International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1520

(01/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Vulnerability/state exchange

Common vulnerabilities and exposures

Recommendation ITU-T X.1520

ITU-T

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	**X.1520–X.1539**
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1520

Common vulnerabilities and exposures

Summary

Recommendation ITU-T X.1520 on the use of the common vulnerabilities and exposures (CVE) provides a structured means to exchange information security vulnerabilities and exposures, which provides common names for publicly known problems in the commercial or open source software used in communication networks, end-user devices or any of the other types of information and communication technology (ICT) capable of running software. The goal of the Recommendation is to define the use of CVE to make it easier to share data across separate vulnerability capabilities (tools, repositories and services) with this common naming. This Recommendation defines the use of CVE to provide a mechanism for vulnerability databases and other capabilities to be used together, and to facilitate the comparison of security tools and services. CVE does not contain information such as risk, impact, fix information or detailed technical information. CVE only contains the standard identifier number with status indicator, a brief description and references to related vulnerability reports and advisories. The repository of CVE identifiers is available at cve.mitre.org/cve/cve.html.

The intention of CVE, the use of which is defined in this Recommendation, is to be comprehensive with respect to all publicly known vulnerabilities and exposures. While CVE is designed to contain mature information, the primary focus is on identifying vulnerabilities and exposures that are detected by security tools and any new problems that become public, and then addressing any older security problems that require validation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1520	2011-04-20	17	11.1002/1000/11061
2.0	ITU-T X.1520	2014-01-24	17	11.1002/1000/12040

* 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

This Recommendation on the use of the common vulnerabilities and exposures (CVE) provides a structured means to exchange information security vulnerabilities and exposures, which provides common names for publicly known problems. The goal of this Recommendation is to define use of CVE to make it easier to share data across separate vulnerability capabilities (tools, repositories and services) with this common naming. This Recommendation is designed to allow vulnerability databases and other capabilities to be used together, and to facilitate the comparison of security tools and services. CVE does not contain information such as risk, impact, fix information or detailed technical information. CVE only contains the standard identifier number with status indicator, a brief description and references to related vulnerability reports and advisories. The repository of CVE identifiers is available at http://cve.mitre.org/cve/cve.html.

The intention of CVE, the use of which is defined in this Recommendation, is to be comprehensive with respect to all publicly known vulnerabilities and exposures. While CVE is designed to contain mature information, the primary focus is on identifying vulnerabilities and exposures that are detected by security tools and any new problems that become public, and then addressing any older security problems that require validation.

This Recommendation is one of a class of ITU-T Recommendations that comes from a large, existing, global development and user community that has written and evolved an open specification that is made available to the ITU-T for adoption, with agreement that any changes or updates to the specification will be done in a manner that ensures full technical equivalency and compatibility will be maintained, that discussions about changes and enhancements will be done through the original user community, and includes explicit reference to the corresponding specific version maintained by the user community.

Recommendation ITU-T X.1520

Common vulnerabilities and exposures

1 Scope

This Recommendation on the use of the common vulnerabilities and exposures provides a "structured means" for the global exchange of publicly known, mature vulnerabilities and exposures information that are detected by security tools or otherwise become public. This "structured means" is often referred to as "CVE compatibility" and defines the correct use of CVE. An information security vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network. An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network. The assignment of CVE identifiers is not within the scope of this Recommendation.

Recommendation ITU-T X.1520 has been developed on a collaborative basis with the MITRE Corporation, bearing in mind the importance of maintaining, to the extent possible, technical compatibility between Recommendation ITU-T X.1520 and the "Requirements and Recommendations for CVE Compatibility", 30 June 2013, available at https://cve.mitre.org/compatible/Requirements_for_CVE_Compatibility_V1.3.pdf.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

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 CVE identifiers.

3.2.2 capability: Security tool, database, website, advisory or service that provides a security vulnerability or exposure identification function.

3.2.3 exposure: An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

3.2.4 map/mapping: The specification of relationships between security elements in a repository and the CVE names that are related to those elements.

3.2.5 owner: The custodian (real person or company) having responsibility for the capability.

3.2.6 repository: An implicit or explicit collection of security elements that supports a capability, e.g., a vulnerability database, advisory archive, the set of signatures in an intrusion detection system (IDS) or website.

3.2.7 review: The process of determining whether a capability is CVE-compatible.

3.2.8 review authority: Any entity that performs a review.

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

3.2.9 review date: The date of the CVE content that is being used for determining CVE compatibility of a capability.

3.2.10 review sample: The set of security elements in the capability's repository that is used by the review authority for evaluating accuracy.

3.2.11 sampling method: The method by which the review authority identifies the set of security elements in the review sample.

3.2.12 sample size: The percentage and/or the number of security elements to be examined by the review authority.

3.2.13 security element: A database record, e-mail message, security advisory, assessment probe, signature, etc., which is related to a specific vulnerability or exposure.

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

3.2.15 tool: A software application or device that either examines a host or network and produces information that is related to vulnerabilities or exposures or aggregates this type of information, e.g., a vulnerability scanner, intrusion detection system, risk management, security information management or compliance reporting tool or service.

3.2.16 user: A consumer or potential consumer of the capability.

3.2.17 vulnerability: Any weakness in software that could be exploited to violate a system or the information it contains (based upon [b-ITU-T X.1500]).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASCII American Standard Code for Information Interchange

CVE Common Vulnerabilities and Exposures

GUI Graphical User Interface

HTML HyperText Markup Language

HTTP HyperText Transfer Protocol

IDS Intrusion Detection System

PDF Portable Document Format

POC Point Of Contact

URL Uniform Resource Locator

XML Extensible Markup Language

5 Conventions

CVE is used as a noun in this Recommendation.

6 High-level requirements

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

Prerequisites

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

6.2 The capability shall provide additional value or information beyond that which is provided in CVE itself (i.e., name, description, references and associated data).

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

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

6.5 The capability owner shall provide the review authority with a completed "CVE compatibility requirements evaluation form".

6.6 For a capability with a repository, the capability owner shall provide the review authority with free access to the repository so that the authority can determine that the repository satisfies all associated requirements.

6.7 For a capability with a repository, the capability owner shall allow the review authority to use the repository to identify any vulnerabilities that should be added to CVE.

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

Functionality

6.9 The capability shall allow users to locate security elements using CVE names ("CVE-searchable").

6.10 When the capability presents security elements to the user, it shall allow the user to obtain the associated CVE names ("CVE-output").

6.11 For a capability with a repository, the capability's mapping shall accurately link security elements to the appropriate CVE names ("mapping accuracy").

6.12 The capability's documentation shall adequately describe CVE, CVE compatibility and how the CVE-related functionality in the capability is used ("CVE-documentation").

6.13 The capability shall state the date of its currency with respect to CVE ("date usage").

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

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

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

- use the same descriptions or references as CVE;
- include every CVE name in its repository.

Miscellaneous

6.17 If the capability does not satisfy all of the applicable requirements above (6.1 through 6.16), then the capability owner shall not advertise that it is CVE-compatible.

7 Accuracy

CVE compatibility only facilitates data sharing if the capability's mapping is accurate. Therefore, CVE-compatible capabilities have to meet the minimum accuracy requirements described below.

7.1 For a capability with a repository, the repository shall have an accuracy percentage of 90 per cent or greater.

7.2 During the review period, the capability owner shall 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 repository or six (6) months for tools and three (3) months for online capabilities and services.

7.4 For a capability with a repository, 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 CVE-compatible capability (the "source" capability), and the capability owner becomes aware of mapping errors in the source capability, then the capability owner shall report those errors to the owner of the source capability.

7.6 The mapping accuracy for advisory archives shall be performed against all of the security elements of the archive repository subsequent to, and including, the archive's first use of a CVE name in a security element.

7.7 A capability shall accurately reflect the status of deprecated CVE names within three (3) months for online capabilities and services.

7.8 A capability shall not output deprecated CVE IDs when more appropriate IDs are specified within the description of the deprecated CVE ID, within three (3) months of the CVE ID being deprecated.

8 Documentation

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

8.1 The documentation shall include a brief description of CVE and CVE compatibility, which can be based on verbatim portions of documents from the CVE website.

8.2 The documentation shall describe how the user can find individual security elements in the capability's repository by using CVE names.

8.3 The documentation shall describe how the user can obtain CVE names from individual elements in the capability's repository.

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

9 CVE date usage

Users must be able to determine how "up-to-date" a capability's repository is with respect to its mapping to CVE. The capability owner needs to indicate the currency of a mapping by providing the date of its last update of CVE information and indicate what portion of CVE content they utilize and from where they gathered the CVE content.

9.1 Each new version of the capability shall identify the most recent date of CVE content 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 date.

9.2 Each new version of the capability shall be up to date with respect to a stated CVE date that is no more than three (3) months before the capability was made available to its users. If a capability does not satisfy this requirement, then it is by definition defined as being "out-of-date".

9.3 The capability owner shall publicize how quickly it will update the capability's repository to include new CVE information.

9.4 The capability owner shall describe the criteria and mechanism for selecting the CVE information they include in their capability.

9.5 The capability owner shall describe from where it gathers new CVE content.

10 Different styles of CVE name support

A capability shall function with CVE names independent of the format of the CVE name's representation in the capability, whether it is using the older style four-digit CVE-ID syntax or the variable-length (four digits or more) CVE-ID syntax (used after the CVE-ID syntax modification in use after 30 December 2013).

10.1 If a user performs a search using YYYY-NNNN, YYYY-NNNNN, YYYY-NNNNNN or other valid IDs with a larger number of digits, the capability shall return the security elements that correspond to CVE-YYYY-NNNN, CVE-YYYY-NNNNN, CVE-YYYY-NNNNNN or other valid IDs with a larger number of digits, respectively, regardless of whether the CVE name has a CVE or a CAN as part of its name, within the capability's repository.

10.2 If the capability contains the CVE name CVE-YYYY-NNNN, but the user searches using the old format for a CVE name, CAN-YYYY-NNNN (used before the CVE naming scheme modification introduced on 19 October 2005), then the capability should return CVE-YYYY-NNNN.

11 Revocation of CVE compatibility

11.1 If a review authority has verified that a capability is CVE-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.

11.1.1 The review authority shall identify the specific requirements that are not being met.

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

11.2.1 The review authority may interpret the phrase "intentionally misleading" as it wishes.

11.3 Unless recommended by two CVE editorial board members who do not have a conflict of interest, the review authority should not consider revoking CVE compatibility for a particular capability more often than once every six (6) months.

Warning and evaluation

11.4 The review authority shall 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.

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

11.5 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.

11.6 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

11.7 The review authority may delay the date of revocation.

11.8 The review authority shall publicize that CVE compatibility has been revoked for the capability.

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

11.10 The review authority may publicize the reason for revocation.

11.11 If the approval is revoked, the capability owner shall not apply for a new review during the period of revocation.

12 Review authority

For any review conducted by the review authority:

12.1 The review authority shall review the capability for CVE compatibility with respect to a specific CVE content date, i.e., the review date.

12.2 The review authority shall clearly identify the review date that was used to determine compatibility for the capability.

12.3 The review authority shall clearly identify the version of the CVE compatibility requirements document that was used to determine compatibility for the capability.

12.4 The review authority shall define and publish a sample size.

12.4.1 The review authority should use a sample size of 50 elements plus 5 per cent of the capability's repository, up to a maximum sample size of 400 elements.

12.4.2 The review authority may review every element in the capability's repository.

12.5 The review authority shall publicize the sampling method.

12.6 The review authority may use a review sample that was not randomly selected.

12.7 The review authority shall use the same sampling method and sample size for all capabilities that are evaluated within the same time-frame.

Annex A

Type-specific requirements

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

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

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

A.1.1 If the capability is a vulnerability assessment scanner, intrusion detection system (IDS) or a product which integrates the results of one or more scanners and IDSs, then it shall satisfy the tool requirements, A.2.1-A.2.8.

A.1.2 If the capability is a service (such as a managed intrusion detection and response service, or a remote scanning service), then it shall satisfy the security service requirements, A.3.1-A.3.5.

A.1.3 If the capability is an online vulnerability or signature database, web-based archive or maintenance/patch site, then it shall satisfy the online capability requirements, A.4.1-A.4.3.

A.1.4 If the capability is an aggregation tool like a security information manager, a compliance reporting tool or a service supplying these types of aggregations of vulnerability type information, then it shall satisfy the aggregation capability requirements, A.5.1-A.5.6.

Tool requirements

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

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

A.2.3 Any required reports or mappings shall satisfy the media requirements as specified in Annex B.

A.2.4 The tool, or the capability owner, should provide the user with a list of all CVE names that are associated with the tool's tasks.

A.2.5 The tool should allow the user to select a set of tasks by providing a file that contains a list of CVE names.

A.2.6 The interface of the tool should allow the user to browse, select and deselect a set of tasks by using individual CVE names.

A.2.7 If the tool does not have a task that is associated with a CVE name as specified by the user in the A.2.5 or A.2.6 tool requirements, then the tool should notify the user that it cannot perform the associated task.

A.2.8 The capability owner shall warrant that (1) the rate of false positives is less than 100 per cent, i.e., if the tool reports a specific security element, it is at least sometimes correct, and (2) the rate of false negatives is less than 100 per cent, i.e., if an event occurs that is related to a specific security element, then sometimes the tool reports that event.

Security service requirements

Security services might use CVE-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 shall be able to use CVE names to tell a user which security elements are tested or detected by the service ("CVE-searchable") by doing one or more of the following: providing the user with a list of CVE names that identify the elements that are tested or detected by that service, providing the user with a mapping between the service's elements and CVE names, responding to a user-supplied list of CVE names by identifying which of the CVE names are tested or detected by the service or by using some other mechanism.

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

A.3.3 Any required reports or mappings that are provided by the service shall satisfy the media requirements as specified in Annex B.

A.3.4 If the service provides the user with direct access to a product that identifies security elements, then that product should be CVE-compatible.

A.3.5 The capability owner shall warrant that (1) the rate of false positives is less than 100 per cent, i.e., if a tool reports a specific security element, it is at least sometimes correct, and (2) the rate of false negatives is less than 100 per cent, i.e., if an event occurs that is related to a specific security element, then sometimes the service reports that event.

Online capability requirements

A.4.1 The online capability shall allow a user to find related security elements from the online capability's repository ("CVE-searchable") by providing one of the following: a search function which returns CVE names for related elements, a mapping that links each element with its associated CVE name(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 under online capability requirements.

Examples:
```
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNN
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNNN
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNNNN
http://www.example.com/cve/CVE-YYYY-NNNN.html
http://www.example.com/cve/CVE-YYYY-NNNNN.html
http://www.example.com/cve/CVE-YYYY-NNNNNN.html
```

A.4.1.2 If the URL template is for a CGI program, the program should accept the HTTP "GET" method.

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

A.4.3 If the online capability does not provide details for individual security elements, then the online capability shall provide a mapping that links each element with its associated CVE name(s).

Aggregation capability requirements

A.5.1 The aggregation capability shall allow the user to use CVE names to locate associated elements in that capability ("CVE-searchable") by providing at least one of the following: a "find" or "search" function, a mapping between that capability's names and CVE names or another mechanism with the approval of the review authority.

A.5.2 For any report that identifies individual security elements, the aggregation capability shall allow the user to determine the associated CVE names for those elements ("CVE-output") by doing at least one of the following: including CVE names directly in the report, providing a mapping between the capability's names and CVE names or using some other mechanism.

A.5.3 Any required reports or mappings shall satisfy the media requirements as specified in Annex B.

A.5.4 The tool, or the capability owner, should provide the user with a list of all CVE names that are associated with the tool's tasks.

A.5.5 The tool should allow the user to select a set of tasks by providing a file that contains a list of CVE names.

A.5.6 The interface of the tool should allow the user to browse, select and deselect a set of tasks by using individual CVE names.

Annex B

Media requirements

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

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

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

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

B.3.1 The document shall be in a commonly available format that has readers which support a "find" or "search" function ("CVE-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 shall list the CVE names that are related to those elements ("CVE-output").

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

Graphical user interface (GUI)

B.4.1 The GUI shall provide the user with a search function that allows the user to enter a CVE name and retrieve the related elements ("CVE-searchable").

B.4.2 If the GUI lists details for an individual element, then it shall list the CVE name (or names) that map to that element ("CVE-output"). Otherwise, the GUI shall provide the user with a mapping in a format that satisfies the B.3.1 electronic documents requirement.

B.4.3 The GUI should allow the user to export or access CVE-related data in an alternate format that satisfies the B.3.1 electronic documents requirement.

Annex C

Media requirements

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

The CVE XML schema included in this annex is available at http://cve.mitre.org/schema/cve/cve_1.0.xsd and replicated below.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns="http://cve.mitre.org/cve/downloads/1.0"
    targetNamespace="http://cve.mitre.org/cve/downloads/1.0"
    elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">

  <!--  ********************************************************************** -->
  <!--  Changelog: 1.0 - Initial version -->
  <!--  ********************************************************************** -->
  <xsd:annotation>
    <xsd:documentation xml:lang="en">
      Simple schema that defines the format of the CVE List provided by MITRE
    </xsd:documentation>
  </xsd:annotation>

  <!--  ********************************************************************** -->
  <!--  Start Item Element Definition -->
  <!--  ********************************************************************** -->
  <xsd:element name="cve">
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        cve is the top level element of the CVE List provided by MITRE.
        It represents holds all CVE Items.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="item" type="ItemType" minOccurs="1" maxOccurs="unbounded"/>
      </xsd:sequence>
      <xsd:attribute name="schemaVersion" type="xsd:token" use="optional"/>
    </xsd:complexType>
  </xsd:element>

  <!--  ********************************************************************** -->
  <!--  Simple Types -->
  <!--  ********************************************************************** -->
  <!-- CUSTOM TYPE DEFINITIONS-->
  <xsd:simpleType name="typeEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="CAN"/>
      <xsd:enumeration value="CVE"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="statusEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Entry"/>
      <xsd:enumeration value="Candidate"/>
    </xsd:restriction>
  </xsd:simpleType>

  <!-- need to verify enumeration -->
  <xsd:simpleType name="simplePhaseEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Proposed"/>
      <xsd:enumeration value="Interim"/>
      <xsd:enumeration value="Modified"/>
      <xsd:enumeration value="Assigned"/>
```

```
  </xsd:restriction>
</xsd:simpleType>

<!--  ********************************************************************** -->
<!--  Complex Types -->
<!--  ********************************************************************** -->
<xsd:complexType name="ItemType">
  <xsd:sequence>
    <xsd:element name="status" type="statusEnumType" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="phase" type="specificPhaseType" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="desc" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="refs" type="refsType" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="votes" type="votesType" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="comments" type="commentsType" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
  <!--Need to Verify Enumeration-->
  <xsd:attribute name="type" type="typeEnumType" use="required"/>
  <xsd:attribute name="name" type="xsd:token" use="required"/>
  <xsd:attribute name="seq" type="xsd:token" use="required"/>
</xsd:complexType>

<xsd:complexType name="commentsType">
  <xsd:sequence>
    <xsd:element name="comment" minOccurs="0" maxOccurs="unbounded">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="voter" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="votesType">
  <xsd:sequence>
    <xsd:element name="accept" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="modify" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="noop" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="recast" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
```

```
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="reject" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="reviewing" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="revote" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="specificPhaseType">
    <xsd:simpleContent>
      <xsd:extension base="simplePhaseEnumType">
        <xsd:attribute name="date" type="xsd:token" use="optional"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>

  <xsd:complexType name="refsType">
    <xsd:annotation>
      <xsd:documentation>holds all hyperlink elements</xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
      <xsd:element name="ref" type="refType" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="refType">
    <xsd:annotation>
      <xsd:documentation>Holds individual hyperlink element</xsd:documentation>
    </xsd:annotation>
    <xsd:simpleContent>
      <xsd:extension base="xsd:string">
        <xsd:attribute name="source" type="xsd:token" use="required"/>
        <xsd:attribute name="url" type="xsd:anyURI" use="optional"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>
</xsd:schema>
```

Bibliography

[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	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, 2014