaluated on a public vulnerabilities report collection system. The target is usually a system or a website exposed on the public network. Security volunteers or experts would be invited/encouraged to spend time discovering technical vulnerabilities of the targets and submit them, thus helping to fix these vulnerabilities in time. During the evaluation, the targets could be a black box to these experts.

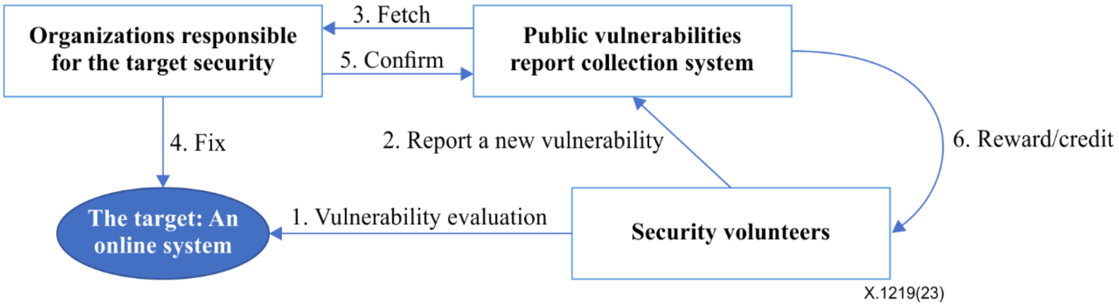
Organizations responsible for the target security
3. Fetch
5. Confirm
Public vulnerabilities report collection system
4. Fix
2. Report a new vulnerability
6. Reward/credit
The target: An online system
1. Vulnerability evaluation
Security volunteers
X.1219(23)

Figure 1 – Generic process of vulnerabilities evaluation by security volunteers or experts

6.2 Security risks

The process of vulnerability evaluation by security teams (security volunteers/experts) has several advantages, such as being more efficient, more economical, and more effective for the discovery of serious vulnerabilities. However, it also brings in security risks that cannot be ignored, such as:

- Targets to be evaluated may be put in the spotlight and become more vulnerable to malicious attacks as soon as their details are publicly disclosed.
- The generic process does not authenticate the identity of the members in a security team and cannot track their behaviours. It makes it difficult for organizations to distinguish between normal evaluations and malicious attacks, so that further protection on the targets becomes harder.
- The generic process usually does not have a standardized process to evaluate the quality of a vulnerability report submitted by security teams. The severity level of a vulnerability may not be accurate and objective enough. Therefore, serious vulnerabilities might not be fixed in a timely manner.
- New vulnerabilities discovered by security teams may be disguised, leaked, or exploited, which could cause serious damage to the targets.

6.3 Security capabilities

According to the above analysis, an evaluation process shall be reliable, auditable, traceable and controllable for it to resist the security risks analysed in the previous clause. To achieve these objectives, the security capabilities of the process to evaluate vulnerabilities by security teams must comply with the following requirements:

- It will have the capability to resist denial of service attacks and to detect and deal with abnormal traffic.

- It will have the capability to support data isolation to prevent the leakage of vulnerabilities and other sensitive data.
- It will have the capability to implement multi-factor authentication authorization management to prevent illegal access to the targets.
- It will have the capability to make a multi-dimensional audit to overhaul the behaviours of any member of a security team.
- It will have the capability to improve the experience of a security team in order to smooth the evaluation process with the integration of some security evaluating tools.

7 The functional framework of the secured process

It is recommended that the functional framework of the secured process be based on the security capabilities given in clause 6.3. The framework includes the three roles and five modules shown in Figure 2.

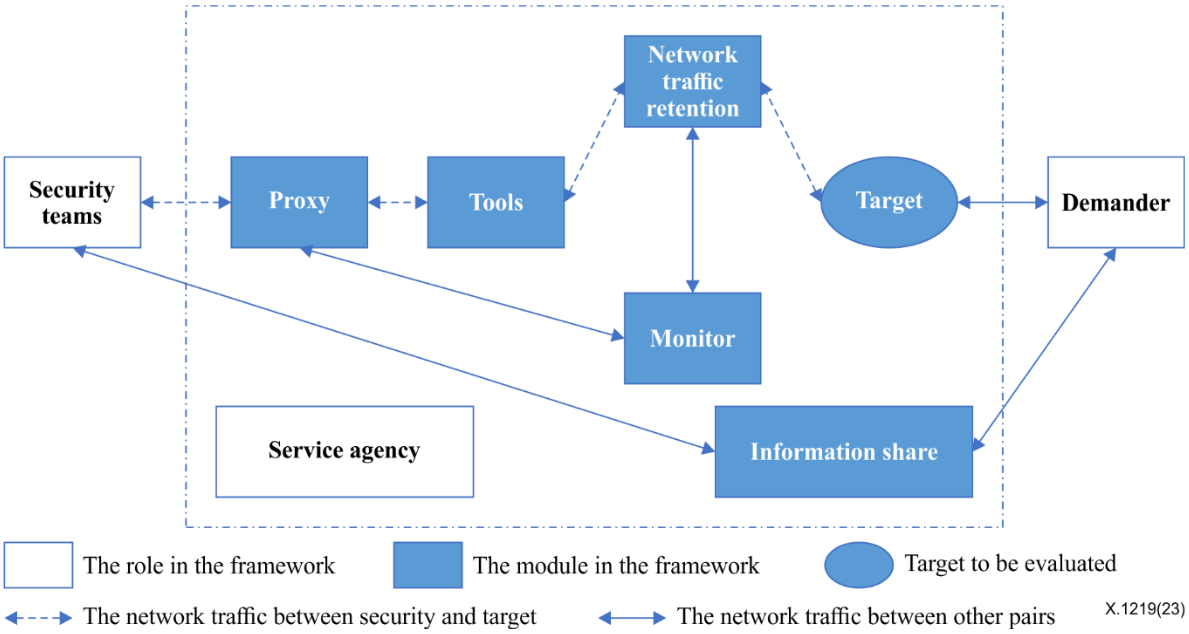
Network traffic retention
Security teams
Proxy
Tools
Target
Demander
Monitor
Service agency
Information share
The role in the framework
The module in the framework
Target to be evaluated
The network traffic between security and target
The network traffic between other pairs
X.1219(23)

Figure 2 – The functional framework of the secured process to evaluate technical vulnerabilities

7.1 The roles in the framework

7.1.1 Service agency

Service agency refers to an organization that has the capability to organize technical vulnerabilities evaluations on the targets authorized by demanders. The service agency would be the key role to regulate all the roles so that the secured process recommended in this Recommendation is followed, and would take the necessary measures to specify, manage and supervise the whole process and to conduct independent audits based on the network traffic and other information.

7.1.2 Demander

Demander refers to an organization, in most cases, that owns a target and would authorize a security agency to organize a technical vulnerabilities evaluation on the target.

7.1.3 Security team

Security team refers to a group of natural persons that would work collaboratively and use their own technical capabilities to perform a security vulnerabilities evaluation on a target under the premises that they will have proper authorization and that they shall not exploit the vulnerabilities to damage/abuse any target. The members of a security team do not necessarily belong to the same organization.

7.2 The modules in the framework

7.2.1 Proxy

The proxy module should be the only authorized and appointed gateway to permit security teams to carry out the technical vulnerability evaluation. This module could be a specific server or a group of dynamic servers in cloud computing. Therefore, the module should have two functions, namely identity authentication and connection management, which would easily allow for demanders to gather and distinguish all the security evaluation actions out of the malicious attacks and the normal service accesses.

7.2.2 Network traffic retention

The network traffic retention module forwards, duplicates (with sampling or filtering) and stores the network traffic exchanged between the security teams and the target with the help of the proxy module. Based on this, this module can implement the traceability of the actions of every member in a security team. The traceability requires the module to recover the sessions between any member and the target. Therefore, if the network traffic is encrypted, the module should have the authorization and the measures to do the decryption.

7.2.3 Monitor

The monitor module audits and manages the actions of the members of security teams. Based on the sessions recovered by the network traffic retention module, this module would audit or overhaul the actions of any members to check if their actions violated the authorization. If there are any, this module could send commands out to the proxy module to limit and abort any further session between a violating member and the target, and even block any further access of a whole security team, depending on the severity of the violation.

7.2.4 Information sharing

The information sharing module publishes the information of targets and shares the vulnerability-related information among the security teams, the service agency and the demander. The security team would submit newly discovered vulnerability information through this module. The service agency would review the submitted vulnerability and submit the validation result through this module. The demander would consider further actions (for example, how to deal with a confirmed vulnerability) according to the shared information. The module should have data isolation to limit the range of the shared information just among the roles binding with the target.

7.2.5 Tools (optional)

The tools module is a combination of the frequently used or popular security detection tools to help improve the efficiency of the security teams. The security detection tools could be the security information collection tool, the automated vulnerability scanner, the network asset mapping tool, or the network traffic packet forging tool, and so on. Any member of a security team could use this module to ease and speed up the evaluation.

8 The secured process

The secured process to evaluate the technical vulnerabilities is recommended as shown in Figure 3. This process should consist of three sub-processes, namely, the evaluation sub-process, management sub-process, and audit sub-process. In the process, these three sub-processes are not consecutive but interactive.

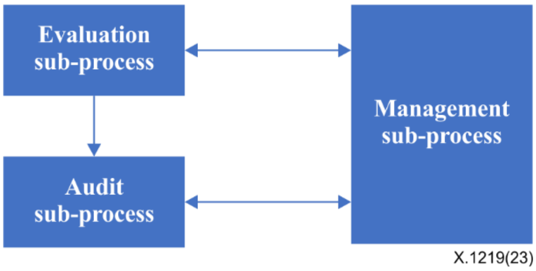

Figure 3 – Secured process to evaluate the technical vulnerabilities

- **Evaluation sub-process**: This sub-process would coordinate a demander, a service agency, and security teams to carry out an authorized evaluation for the technical vulnerabilities of a specified target.
- **Management sub-process**: This sub-process would assist a service agency to manage the authorization and the identification to serve the evaluation sub-process, and would respond to the audit results offered by the audit sub-process and take necessary measures on the evaluation sub-process.
- **Audit sub-process**: This sub-process would assist a service agency to audit the actions or behaviours of security teams according to the traceable information from the evaluation sub-process, to check any existence of a violation.

8.1 Evaluation sub-process

The evaluation sub-process includes the four steps shown in Figure 4.

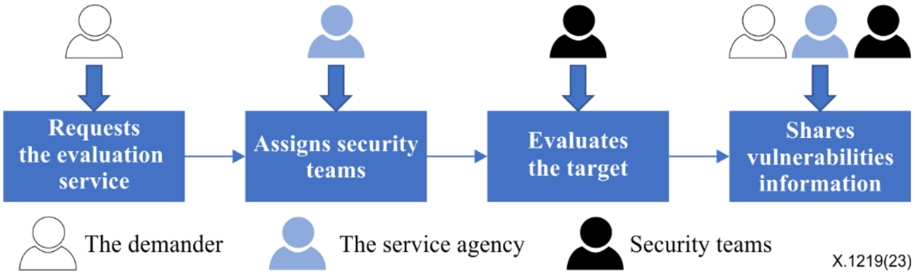

Figure 4 – Evaluation sub-process

- **Step 1**: An evaluation service would be required by a demander through the information sharing module. At the same time, the target, the time, and any other specific requirements or limits would be clarified by the demander to a service agency.
- **Step 2**: The announcement of the target would be available in the information sharing module. At least one security team would be assigned or recruited by the service agency and would be informed of the detailed requirements about the target through the information sharing module. On the other hand, the information technology (IT) environment necessary for the evaluation would also be prepared by the service agency, which would build only one permitted access path between the security teams and the target through the proxy module.
- **Step 3**: The module of proxy would be accessed by the members of the security teams to carry out the evaluation work collaboratively with their technical capabilities and the assistance of the tools module. Meanwhile, all the network traffic caused by the members of the security teams would be duplicated (filtered) and stored by the network traffic retention module.
- **Step 4**: Any newly discovered vulnerability with proofs would be submitted to the information sharing module by the members of the security teams, and the validation would be taken by the service agency accordingly. It would be considered that members that

discover more confirmed vulnerabilities could be credited more. When the evaluation period ends, the service agency submits to the demander the final report with all the target's confirmed technical vulnerabilities.

8.2 Management sub-process

The management sub-process includes the three steps shown in Figure 5.

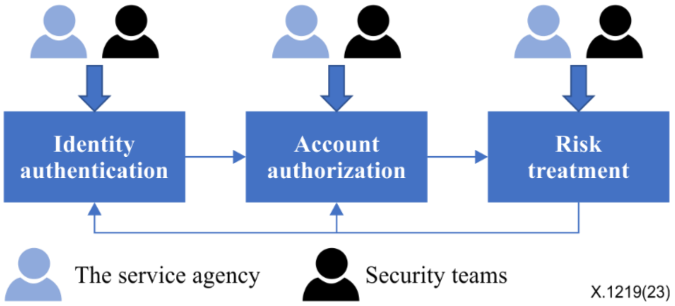

Figure 5 – The management sub-processes

- **Step 1**: The initialization of a profile of any member of a security team would be established or updated in the information sharing module. The authenticity of a new or updated profile should be verified by multi-factor authentication, such as the double confirmation by email or short message service. If required by a demander, it should be possible that the social identity of a member should be available and verifiable. As a member of a security team accesses the proxy module to do the evaluation-related work, the monitor module would authenticate the member's identity, secure the access (continuously) and log for audit.
- **Step 2**: As the agreement between a member of a security team and a service agency is achieved, the monitor module would authorize the member to access the target. A unique ID would be assigned to each member of a security team so that the network traffic between each member and the target could be marked and distinguished by the network traffic retention module.
- **Step 3**: If the audit results proof any (suspicious) violation of a member of a security team, the monitor module could be commanded by a service agency or automatically to deal with the authorization and the identity of the member, and maybe even those of the whole team. With the assistance of the proxy module, this could include the suspension of an/or multi-authorization, the cancellation of an/or multi-authorization, the deletion, or the embargo of one or multiple identities.

8.3 Audit sub-process

The audit sub-process includes the three steps shown in Figure 6.

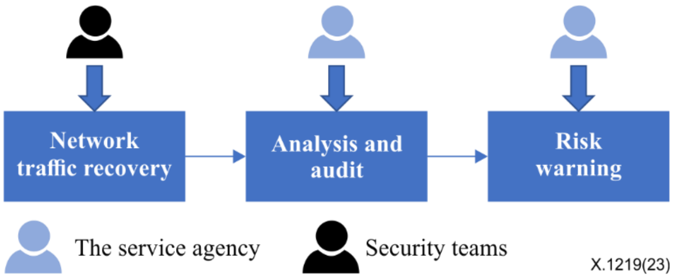

Figure 6 – The audit sub-process

- **Step 1**: The network traffic between any member and a target pair should be recovered in quasi-real time under the work of the network traffic retention module. The recovered network traffic with the integration of other logged information, such as the unique ID of any member, should show up the details of the actions or behaviours of any member in several dimensions, such as time, session ID, protocol type, protocol head, decrypted payload, source address, destination address, etc.

- **Step 2**: The monitor module should analyse and audit the actions or the behaviours of any member of a security team according to the recovered network traffic and all the logs in quasi-real time. It would identify and outline if there are any (suspicious) violation made by any member against the committed agreement during the evaluation sub-process. After the completion of an evaluation sub-process, an offline audit should be taken to clear any hidden risks, such as damaging the integrity of the data and concealment of discovered vulnerabilities.
- **Step 3**: A risk warning should be triggered to a service agency, through the information sharing module, if any (suspicious) violation is identified, such as download of sensitive data, abuse of computing resources, or installation of backdoor software, etc. These risk warnings and the corresponding proofs should be archived for further investigation.

Appendix I

Additional requirements for responsibilities of the roles

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

I.1 Service agency

A service agency should have the duty to submit a final report to a demander after the end of an evaluation. In the report, the service agency should give an overview of the security status of the specified target, and cover all the details of the confirmed or highly suspicious vulnerabilities. If feasible, the service agency report should also provide suggestions on the vulnerability repairs, and on how to improve future security works.

I.2 Demander

Before authorizing a service agency to carry out an evaluation on technical vulnerabilities, a demander should take seriously the agreement with the service agency. In the agreement, a demander should fully understand the characteristics of the evaluation and clarify its security control requirements and the technical limitations of the evaluation.

I.3 Security team

A security team should have the obligation of confidentiality in terms of the agreement with a service agency. Generally, no member of the security team should leak any information that could be exploited to damage the benefits or social image of a demander. The confidential information could include, but is not limited to the topology, the source code, the configuration file, the business data, the security strategies, etc.

A security team should submit a technical and verifiable vulnerability in which the detailed information of the vulnerability should include proofs and necessary descriptions, such as the vulnerability's name, type, hazard level, position, abstract, repair suggestion, etc.

When required by a service agency, any member of a security team should provide veridic information to identify and qualify themselves.

Bibliography

[b-ITU-T P.912]	Recommendation ITU-T P.912 (2016), *Subjective video quality assessment methods for recognition tasks*.
[b-ITU-T X.1500]	Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

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

Published in Switzerland
Geneva, 2023