International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1544

(04/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange –
Event/incident/heuristics exchange

Common attack pattern enumeration and classification

Recommendation ITU-T X.1544

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	**X.1540–X.1549**
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1544

Common attack pattern enumeration and classification

Summary

Recommendation ITU-T X.1544 is an XML/XSD-based specification for the identification, description, and enumeration of attack patterns. Attack patterns are a powerful mechanism to capture and communicate the attacker's perspective. They are descriptions of common methods for exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. The objective of the common attack pattern enumeration and classification (CAPEC) is to provide a publicly available catalogue of attack patterns along with a comprehensive schema and classification taxonomy.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1544	2013-04-26	17

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

Page

Introduction

The common attack pattern enumeration and classification (CAPEC) Recommendation is an XML/XSD-based specification for the identification, description and enumeration of attack patterns. Attack patterns are a powerful mechanism to capture and communicate the attacker's perspective. They are descriptions of common methods for exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. The objective of CAPEC is to provide a publicly available catalogue of attack patterns along with a comprehensive schema and classification taxonomy.

CAPEC enables:

- Standardizing the capture and description of attack patterns
- Collecting known attack patterns into an integrated enumeration that can be consistently and effectively leveraged by the community
- Classifying attack patterns so that users can easily identify the subset of the entire enumeration that is appropriate for their context
- Linking, through explicit references, the attack patterns and the common weakness enumerations (CWEs) that they are effective against.

Recommendation ITU-T X.1544 has been developed bearing in mind the importance of maintaining, to the extent possible, technical compatibility with *Requirements and Recommendation for CAPEC Compatibility*, version 1.0, published by the MITRE Corporation, dated 30 August 2012 (https://capec.mitre.org/compatible/requirements_v1.0.html).

Recommendation ITU-T X.1544

Common attack pattern enumeration and classification

1 Scope

This Recommendation provides for the structured exchange of publicly available attack patterns along with a comprehensive schema and classification taxonomy.

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.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange (CYBEX).*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 review authority [b-ITU-T X.1520]: An entity that performs a review.

NOTE – MITRE is the only review authority at this time.

3.1.2 vulnerability [ITU-T X.1500]: Any weakness in software 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 accuracy percentage: The percentage of security elements in the review sample that reference the correct CAPEC identifiers.

3.2.2 attack instance: A specific detailed attack against an application or system targeting vulnerabilities or weaknesses in that system.

3.2.3 attack pattern: An abstraction of common approaches of attack observed in the wild against applications or systems (e.g., SQL injection, man-in-the-middle, session hijacking).

NOTE – A single attack pattern may potentially have many varying attack instances associable with it.

3.2.4 capability: An assessment tool, dynamic application security testing (DAST) tool, penetration testing tool, exploit framework tool, threat modelling tool, database, website, advisory, or service that provides information about attack instances and patterns.

3.2.5 map/mapping: The specification of relationships between attack pattern elements in a repository and the CAPEC items that are related to those elements.

3.2.6 owner [based on b-ITU-T X.1520]: The custodian (real person or company) having responsibility for the capability (as defined in this Recommendation).

3.2.7 repository: An implicit or explicit collection of attack pattern elements that supports a capability, e.g., a database of attack patterns, the set of attack instances in a DAST tool, or a website.

3.2.8 review: The process of determining whether a capability is CAPEC-compatible.

3.2.9 review version: The dated version of CAPEC that is being used for determining CAPEC compatibility of a capability.

3.2.10 security element: A database record, assessment probe, attack instance, exploit, payload, etc., that is related to a specific attack pattern.

3.2.11 task: A tool's probe, check, signature, etc., that performs some action that produces security information (i.e., the security element).

3.2.12 tool: A software application or device that tests the security properties of an application or system through simulation, emulation or characterization of potential attacks against that system, e.g., an assessment tool, dynamic application security testing (DAST) tool, penetration testing tool, exploit framework tool, threat modelling tool.

3.2.13 user [based on b-ITU-T X.1520]: A consumer or potential consumer of the capability (as defined in this Recommendation).

3.2.14 weakness: A shortcoming or imperfection in the software code, design, architecture, or deployment that could, at some point, become a vulnerability or could contribute to the introduction of other vulnerabilities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CAPEC	Common Attack Pattern Enumeration and Classification
CCR	Coverage Claim Representation
CIA	Confidentially, Integrity or Availability
CWE	Common Weakness Enumeration
DAST	Dynamic Application Security testing Tool
GUI	Graphical User Interface
IDS	Intrusion Detection System
POC	Point Of Contact

5 Conventions

The keywords "required", "shall", "shall not", "should", "should not", "recommended", "may" and "optional" in this Recommendation are interpreted in accordance with the ITU-T Author's Guide (available at http://www.itu.int/oth/T0A0F000004/en).

6 High-level requirements

The following items define the concepts, roles and responsibilities related to the proper use of CAPEC identifiers to share data across separate security testing capabilities (tools, repositories and services) to allow these security testing capabilities to be used together, and to facilitate the comparison of security testing tools and services.

Prerequisites

6.1 The capability owner must be a valid legal entity, i.e., an organization or a specific individual, with a valid phone number, e-mail address and street mail address.

6.2 The capability must provide additional value or information beyond that which is provided in CAPEC itself (i.e., name, description, risks, references and associated weakness information).

6.3 The capability owner must provide the review authority with a technical point of contact who is qualified to answer questions related to the mapping accuracy and any CAPEC-related functionality of the capability.

6.4 The capability must be available to the public, or to a set of consumers, in a production or public version.

6.5 For CAPEC compatibility the capability owner must provide the review authority with a completed "CAPEC compatibility Requirements Evaluation Form".

6.6 The capability owner must provide the review authority with free access to the repository so that the review authority can determine that the repository satisfies all associated mapping accuracy requirements.

6.7 The capability owner must allow the review authority to use the repository to identify any attack pattern that should be added to CAPEC.

6.8 The capability owner must agree to abide by all of the mandatory CAPEC compatibility requirements, which includes the mandatory requirements for the specific type of capability.

Functionality

6.9 For CAPEC compatibility, the capability must allow users to locate security elements using CAPEC identifiers ("CAPEC-Searchable").

6.10 For CAPEC compatibility when the capability presents security elements to the user, it must allow the user to obtain the associated CAPEC identifiers ("CAPEC-Output").

6.11 For CAPEC compatibility, the capability's mapping must accurately link security elements to the appropriate CAPEC identifiers ("Mapping Accuracy").

6.12 For CAPEC compatibility, the capability's documentation must adequately describe CAPEC, CAPEC compatibility and how the CAPEC-related functionality in the capability is used ("CAPEC-Documentation").

6.13 For CAPEC compatibility, the capability's publicly available documentation must explicitly list the CAPEC identifiers that the capability owner considers the capability to cover as part of its functionality ("CAPEC-Coverage").

6.14 For CAPEC compatibility, the capability's publicly available web site should provide the capability's CAPEC coverage as a CAPEC Coverage Claim Representation (CCR) XML document(s).

6.15 The capability must denote the dated CAPEC version used ("Version Usage").

6.16 The capability must satisfy any additional requirements for the specific type of capability, as specified in Annex A.

6.17 The capability must satisfy all requirements for its distribution media, as specified in Annex B.

6.18 The capability is not required to do any of the following:

- use the same descriptions or references as CAPEC;
- include every CAPEC identifier in its repository.

Miscellaneous

6.19 If the capability does not satisfy all of the applicable requirements above (clauses 6.1 to 6.18), then the capability owner shall not advertise that it is CAPEC-compatible.

7 Accuracy

CAPEC compatibility only facilitates data sharing and correlation if the capability's mapping is accurate. Therefore, CAPEC-compatible capabilities must meet the following minimum accuracy requirements.

7.1 The repository must have an accuracy of 100 percent.

7.2 During the review period, the capability owner must correct any mapping errors found by the review authority.

7.3 After the review period, the capability owner should correct a mapping error within a reasonable time frame after the error was initially reported, i.e., within two (2) versions of the capability repository or six (6) months, whichever is shorter.

7.4 The capability owner should prepare and sign a statement that, to the best of the capability owner's knowledge, there are no errors in the mapping.

7.5 If the capability is based on, or uses, another CAPEC-compatible capability (the "source" capability), and the capability owner becomes aware of mapping errors in the source capability, then the capability owner must report those errors to the capability owner of the source capability.

8 Documentation

The following requirements apply to documentation that is provided with the capability.

8.1 The documentation must include a brief description of CAPEC and CAPEC compatibility, which can be based on verbatim portions of documents from the CAPEC Web site.

8.2 The documentation must describe how the user can find individual security elements in the capability's repository by using CAPEC identifiers.

8.3 The documentation must describe how the user can obtain CAPEC identifiers from individual elements in the capability's repository.

8.4 If the documentation includes an index, then it should include references to CAPEC-related documentation under the term "CAPEC".

9 CAPEC version usage

Users must know what version of CAPEC is used in a capability's repository with respect to its mapping to CAPEC. The capability owner can indicate the currency of a mapping by using the CAPEC version or date the mapping was updated.

9.1 The capability must identify the CAPEC version or update date that was used in creating or updating the mapping through at least one of the following: change logs, new feature lists, help files, or some other mechanism. The capability is "up-to-date" with respect to that version or update date.

9.2 Each new version of the capability should be up-to-date with respect to a CAPEC version that was released no more than four (4) months before the capability was made available to its users. If a capability does not satisfy this requirement, then it is "out-of-date."

9.3 The capability owner should publicize how quickly it will update the capability's repository after a new CAPEC version or update becomes available on the CAPEC website.

10 Revocation of CAPEC compatibility

10.1 If a review authority has verified that a capability is CAPEC-compatible, but at a later time the review authority has evidence that the requirements are not being met, then the review authority may revoke its approval.

10.1.1 The review authority must identify the specific requirements that are not being met.

10.2 The review authority must determine if the actions or claims of the capability owner are "intentionally misleading".

10.2.1 The review authority may interpret the phrase "intentionally misleading" at its discretion.

10.3 The review authority should not consider revoking CAPEC compatibility for a particular capability more often than once every six (6) months.

Warning and evaluation

10.4 The review authority must provide the capability owner and technical point of contact (POC) with a warning of revocation at least two (2) months before revocation is scheduled to occur.

10.4.1 If the review authority has found that the capability owner's actions or claims are intentionally misleading, then the review authority may disregard the warning period.

10.5 If the capability owner believes that the requirements are being met, then the capability owner may respond to the warning of revocation by providing specific details that indicate why the capability meets the requirements under question.

10.6 If the capability owner modifies the capability so that it complies with the requirements in question during the warning period, then the review authority should end the revocation action for the capability.

Revocation

10.7 The review authority may delay the date of revocation.

10.8 The review authority must publicize that CAPEC compatibility has been revoked for the capability.

10.9 If the review authority finds that the capability owner's actions with respect to CAPEC compatibility requirements are intentionally misleading, then revocation should last a minimum of one year.

10.10 The review authority may publicize the reason for revocation.

10.11 The capability owner may post a public statement regarding the revocation on the same site.

10.12 If the approval is revoked, the capability owner must NOT apply for a new review during the period of revocation.

11 Review authority

11.1 The review authority must review the capability for CAPEC compatibility with respect to a specific CAPEC version, i.e., the review version.

11.2 The review authority must clearly identify the review version that was used to determine compatibility for the capability.

11.3 The review authority must clearly identify the version of the CAPEC compatibility requirements document that was used to determine compatibility for the capability.

11.4 The review authority must review every element in the capability's repository for CAPEC mapping accuracy.

11.5 The review authority should review a capability for mapping accuracy at least once per year.

11.6 The review authority must provide a copy of the CAPEC compatibility declaration form upon request from any valid capability owner wishing to start the CAPEC-compatibility process.

11.7 The review authority must provide a copy of the CAPEC compatibility requirements evaluation form upon request from any capability owner that has submitted a completed CAPEC-compatibility declaration form.

Annex A

Type-specific requirements

(This annex forms an integral part of this Recommendation.)

Since a wide variety of capabilities uses CAPEC, certain types of capabilities may have unique features that require special attention with respect to CAPEC compatibility.

A.1 The capability must satisfy all additional requirements that are related to the specific type of capability.

A.1.1 If the capability is an assessment tool, dynamic application security testing (DAST) tool, penetration testing tool, exploit framework tool, threat modelling tool, or a product that integrates the results of one or more of these types of items, then it must satisfy the tool requirements, clauses A.2.1-A.2.8.

A.1.2 If the capability is a service (such as a security assessment service, a penetration testing service, or an education or training service) then it must satisfy the security service requirements, clauses A.3.1-A.3.5.

A.1.3 If the capability is an online database of known attacks, web-based resource, or information site, then it must satisfy the online capability requirements, clauses A.4.1-A.4.3.

A.2 Tool requirements

A.2.1 The tool must allow the user to use CAPEC identifiers to locate associated tasks in that tool ("CAPEC-searchable") by providing at least one of the following: a "find" or "search" function, a mapping between that tool's task names and CAPEC identifiers, or another mechanism determined to be sufficient by the review authority.

A.2.2 For any report that identifies individual security elements, the tool must allow the user to determine the associated CAPEC identifiers for those elements ("CAPEC-output") by doing at least one of the following: including CAPEC identifiers directly in the report, providing a mapping between the tool's task names and CAPEC identifiers, or using some other mechanism determined to be sufficient by the review authority.

A.2.3 The publicly available documentation must explicitly list the CAPEC identifiers that the capability owner considers the tool effective at instantiating ("CAPEC-Compatibility Claim Coverage").

A.2.4 The capability's publicly available website may provide the capability's CAPEC-Compatibility Claim Coverage as a CAPEC Coverage Claim Representation (CCR) XML document(s).

A.2.5 Any required reports or mappings must satisfy the media requirements as specified in Annex B.

A.2.6 The tool, or the capability owner, should provide the user with a list of all CAPEC identifiers that are associated with the tool's tasks.

A.2.7 The tool should allow the user to select a set of tasks by providing a file that contains a list of CAPEC identifiers.

A.2.8 The interface of the tool should allow the user to browse, select, and deselect a set of tasks by using individual CAPEC identifiers.

A.2.9 If the tool does not have a task that is associated with a CAPEC identifier as specified by the user in clause A.2.5 or clause A.2.6 tool requirements, then the tool should notify the user that it cannot perform the associated task.

A.3 Security service requirements

Security services might use CAPEC-compatible tools in their work, but they may not provide their customers with direct access to those tools. Thus it could be difficult for customers to identify and compare the capabilities of different services. The security service requirements address this potential limitation.

A.3.1 The security service must be able to use CAPEC identifiers to tell a user which security elements are tested or covered by the service offering ("CAPEC-searchable") by doing one or more of the following: providing the user with a list of CAPEC identifiers that identify the elements that are tested or covered by that service, providing the user with a mapping between the service's elements and CAPEC identifiers, responding to a user-supplied list of CAPEC identifiers by identifying which of the CAPEC identifiers are tested or covered by the service, or by using some other mechanism.

A.3.2 For any report that identifies individual security elements, the service must allow the user to determine the associated CAPEC identifiers for those elements ("CAPEC-Output") by doing one or more of the following: allowing the user to include CAPEC identifiers directly in the report, providing the user with a mapping between the security elements and CAPEC identifiers, or by using some other mechanism.

A.3.3 The publicly available documentation must explicitly list the CAPEC identifiers that the capability owner considers the Security Service to effectively cover in its offering ("CAPEC-Compatibility Claim Coverage").

A.3.4 The capability's publicly available web site may provide the capability's CAPEC-Compatibility Claim Coverage as (a) CAPEC Coverage Claim Representation (CCR) XML document(s).

A.3.5 Any required reports or mappings that are provided by the Service must satisfy the media requirements as specified in Annex B.

A.3.6 If the Service provides the user with direct access to a product that identifies security elements, then that product should be CAPEC-compatible.

A.4 Online capability requirements

A.4.1 The online capability must allow a user to find related security elements from the online capability's repository ("CAPEC-searchable") by providing one of the following: a search function that returns CAPEC identifiers for related elements, a mapping that links each element with its associated CAPEC identifier(s), or some other mechanism.

A.4.1.1 The online capability should provide a URL "template" that allows a computer program to easily construct a link that accesses the search function as outlined in clause A.4.1 online capability requirements .

Examples of constructing links:

http://www.example.com/cgi-bin/db-search.cgi?capecid=XXX
http://www.example.com/capec/xxx.html

A.4.1.2 If the site is publicly accessible without requiring login, then the CGI program should accept "GET" method.

A.4.2 For any report that identifies individual security elements, the online capability must allow the user to determine the associated CAPEC identifiers for those elements ("CAPEC-output") by doing at least one of the following: by allowing the user to include CAPEC identifiers directly in the report, providing the user with a mapping between the security elements and CAPEC identifiers, or by some other mechanism.

A.4.3 The publicly available documentation must explicitly list the CAPEC identifiers that the capability owner considers the online capability's repository to cover ("CAPEC-Compatibility Claim Coverage").

A.4.4 The capability's publicly available web site may provide the capability's CAPEC-Compatibility Claim Coverage as a CAPEC Coverage Claim Representation (CCR) XML document(s).

A.4.5 If the online capability does not provide details for individual security elements, then the online capability must provide a mapping that links each element with its associated CAPEC identifier(s).

Annex B

Media requirements

(This annex forms an integral part of this Recommendation.)

B.1 The distribution media that is used by a CAPEC-compatible capability must use a media format that is covered in this annex.

B.2 The media format must satisfy the specific requirements for that format.

B.3 Electronic documents (HTML, word processor, PDF, ASCII text, etc.)

B.3.1 The document must be in a commonly available format that has readers which support a "find" or "search" function ("CAPEC-searchable"), such as raw ASCII text, HTML, or PDF.

B.3.2 If the document only provides short names or titles for individual elements, then it must list the CAPEC identifiers that are related to those elements ("CAPEC-output").

B.3.3 The document should include a mapping from elements to CAPEC identifiers, which lists the appropriate pages for each element.

B.4 Graphical user interface

B.4.1 The graphical user interface (GUI) must provide the user with a search function that allows the user to enter a CAPEC identifier and retrieve the related elements ("CAPEC-searchable").

B.4.2 If the GUI lists details for an individual element, then it must list the CAPEC identifiers that map to that element ("CAPEC-output"). Otherwise, the GUI must provide the user with a mapping in a format that satisfies the electronic document requirements in clause B.3.1.

B.4.3 The GUI should allow the user to export or access CAPEC-related data in an alternate format that satisfies the electronic document requirements in clause B.3.1.

Bibliography

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2011), *Common vulnerabilities and exposures.*

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, 2013