

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1570

(09/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Identification and
discovery

**Discovery mechanisms in the exchange of
cybersecurity information**

Recommendation ITU-T X.1570



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.1570

Discovery mechanisms in the exchange of cybersecurity information

Summary

Recommendation ITU-T X.1570 provides a framework for discovering cybersecurity information and the mechanism that enables this. Discovery can be seen as a stage of the cybersecurity information lifecycle adjacent to information publishing and acquisition, which are integral and necessary stages for discovery. Thus, the framework covers how to publish cybersecurity information, obtain the candidate list, and acquire the needed information. A discovery scheme may be implemented with arbitrary mechanisms so long as they comply with the framework. Among these mechanisms are object identifier (OID)-based discovery and resource description framework (RDF)-based discovery, which are also elaborated in this Recommendation.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1570	2011-09-02	17

Keywords

Cybersecurity information, information discovery, source discovery.

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/>.

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	1
4 Abbreviations and acronyms	2
5 Conventions	2
6 Framework to identify and locate the source of cybersecurity information.....	3
7 Types and level of details of discovered cybersecurity information	3
8 Cybersecurity information identifier	4
9 Types of discovery mechanisms	5
9.1 OID-based discovery mechanisms in the exchange of cybersecurity information	5
9.2 RDF-based discovery mechanisms in cybersecurity information exchange..	6
10 Methods available for access to discovered information.....	7
Appendix I – Cybersecurity operational information ontology	8
I.1 Cybersecurity operation domains	8
I.2 Roles	8
I.3 Cybersecurity information.....	9
Appendix II – Specifications describing databases and knowledge bases.....	12
Appendix III – An illustrated implementation of RDF-based discovery	13
III.1 RDF-based discovery implementation example.....	13
III.2 Class hierarchy of cybersecurity information.....	13
Bibliography.....	15

Introduction

Greater importance than ever is being placed on the exchange of cybersecurity information. An international standard for exchanging cybersecurity information, called CYBEX, is drawing particularly significant attention. CYBEX discovery, which provides a scheme for finding the source of cybersecurity information, is among CYBEX's various technical specifications. This Recommendation explains its framework and techniques.

Recommendation ITU-T X.1570

Discovery mechanisms in the exchange of cybersecurity information

1 Scope

This Recommendation provides a framework for discovering cybersecurity information and the mechanism that enables this. Discovery can be seen as a stage of the cybersecurity information lifecycle adjacent to information publishing and acquisition, which are integral and necessary stages for discovery. Thus, the framework covers how to publish cybersecurity information, obtain the candidate list, and acquire the needed information. A discovery scheme may be implemented with arbitrary mechanisms so long as they comply with the framework. Among these mechanisms are object identifier (OID)-based discovery and resource description framework (RDF)-based discovery, which are also elaborated on in this Recommendation.

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.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree.*

[W3C RDF] W3C Recommendation (2004), *Resource Description Framework (RDF): Concepts and Abstract Syntax.*
<<http://www.w3.org/TR/rdf-concepts/>>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 object identifier [ITU-T X.660]: An ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node.

3.1.2 ontology [b-Gruber]: An explicit specification of a conceptualization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cybersecurity information: Structured information or knowledge concerning:

1. the "state" of equipment, software or network-based systems as related to cybersecurity, especially vulnerabilities;
2. forensics related to incidents or events;
3. heuristics and signatures gained from experienced events;

4. parties who implement cybersecurity information exchange capabilities within the scope of this framework;
5. specifications for the exchange of cybersecurity information, including modules, schemas, policies and assigned numbers;
6. the identities and trust attributes of all of the above;
7. implementation requirements, guidelines and practices.

NOTE – This definition is based on the description given for cybersecurity information in [b-ITU-T X.1500].

3.2.2 exchange (cybersecurity information): The transfer of cybersecurity information between two or more cybersecurity entities. This transfer may be uni-directional, bi-directional, or multi-directional, i.e., many-to-many.

3.2.3 discovery: The act or process of discovering the target, i.e., obtaining knowledge of the target for the first time.

3.2.4 retriever: An entity retrieving cybersecurity information.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CCE	Common Configuration Enumeration
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
CYBEX	CYBersecurity information EXchange
HTTP	Hypertext Transfer Protocol
IODEF	Incident Object Description Exchange Format
MAEC	Malware Attribute Enumeration and Characterization
OID	Object Identifier
OVAL	Open Vulnerability and Assessment Language
RDF	Resource Description Framework
SCAP	Security Content Automation Protocol
SNMP	Simple Network Management Protocol
XCCDF	eXtensible Configuration Checklist Description Format

5 Conventions

None.

6 Framework to identify and locate the source of cybersecurity information

Different cybersecurity organizations are implementing common cybersecurity protocols for the capture and exchange of information on the system state, vulnerability, incident forensics, and incident heuristics, in operational applications. As this information is becoming available from many different sources, implementers should harmonize how they identify cybersecurity organizations, trust and information exchange policies, and the information itself that is exchanged or distributed. To address this issue, this clause introduces a framework to identify and locate the source of cybersecurity information – the cybersecurity information discovery framework.

Finding cybersecurity information involves three entities: retriever, source, and directory. The retriever retrieves the information by sending a request, the source provides requested information, and the directory registers the metadata of the source's information and assists the retriever in finding a proper source.

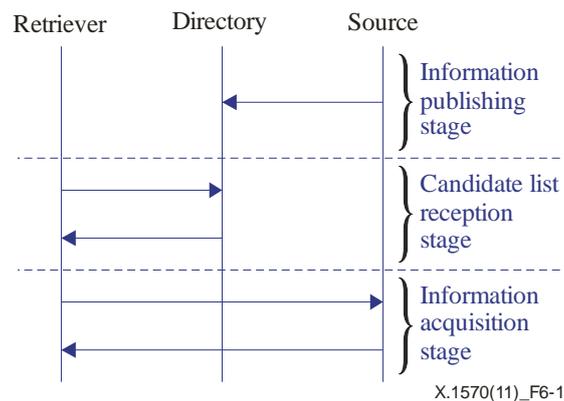
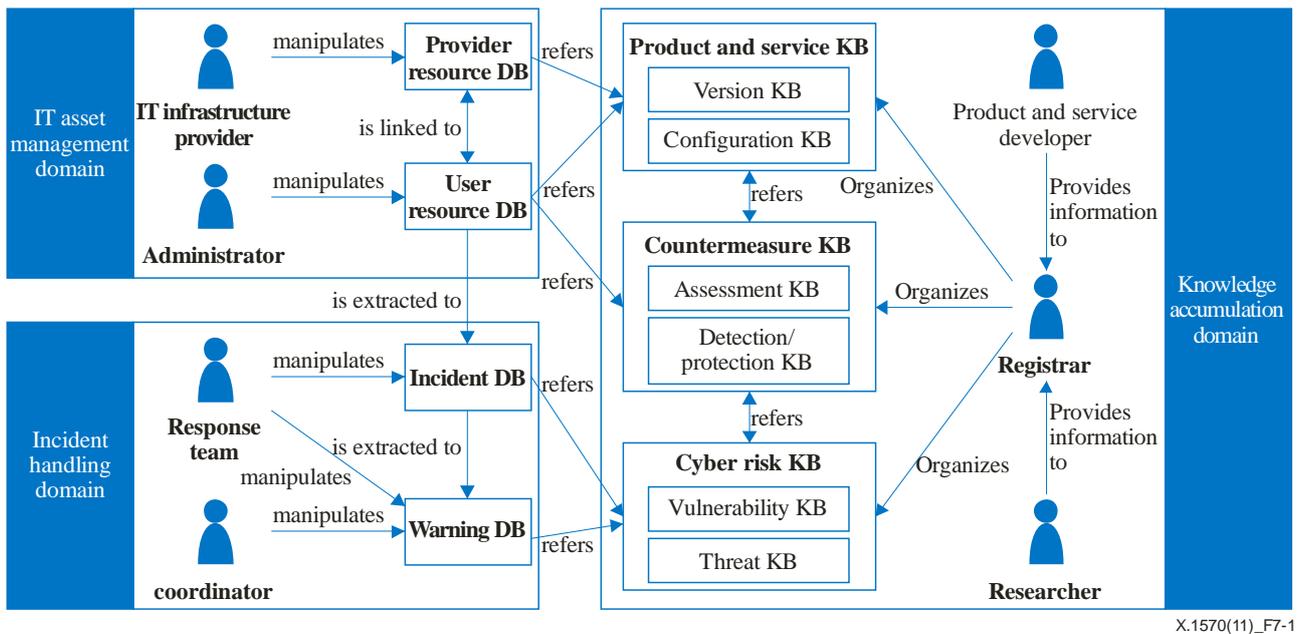


Figure 6-1 – Three stages of discovery

The discovery process is the communication process of the three entities, as depicted in Figure 6-1. It has three stages: information publishing, candidate list reception, and information acquisition. The source publishes its information for the cyber society by registering it with the directory at the information publishing stage. The retriever queries a registrar directory for the list of candidate sources at the candidate list reception stage. It then selects a source that seems best suited from the list and receives the source's information at the source selection stage.

7 Types and level of details of discovered cybersecurity information

The discovery mechanisms are able to discover cybersecurity information. This mechanism intends to discover the following seven types of information: user resource database; provider resource database; incident database; warning database; product and service knowledge base; cyber risk knowledge base; and countermeasure knowledge base. Figure 7-1 provides the ontology model used in this Recommendation and shows the relationship between the information types used in this model.



X.1570(11)_F7-1

DB: Database KB: Knowledge base

Figure 7-1 – Cybersecurity operational information ontology

This ontology is a model for describing the acquisition, accumulation and use of cybersecurity information knowledge that consists of a set of operation domains, roles, and information types. The roles, described with human icons in the figure, are generic and entities such as CIRTs may encompass one or more of these functions. This model is used to define domains for cybersecurity operations, and is then used to identify required cybersecurity entities to support the operations in each domain. The details of the ontology are described in Appendix I.

Table II.1 shows cybersecurity specifications which are consistent with the seven types of information described in this ontology model. The level of detail of discovered cybersecurity information will follow the level of detail of the standards. Using this approach, the level of detail is flexible and thus various standards could be built for specific purposes.

8 Cybersecurity information identifier

A unique identifier is needed to identify cybersecurity information. Any globally unique identifier used for global cybersecurity information exchange shall have the following characteristics:

- simplicity, usability, flexibility, extensibility, scalability, and deployability
- distributed management of diverse identifier schemes
- long-term reliability of identifier registrars, and the availability of high-performance tools for discovering information associated with any given identifier.

Two unique identifier candidates fulfil the requirements mentioned above: the object identifier (OID) and the resource description framework (RDF). These represent two primary paradigms for common service and information discovery, as discussed in clause 9.

9 Types of discovery mechanisms

Discovery schemes may be implemented with arbitrary mechanisms so long as they comply with the framework. They are classified into two types – centralized and decentralized – from the standpoint of how they register and manage cybersecurity information registries.

In the case of a centralized mechanism, directories manage one or more "central" registries, which enable easy location and quick discovery of targeted information (the candidate list reception stage may be omitted in some cases). The searching party, however, needs to first know of the existence of a given registry before it can use it. The varied resources and costs involved in maintaining a central repository can also make it prohibitive for those with limited resources. OID-based discovery is a typical mechanism here.

In the case of a decentralized mechanism, directories manage multiple "distributed" registries. This enjoys minimal resources and costs associated with making information available, and those providing and seeking information need not know of each other's existence beforehand. Yet, in order to find information starting from zero knowledge, the searcher literally needs to crawl the entire Internet. RDF-based discovery is a typical mechanism here.

9.1 OID-based discovery mechanisms in the exchange of cybersecurity information

An OID-based discovery mechanism identifies and locates sources of cybersecurity information using OIDs, within a hierarchical tree structure whose leaves identify objects. OIDs build hierarchical naming, i.e., concatenations of values of arcs starting from the root of the tree and proceeding to one of its leaves. Registered cybersecurity information is reachable by following the tree from its root to one of the leaves. Note that cybersecurity information is registered under the object identifier arc for cybersecurity information exchange {joint-iso-itu-t(2) cybersecurity(48)} [b-ITU-T X.1500.1].

The discovery stages introduced in clause 6 are detailed in clauses 9.1.1 to 9.1.3.

9.1.1 Information publishing stage

When registering information, a source provides multiple types of metadata information, among which the major categories are: country/region, organization ID, information type, and information description format. Country/region specifies the organization's country, or organization's region if the source is a cross-national organization such as ITU. The organization ID specifies the organization and can be described by, for instance, using a stock ticker number or unique corporate name. Information type specifies the type of information described in clause 7. The information description format specifies the format, such as CVE-compatible [b-ITU-T X.1520] or ARF-compatible [b-ARF].

Upon receiving the registration request from the source, the directory registers and stores information based on the metadata and constructs OID subtrees. Although this Recommendation does not specify any normative structure for the tree, some candidates are described in the Appendices I and II.

9.1.2 Candidate list reception stage

The retriever does not necessarily send a query to the directory that has the single consistent registry of the OID tree. It can know the structure of the tree beforehand, and by following it, may identify the needed information without sending a query.

The directory may accept an arbitrary query (including text search query) and reply with a candidate list.

9.1.3 Information acquisition stage

Based on the candidate list or following the OID tree from the root to a leaf, a retriever chooses one source, and then sends a request to the source, which in return provides cybersecurity information.

For OID-based discovery, the candidate list reception and information acquisition stages could be called inseparable, since narrowing down the candidate by following the tree leads to selection of a single source.

9.2 RDF-based discovery mechanisms in cybersecurity information exchange

An RDF-based discovery mechanism identifies and locates sources of cybersecurity information based on RDF. Figure 9-1 describes the concept of this mechanism. The source may register itself to one or more directories (containing registries), which facilitate retrievers so that they can retrieve the information. Information on identities and capabilities of cybersecurity entities are exchanged among the entities during the discovery process. Cybersecurity entities send discovery requests to a directory, each of which has different sources, which become the range of the search for the search engine.

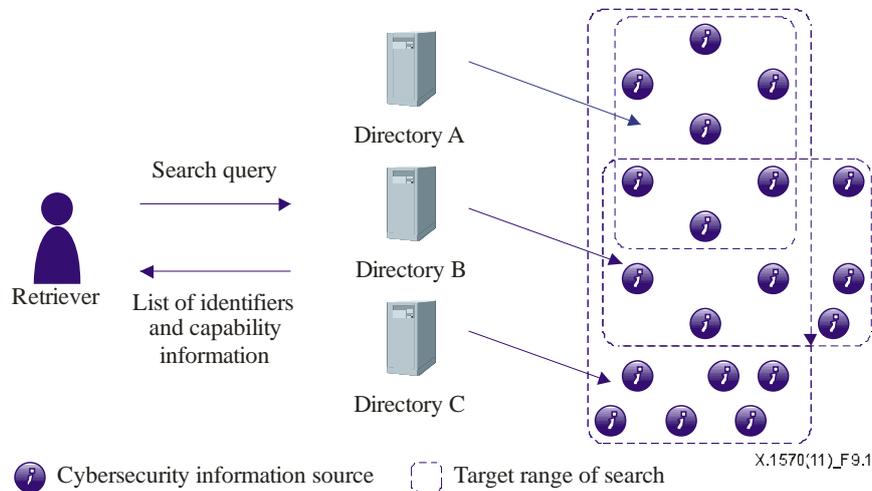


Figure 9-1 – Concept of RDF-based discovery

Different from OID-based discovery, RDF-based discovery has directories consisting of multiple entities, see Figure 9-2. From a functional standpoint, a directory consists of a discovery agent and registry agent. The discovery agent communicates with the retriever (an interface for the receiver), and the registry agent communicates with the source (an interface for the source). The discovery agent and registry agent may in some cases reside inside one computer. Capability and identifier information is exchanged among the four entities.

The discovery stages introduced in clause 6 are detailed in clauses 9.2.1 to 9.2.3.

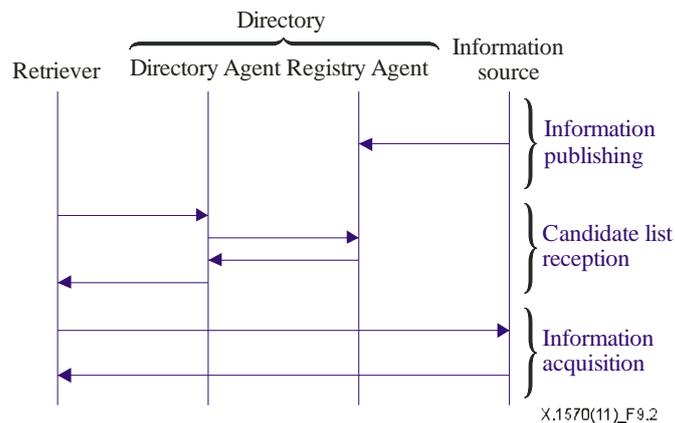


Figure 9-2 – Sequence diagram of RDF-based discovery

9.2.1 Information publishing stage

A source registers its information with a registry agent, which generates and arranges suitable metadata for the data at the information publishing stage. As with OID-based discovery, the source provides multiple types of metadata information when registering cybersecurity information, among which the major categories are: country/region, organization ID, information type, and information description format. Country/region specifies the organization's country, or organization's region if the source is a cross-national organization such as ITU. The organization ID specifies the organization and can be described by, for instance, using the stock ticker number or unique corporate name. The information type specifies the type of information described in clause 7. The information description format specifies the format, such as CVE-compatible or ARF-compatible.

Upon receiving the registration request from the source, the directory registers and stores information based on the metadata and updates the RDF database. Since registry agents often use hierarchically distributed registries, the registry agent needs to identify in which registry the data needs to be stored.

Though this Recommendation does not specify a normative structure for the RDF metadata format, some candidates are described in the Appendices I and II.

9.2.2 Candidate list reception stage

The retriever sends queries to a discovery agent, which forwards them to one or more suitable registry agents, which retrieve their metadata database and reply with a list of candidate sources at the candidate list reception stage. The discovery agent aggregates the information received from multiple-registry agents and sends it to the retriever.

9.2.3 Information acquisition stage

The retriever selects the best-suited source from the list at the information acquisition stage.

10 Methods available for access to discovered information

Various communication protocols can be used to exchange cybersecurity information including HTTP (which uses RDF) and SNMP (which uses OID).

Some parties may wish to limit parties who can access discovered information by establishing access control policies. Major criteria of the policies include the IP address, domain, communication protocol, ID and password, and identification certificate.

Any party seeking cybersecurity information exchanges various messages, including request messages. These methods will be defined in the ITU-T X.1500 family of Recommendations.

Appendix I

Cybersecurity operational information ontology

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

Clause 7 of this Recommendation uses an ontology of cybersecurity operational information as depicted in Figure 7-1. This appendix details the ontology.

It consists of cybersecurity operation domains, roles required to run the operations in the domains, and cybersecurity information associated with the roles. They are elaborated on below.

I.1 Cybersecurity operation domains

The term "cybersecurity operation" covers a range of security operations in cyber society, but this ontology focuses on the cybersecurity operations that preserve information security in cyber societies. Information security is the preservation of information confidentiality, integrity, and availability, and it sometimes also encompasses accountability, authenticity, and reliability of information.

To describe the domain of such operations, the ontology provides three cybersecurity operation domains: IT asset management, incident handling, and knowledge accumulation.

IT asset management: This domain runs cybersecurity operations inside user organizations such as installing, configuring and managing IT assets, and covers both incident prevention and damage control operations. IT assets include not only a user's own IT assets but also network connectivity, cloud services, and identity services provided by external entities for the user.

Incident handling: This domain detects and responds to incidents occurring in cyber societies by monitoring computer events, incidents comprised of multiple computer events, and attack behaviours that caused the incidents. More specifically, it monitors computer events, and when an anomaly is detected, it produces an incident report. Based on the report, it investigates the incident in detail so that it can clarify the attack pattern and its countermeasures. Based on the incident analysis, it may provide alerts and advisories, e.g., early warnings against potential threats, to user organizations.

Knowledge accumulation: This domain collects and generates cybersecurity information and extracts reusable knowledge for other organizations. To facilitate the reusability, it provides common naming and taxonomy, with which it organizes and accumulates the knowledge. This domain serves as the basis of global collaboration beyond organization borders.

I.2 Roles

Based on the cybersecurity operation domains defined above, this clause identifies roles necessary for running cybersecurity operations in each domain. The IT asset management domain has an administrator and an IT infrastructure provider, the incident handling domain has a response team and a coordinator, and the knowledge accumulation domain has a researcher, a product and service developer, and a registrar for their operations, respectively. Note that the roles are defined from the viewpoint of functions; therefore one entity may take on several roles depending on the context.

Administrator: This role administers the system of its organization and maintains its functionality. For this purpose, this role monitors the system usage, diagnoses the system by running integrity checks, scanning vulnerability, and running penetration tests, and then assesses the security level of the system. A system administrator inside each organization is one typical instance. A managed security service provider (MSSP) also serves as an administrator if an organization outsources some of the above operations to it.

IT infrastructure provider: This role provides the IT infrastructure for an organization. The infrastructure includes the network connectivity and cloud services such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The IT infrastructure provider possesses information on inter-organizational networks; e.g., network topology information and specifications of cloud services. An Internet service provider (ISP), application service provider (ASP), and cloud service provider (CSP) are typical instances.

Response team: This role monitors and analyses assorted incidents in cyber societies, e.g., unauthorized access, distributed denial of service (DDoS) attacks and phishing, and accumulates incident information. Based on the information, it may implement countermeasures, e.g., blocking traffic and registering phishing site addresses on black lists. The incident response team inside an MSSP is a typical instance.

Coordinator: This role coordinates with the other roles and addresses potential threats based on known incident-related information. It provides warnings to other organizations and sometimes leads the collaborative mitigation to handle devastating and large-scale attacks such as DDoS attacks. The CERT Coordination Center (CERT/CC), be it either commercial or non-commercial, is a typical instance.

Researcher: This role researches cybersecurity issues including vulnerabilities and attacks, extracts knowledge from the research, and accumulates it. It publishes many of the reusable information through the registrar so that individual organizations may implement needed countermeasures. X-force within International Business Machines Corp. (IBM), the Risk Research Institute of Cyber Space (RRICS) at the Little eArth Corporation Co., Ltd. (LAC), and McAfee Lab within McAfee Inc., are typical instances.

Product and service developer: This role develops products and services and accumulates their information, such as their versions, configurations, vulnerabilities and patches. It publishes much of the reusable information through the registrar so that, as with the researcher, individual organizations may implement needed countermeasures. A software vendor and individual private software programmer are typical instances.

Registrar: This role classifies, organizes, and accumulates cybersecurity knowledge provided by the researcher and the product and service developer so that the knowledge can be reutilized by other organizations. NIST and the Information-Technology Promotion Agency, Japan, are typical instances. In some cases, an entity serving as researcher or product and service developer may also serve as registrar and publish information.

I.3 Cybersecurity information

Based on the operation domains and roles, this clause identifies cybersecurity information needed for operations. Considering the information each of the roles engages in, this ontology defines four databases; user resource, provider resource, incident, and warning, and three knowledge bases: product and service, countermeasure, and cyber risk.

I.3.1 User-resource database

The user-resource database accumulates information on assets inside individual organizations and contains information, such as lists of software/hardware, their configurations, status of resource usage, security policies including access control policies, security level assessment results, and intranet topology. It also contains external resource information that individual user organizations utilize, such as lists of subscribing cloud services (e.g., data centres and SaaS) and their usage records. The administrator manipulates such information. The ARF and CRF can be utilized for describing the IT asset assessment results while the CVSS and CWSS scores can be utilized for scoring the security level of the IT asset. The scores are useful for administrators in prioritizing the urgency of security operations on IT assets.

I.3.2 Provider-resource database

The provider-resource database accumulates information on assets outside individual organizations. In order to run effective and efficient cybersecurity operations, the database needs to be linked to a user resource database since the border between internal and external IT assets becomes increasingly unclear, especially in cloud computing. The IT infrastructure provider manipulates such information. The database mainly contains information on provider networks and cloud services. Provider network information is on networks with which each organization is connected with other organizations, such as topology, routing information, access control policies, traffic status, and security levels. Cloud service information includes the service specifications, workload information, and security policy information of each cloud service. Note that information specific to user organizations, such as the local configuration of each cloud service, is stored in the user resource database.

I.3.3 Incident database

The incident database contains information on incidents, which is generated on the basis of an analysis of the information in the user resource database. The response team manipulates the information. This database includes three records: event record, incident record, and attack record.

The event record contains information on computer events including that on packets, files, and their transactions. Usually, computers automatically provide most of the records as computer logs, such as for log-in time and date as well as terminal information provided when root users log in to a system. The logs are instances of this record. CEE can be utilized to describe the record.

The incident record contains information on security incidents and provides information such as the current state of user systems and further risks. It is derived from analyses of several event records and their conjectures, which are created automatically or manually. For instance, when excessive access to one computer is detected, the state of the computer (excessive access to one computer) and its expected consequence (denial of service) should be recorded in the incident record. The harmfulness of the incident as well as the need for countermeasures can be judged based on this record. Note that an incident record may record false incidents; i.e., incident candidates judged as non-incidents after an investigation. The incident object description exchange format (IODEF) can be utilized to describe the record.

The attack record contains information on attacks derived from analyses of incident records. It describes the attack sequence; such as how the attack was initiated, which part of the IT assets were targeted, and how the attack's damage was propagated. Note that this record needs to be linked to the incident record.

I.3.4 Warning database

The warning database contains information on cybersecurity warnings. The information is designed for either the general public or a specific organization. The one for the general public usually contains statistical information and alerts while the one for a specific organization contains security advice customized for the organization. The information is generated on the basis of the information in the incident database and the cyber risk knowledge base. The coordinator and response team manipulate such information. Based on the warnings, user organizations may implement countermeasures against warned cybersecurity risks.

I.3.5 Cyber risk knowledge base

The cyber risk knowledge base accumulates cybersecurity risk information. It is provided by the researcher and product and service developer, and is then organized and classified by the registrar. The knowledge base includes vulnerability and threat knowledge bases.

Vulnerability knowledge base: This knowledge base accumulates known vulnerability information, which includes naming, taxonomy, and enumeration of known software and system vulnerability. It also includes information on human vulnerabilities, which are vulnerabilities that human IT users are exposed to. The National Vulnerability Database (NVD) and the Open Source Vulnerability Database (OSVDB) are practical instances of this database, and CVE and CWE can be utilized to describe the contents of the knowledge base.

Threat knowledge base: This knowledge base accumulates known cybersecurity threat information. It includes attack and misuse knowledge bases. The attack knowledge base accumulates information on attacks such as attack patterns, attack tools (e.g., malware), and their trends. Trend information includes, for instance, past attack trends in terms of geography and attack targets, and statistical information on past attacks. CAPEC and MAEC can be utilized to describe the contents of the knowledge base.

The misuse knowledge base accumulates information on misuses attributed to users' inappropriate usage, be it either benign or malicious. Benign usage includes mistyping, misrecognition caused by inattentive blindness, misunderstanding, and being caught in phishing traps. Malicious usages include compliance violations such as unauthorized service usage and access to inappropriate materials. Note that the attack and misuse knowledge bases are omitted from Figure 7-1 for simplicity.

I.3.6 Countermeasure knowledge base

The countermeasure knowledge base accumulates information on countermeasures to cybersecurity risks. It is provided by the researcher and product and service developer, and is then organized and classified by the registrar. The knowledge base contains assessment and detection/protection knowledge bases.

Assessment knowledge base: This knowledge base accumulates known rules and criteria for assessing the security level of IT assets, checklists of configurations, and heuristics including best practices. The CVSS/CWSS formulae are two of the best practices for assessing security levels and are accumulated in this knowledge base. Apart from that, XCCDF and OVAL can be utilized to describe rules and provide checklists.

Detection/protection knowledge base: This knowledge base accumulates known rules and criteria for detecting/protecting security threat. It also accumulates heuristics including best practices.

I.3.7 Product and service knowledge base

The product and service knowledge base accumulates information on products and services. It is provided by the researcher and product and service developer, and is then organized and classified by the registrar. The knowledge base includes the version and configuration knowledge bases.

Version knowledge base: This knowledge base accumulates version information on products and services, which includes naming and enumeration of their versions. Regarding the product, security patches are also included here. CPE can be utilized to enumerate common platforms.

Configuration knowledge base: This knowledge base accumulates configuration information on products and services. It includes naming, taxonomy and enumeration of known configurations of products and services. Regarding service configuration, it also contains guidelines on service usages. CCE can be utilized to enumerate common configurations of products.

Some supplementary information on this ontology is found in [b-Ontology] and in Appendix II of [b-ITU-T X.1500].

Appendix II

Specifications describing databases and knowledge bases

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

The seven types of information introduced in clause 7 are described with a range of cybersecurity specifications including ITU-T X.1500-compatible specifications (e.g., CVE and IODEF), as can be seen in Table I.1. Thus, the level of details of discovered cybersecurity information will follow the level of detail of the specifications. Using the approach the level of details is flexible and thus various specifications could be built for specific purposes.

Table II.1 – Specifications supporting the ontology

Domains	KBs/DBs		Specifications
IT asset management	User resource DB		ARF, AI, CVSS/CWSS scores
	Provider resource DB		---
Incident handling	Incident DB		CEE, IODEF
	Warning DB		IODEF
Knowledge accumulation	Cyber risk KB	Vulnerability KB	CVE, CWE, CVRF
		Threat KB	CAPEC, MAEC
	Countermeasure KB	Assessment KB	CVSS/CWSS formula
		Detection/protection KB	OVAL, XCCDF
	Product and service KB	Version KB	CPE
		Configuration KB	CCE
NOTE – DB: Database; KB: Knowledge base.			

Appendix III

An illustrated implementation of RDF-based discovery

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

III.1 RDF-based discovery implementation example

The concept depicted in Figure 9-1 could be implemented by putting the discovery agents and the registry agents together inside RDF search engines. Cybersecurity entities send a discovery request to an RDF search engine, which returns list of identities and their capabilities. Note that each search engine has different sources, which become its search range.

In a practical environment, to secure scalability, the source can be registered and managed hierarchically, as shown in Figure III.1. Tier 1 can be an individual RDF search engine that actually works as the discovery agent, tier 2 might be an entity registered under the rules of operation of a regional registry such as the American Registry for Internet Numbers (ARIN), Réseaux IP Européens (RIPE), or the Asia Pacific Network Information Centre (APNIC), and more hierarchy may be introduced depending on the implementation. A source may be CERT or any other cybersecurity entity.

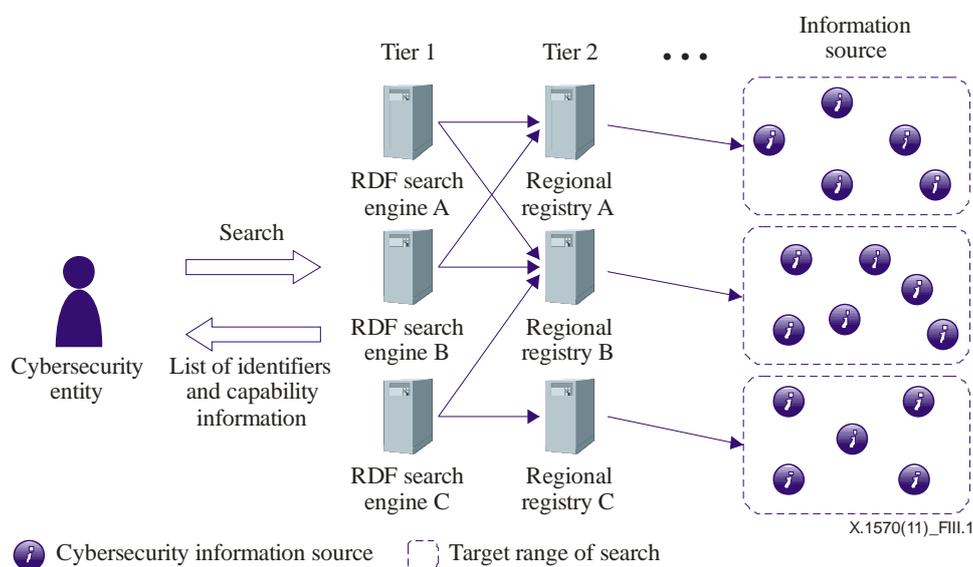


Figure III.1 – Hierarchy of source registry

III.2 Class hierarchy of cybersecurity information

Figure III.2 shows the discovery mechanism's class hierarchy. Each class represents the category introduced in Appendix II of [b-ITU-T X.1500]. For detail on each category, refer to the Recommendation. Note that the XML namespace defined by ITU-T is used [b-ITU-T X.1500].

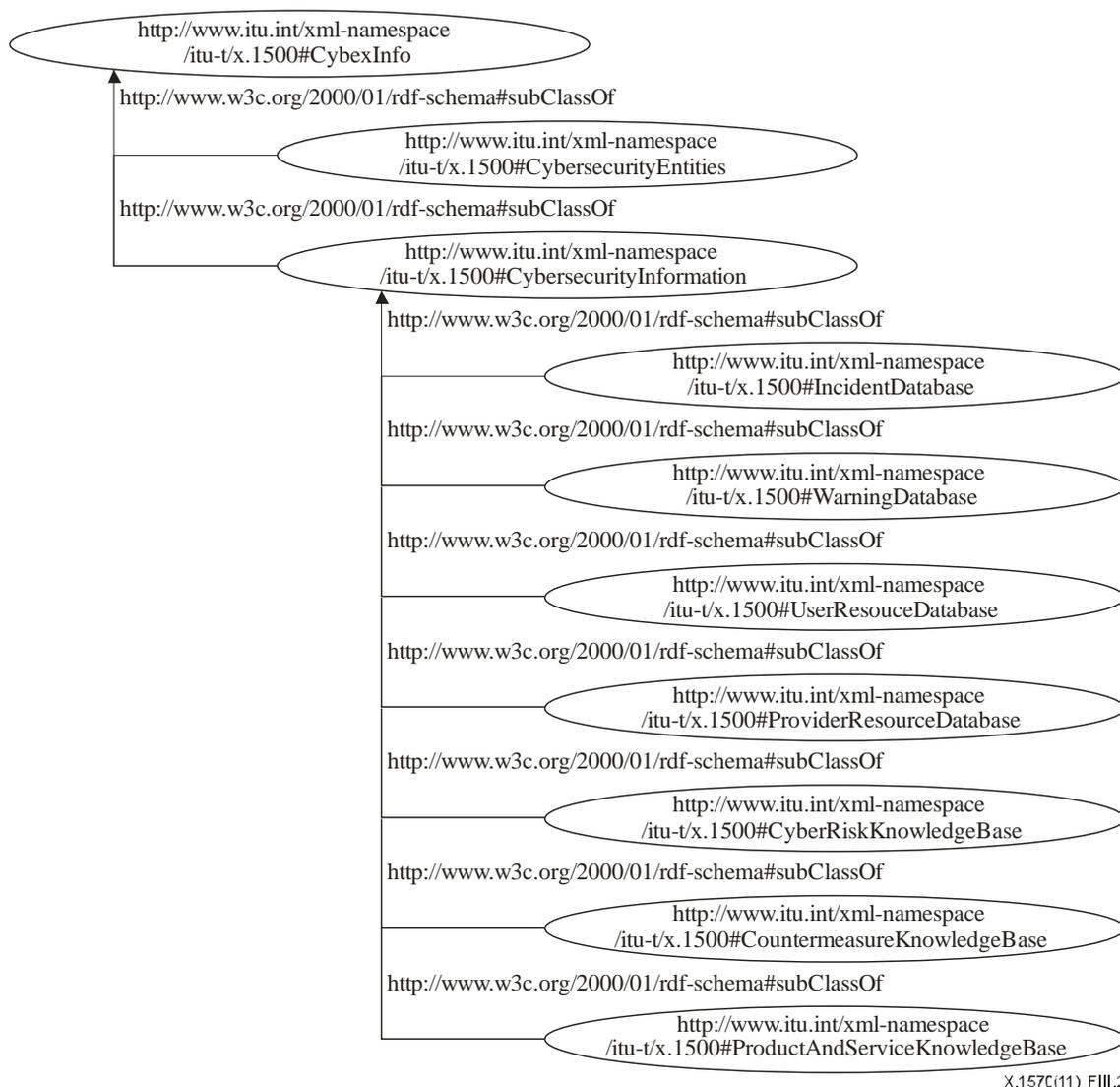


Figure III.2 – Class hierarchy of cybersecurity information

NOTE – The use of the **.int** in the top level domain name is shown as an example in Figure III.3, and is not intended to be used operationally.

Each cybersecurity class usually includes the following attributes:

- **entry_date**: stores the date of data entry/modification
- **issuer_name**: stores the issuer name (the issuer can be either private or corporate)
- **contact_email**: stores the contact party's email address
- **resources**: stores the identifiers, such as web addresses, to further resources
- **Info_type**: stores the type of information such as CVE, CWSS [b-CWSS], CVSS [b-ITU-T X.1521], OVAL [b-OVAL], SCAP [b-SCAP], XCCDF [b-XCCDF], CPE [b-CPE], CCE [b-CCE], and ARF.

Any party seeking cybersecurity information can request data in a unit of any particular class. Information can be searched for by criteria including class name, class attribute, and last modification date and time.

The test implementation of the discovery scheme is available online: <http://cybiet.sourceforge.net/>

NOTE – The implementation discovers cybersecurity information that is structured following the ontology described in Figure 7-1.

Bibliography

- [b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.
- [b-ITU-T X.1500.1] Recommendation ITU-T X.1500.1 (2012), *Procedures for the registration of arcs under the object identifier (OID) arc for cybersecurity information exchange*.
- [b-ITU-T X.1520] Recommendation ITU-T X.1520 (2011), *Common vulnerabilities and exposures*.
- [b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.
- [b-AI] NIST, *The Asset Identification*.
<<http://scap.nist.gov/specifications/ai/>>
- [b-ARF] *Assessment Results Format*
<<https://measurablesecurity.mitre.org/incubator/arf/>>
- [b-CCE] *Common Configuration Enumeration*.
<<https://cce.mitre.org/>>
- [b-CPE] *Common Platform Enumeration*.
<<https://cpe.mitre.org/>>
- [b-CWSS] *Common Weakness Scoring System*.
<<https://cwe.mitre.org/cwss/>>
- [b-Gruber] Gruber T.R. (1993), *Toward principles for the design of ontologies used for knowledge sharing*. International Journal of Human-Computer Studies, Vol. 43, Issues 4-5, November 1995, pp. 907-928.
- [b-Ontology] Takahashi T., Kadobayashi Y., Fujiwara H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks (SIN), September 2010.
- [b-OVAL] *Oval – Open Vulnerability and Assessment Language*.
<<https://oval.mitre.org/>>
- [b-SCAP] *Security Content Automation Protocol (SCAP)*.
<<http://scap.nist.gov/>>
- [b-XCCDF] *XCCDF – The Extensible Configuration Checklist Description Format*
<<http://scap.nist.gov/specifications/xccdf/>>

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