International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1500
Amendment 12
(03/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Overview of cybersecurity

Overview of cybersecurity information exchange

Amendment 12

Recommendation ITU-T X.1500 (2011) – Amendment 12

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	**X.1500–X.1519**
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1500

Overview of cybersecurity information exchange

Amendment 12

Summary

Recommendation ITU-T X.1500 describes techniques for exchanging cybersecurity information. These techniques can be used individually or in combinations, as desired or appropriate, to enhance cybersecurity through coherent, comprehensive, global, timely and assured information exchange. No obligations to exchange information are implied, nor are the means of acquisition or ultimate use of the information treated. Cybersecurity information exchange (CYBEX) is one of the elements providing confidence and security in the use of ICTs.

Amendment 12 provides a list of structured cybersecurity information techniques that have been created to be continually updated as these techniques evolve, expand, are newly identified or are replaced. The list follows the outline provided in the body of the Recommendation. This amendment reflects the situation of recommended techniques as of March 2017, including bibliographical references.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1500	2011-04-20	17	11.1002/1000/11060
1.1	ITU-T X.1500 (2011) Amd. 1	2012-03-02	17	11.1002/1000/11574
1.2	ITU-T X.1500 (2011) Amd. 2	2012-09-07	17	11.1002/1000/11751
1.3	ITU-T X.1500 (2011) Amd. 3	2013-04-26	17	11.1002/1000/11942
1.4	ITU-T X.1500 (2011) Amd. 4	2013-09-04	17	11.1002/1000/12041
1.5	ITU-T X.1500 (2011) Amd. 5	2014-01-24	17	11.1002/1000/12159
1.6	ITU-T X.1500 (2011) Amd. 6	2014-09-26	17	11.1002/1000/12334
1.7	ITU-T X.1500 (2011) Amd. 7	2015-04-17	17	11.1002/1000/12446
1.8	ITU-T X.1500 (2011) Amd. 8	2015-09-17	17	11.1002/1000/12596
1.9	ITU-T X.1500 (2011) Amd. 9	2016-03-23	17	11.1002/1000/12851
1.10	ITU-T X.1500 (2011) Amd. 10	2016-09-07	17	11.1002/1000/13071
1.11	ITU-T X.1500 (2011) Amd. 11	2017-03-30	17	11.1002/1000/13263
1.12	ITU-T X.1500 (2011) Amd. 12	2018-03-29	17	11.1002/1000/13590

_____

* 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 is intended to be adaptable, extensible, and non-prescriptive to allow a wide range of techniques – some of which are continuously evolving and in varying stages of completion – to be applied in different instantiations to enhance the exchange of cybersecurity information about telecommunication/ICT infrastructure, devices, and services. It will be revised periodically as those techniques evolve – those that are appropriate will be published as ITU-T Recommendations in the ITU-T X.1500 series.

The expectation for the techniques embodied in this Recommendation is that telecommunication/ ICT organizations, including computer incident response teams (CIRTs), both within and between jurisdictions, will:

a) have information to enable decision making and action to substantially enhance the confidentiality, integrity and availability of global telecommunication/ICT facilities and services;

b) have information to facilitate secure collaborative processes and controls which improve the level of assurance in the information exchanges between organizations;

c) enable a coherent approach to manage and exchange cybersecurity information on a global basis;

d) improve security awareness and collaboration to diminish cyberthreats, cyberattacks and malware.

The techniques include:

• structuring cybersecurity information for exchange purposes;

• identifying and discovering cybersecurity information and entities;

• establishment of trust and policy agreement between exchanging entities;

• requesting and responding with cybersecurity information;

• assuring the integrity of the cybersecurity information exchange;

and are organized into "clusters":

• Weakness, vulnerability and state.

• Event, incident, and heuristics.

• Information exchange policy.

• Identification, discovery, and query.

• Identity assurance.

• Exchange protocols.

Recommendation ITU-T X.1500

Overview of cybersecurity information exchange

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T X.1500 (2011). Amendments 1 to 11 have been superseded.

1   Scope

This Recommendation presents a cybersecurity information exchange (CYBEX) model and discusses techniques that can be used to facilitate the exchange of cybersecurity information. These techniques can be used individually or in combinations, as desired or appropriate, to enhance cybersecurity through coherent, comprehensive, global, timely and assured information exchange. No obligations to exchange information are implied, nor are the means of acquisition or ultimate use of the information treated. The techniques include the structured global discovery and interoperability of cybersecurity information in such a way as to allow for continual evolution to accommodate the significant activities and specification evolution occurring in numerous cybersecurity forums. CYBEX is one of the elements providing confidence and security in the use of ICTs.

This Recommendation has the following basic functions that can be used separately or together as appropriate:

•   structuring cybersecurity information for exchange purposes;

•   identifying and discovering cybersecurity information and entities;

•   establishment of trust and policy agreement between exchanging entities;

•   requesting and responding with cybersecurity information;

•   assuring the integrity of the cybersecurity information exchange.

Subject to agreed policies and applicable laws and regulations, the means of acquiring information as well as the uses made of the information are specifically out of scope and not treated in this Recommendation. Some specific national and regional regulations and legislations may require implementation of mechanisms to protect personally identifiable information. Neither the techniques described in this Recommendation nor the exchange of related cybersecurity information are mandated by this Recommendation.

2   References

None.

3   Definitions

3.1   Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1   cybersecurity [b-ITU-T X.1205]: The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant

security risks in the cyber environment. The general security objectives comprise availability, integrity (which may include authentication and non-repudiation) and confidentiality.

NOTE – Some specific national regulations and legislations may require implementation of mechanisms to protect personally identifiable information.

3.1.2 **security incident** [b-ITU-T E.409]: Any adverse event whereby some aspect of security could be threatened.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **assurance**: The degree of confidence that the process or deliverable meets defined characteristics or objectives.

3.2.2 **exchange protocol**: A set of technical rules and format governing the exchange of information between two or more entities.

3.2.3 **information exchange policy**: The terms and conditions associated with the use and sharing of cybersecurity information.

3.2.4 **system state**: The current status of a system or entity, including such information as its configuration, memory usage, or other data relevant to cybersecurity.

3.2.5 **vulnerability** (aligned with [b-ITU-T X.800]): Any weakness that could be exploited to violate a system or the information it contains.

3.2.6 **weakness**: A shortcoming or imperfection that, while not itself being recognized as a vulnerability, 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:

ARF Assessment Results Format or Asset Reporting Format (depending on the context)

BEEP Blocks Extensible Exchange Protocol

CA Certification Authority

CAPEC Common Attack Pattern Enumeration and Classification

CCE Common Configuration Enumeration

CEE Common Event Expression

CEEE Common Event Expression Exchange

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

CYIQL Cybersecurity Information Query Language

DDoS Distributed Denial of Service

EVC	Extended Validation Certificates
EVCERT	Extended Validation Certificate
HTTP	HyperText Transfer Protocol
IC	Integrated Circuit
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IODEF	Incident Object Description Exchange Format
IPS	Intrusion Prevention System
IT	Information Technology
MAEC	Malware Attribute Enumeration and Characterization
OID	Object Identifier
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
RID	Real-time Inter-network Defense
SCAP	Security Content Automation Protocol
SOAP	Simple Object Access Protocol
TLP	Traffic Light Protocol
TLS	Transport Layer Security
TNC	Trusted Network Connect
TPM	Trusted Platform Module
XCCDF	eXtensible Configuration Checklist Description Format

5   Conventions

When the term "standard" or "standards" is used in this Recommendation in the generic sense, it should be interpreted to include: standards; specifications and Recommendations.

6   Basic concept – Cybersecurity information exchange (CYBEX)

This cybersecurity information exchange (CYBEX) Recommendation is intended to accomplish a simple, limited objective – describe techniques by which cybersecurity entities can exchange cybersecurity information using methods which provide a suitable level of assurance. Such entities typically consist of organizations, persons, devices, or processes possessing or seeking cybersecurity information. Most frequently, these entities are CIRTs and the operators or vendors of equipment, software or network-based systems.

Cybersecurity information exchange is valuable for achieving enhanced cybersecurity and infrastructure protection, as well as contributing to the principal functions performed by CIRTs.

The exchange of cybersecurity information can occur within highly compartmentalized trust communities adhering to need-to-know principles based on previously agreed-upon policies, as well as within the public domain. Knowledge of threats, vulnerabilities, incidents, risks, and mitigations and their associated remedies are typical examples of the types of cybersecurity information exchanged between entities. The related techniques included in this Recommendation are intended to facilitate this information exchange and thereby enhance cybersecurity.
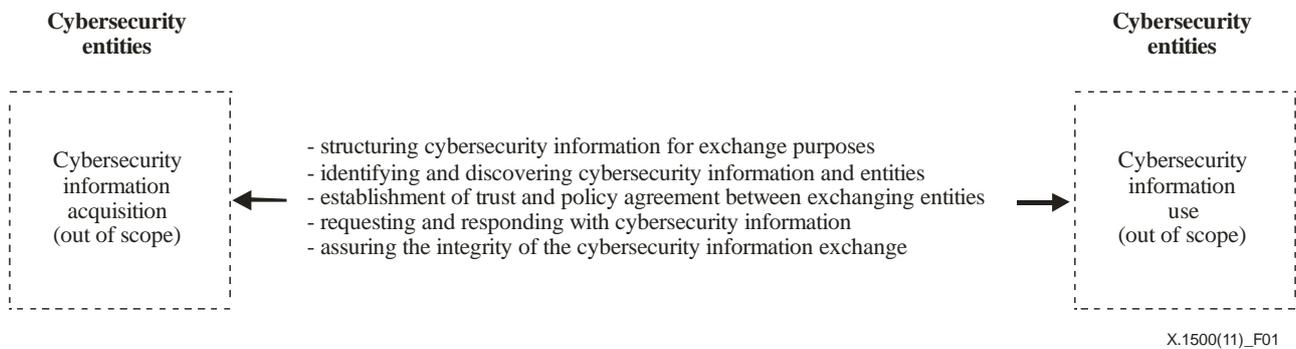
Figure 1 – CYBEX model

The general cybersecurity information exchange model used in this Recommendation, as shown in Figure 1, consists of basic functions that can be used separately or together as appropriate, and extended as needed in order to facilitate assured cybersecurity information exchanges. These are:

- structuring cybersecurity information for exchange purposes;

- identifying and discovering cybersecurity information and entities;

- establishment of trust and information exchange policy agreements between exchanging entities;

- requesting and responding with cybersecurity information;

- assuring the integrity of the cybersecurity information exchange.

Clause 7 describes techniques for accomplishing these functions.

The exchange of cybersecurity information may be bidirectional. This bidirectionality allows for verified information requests and responses to facilitate required levels of assurance between the parties or to provide certification of delivery.

Subject to agreed policies and applicable laws and regulations, the means of acquiring information as well as the uses made of the information are specifically out of scope and not treated in this Recommendation. For example, some specialized cybersecurity information exchange implementations such as traceback of attack sources may require application-specific mechanisms that allow for a recursive series of requests and responses to obtain required information. However, other implementations such as making cybersecurity measureable and manageable through the use of security automation capabilities are in scope. These and other types of use-cases may be facilitated by the techniques included in this Recommendation. Neither the included techniques nor the exchange of related cybersecurity information are mandated by this Recommendation, and other techniques may be appropriate.

7   Structured cybersecurity information exchange techniques

For the exchange of cybersecurity information to occur between any two entities, the exchange must be structured and described in some consistent manner that is understood by both of those entities. The goal of CYBEX is to make it easier to share cybersecurity information that includes "common enumerations," that is, ordered lists of well-established information values for the same data type. Common enumeration allows distributed databases and other capabilities to be linked together, and facilitates cybersecurity-related comparisons.

For the purposes of accomplishing these exchanges, cybersecurity information includes structured information or knowledge concerning:

- the "state" of equipment, software, or network-based systems as related to cybersecurity, especially vulnerabilities;

- forensics related to incidents or events;
- heuristics and signatures gained from experienced events;
- cybersecurity entities involved;
- specifications for the exchange of cybersecurity information, including modules, schemas, terms and conditions, and assigned numbers;
- the identities and assurance attributes of all cybersecurity information;
- implementation requirements, guidelines and practices.

As a means of describing at a general level the desired attributes of cybersecurity information exchange, the structured information capabilities are organized into six "clusters" of techniques for distinct cybersecurity information exchange groups. These are:

- weakness, vulnerability and state;
- event, incident, and heuristics;
- information exchange policy;
- identification, discovery, and query;
- identity assurance;
- exchange protocol.

These clusters are broad classifications, and capabilities in one cluster may actually be used in one or more other clusters, depending on the application.

Each of the clusters listed above is described in detail in the subclauses below. Each cluster description provides an overview of its role in CYBEX, and lists techniques for its realization. None of the identified techniques are intended to be prescriptive; rather, they simply illustrate techniques considered consistent with the purposes of the relevant cluster. The choice of treatment has primarily to do with the degree of specialization of the "owning" user community and the global benefits derived from importation.

The CYBEX techniques in this Recommendation identify an array of complementary techniques that enable and facilitate these and other instantiations.

The remainder of this clause and the associated Appendix I describe each cluster, including an overview of the role of each within CYBEX, and lists techniques for the realization of each cluster. The references are non-normative and further detailed in the Bibliography.

Implementers and users of the cluster techniques shall comply with all applicable national and regional laws, regulations and policies.

7.1 Weakness, vulnerability and state – exchange cluster

The enabling capabilities associated with the weakness, vulnerability, and state exchange cluster support the exchange of weakness and vulnerability information and assessment of the state of systems and applications.

Table I.1 provides a list of enabling capabilities that are representative of the types that can facilitate the support of exchange of weakness, vulnerability, and state information.

7.2 Event, incident, and heuristics – exchange cluster

The enabling capabilities associated with the event, incident, and heuristics exchange cluster support the exchange of information pertaining to observed events, incidents, or heuristics.

Table I.2 provides a list of enabling capabilities that are representative of the types that can facilitate the exchange of observed event, incident or heuristic information in a structured fashion among CIRTs and others. This exchanged information may be used to create comprehensive responses to attacks as well as reduce existing weaknesses and vulnerabilities.

7.3 Information exchange policy – exchange cluster

The enabling capabilities associated with the information policy exchange cluster supports the sharing and use of cybersecurity information between entities concerning the terms and conditions associated with the information being shared. This understanding may be bound to the specific information being shared, or to the broad class of information to which it belongs, or be associated with the entities involved. To the extent it is necessary under the circumstances, it is desirable to provide notice of these policies to the entities involved. This notice may take many forms, and be conveyed together with the information or independently provided through a query-response mechanism.

Table I.3 provides a list of enabling capabilities that are representative of the types that can facilitate the exchange of policy information between cybersecurity entities. Note that requirements and protocols for policy exchange continue to emerge within information security exchange forums, and care should be taken to ensure their proper implementation.

7.4 Identification, discovery, and query cluster

The enabling capabilities associated with the identification, discovery, and query cluster supports identification, discovery and query processes.

Common interests exist among cybersecurity communities regarding cybersecurity identifiers and their creation, administration, discovery, verification, and use. Some of those interests include:

- Enhancing the value of the cybersecurity information by enabling widespread exchange of the related event information and analysis of events over long periods of time.
- Enhancing the security of cybersecurity information exchanges by enabling identifier information to be obtained for verification and the related policies to be known.
- Enhancing the flexibility of cybersecurity information exchanges by enabling new or additional information associated with the message to be obtained, e.g., information status.

Different cybersecurity organizations may desire to implement common cybersecurity protocols for the capture and exchange of system state, vulnerability, incident forensics, and incident heuristics information 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. That a globally unique identifier used for global cybersecurity information exchange may exist necessarily implies that it has 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.

Table I.4 provides a list of enabling capabilities that are representative of the types that can facilitate identification of cybersecurity organizations, and discovering and querying for cybersecurity information processes.

7.5 Identity assurance cluster

The enabling capabilities associated with the identity assurance cluster supports identity assurance.

Within CYBEX, the actual exchange of structured information can occur many different ways – via a network or physically transported. A key element for this exchange is trust – trust in the identity of the parties, as well as the information being conveyed.

Table I.5 provides a list of enabling capabilities that are representative of the types that can support identity assurance.

7.6 Exchange protocol cluster

The enabling capabilities within the exchange protocol cluster include exchange protocols that may be used in diverse cybersecurity information exchange contexts. The secure exchange of information requires a combination of protocols listed below. Real-time inter-network defense (RID) provides a messaging framework to communicate incident information and associated policies of that information. The transport protocol for RID messages encapsulating IODEF (as well as any extensions to IODEF) incident documents includes BEEP, SOAP, and HTTPS transport options listed. The transport for RID messages (the initial protocol developed for the transport of RID) may be substituted by SOAP, BEEP, or future protocols as they are developed. The security and privacy considerations are contained in RID to enable the separation of the messaging from transport.

Table I.6 provides a list of enabling capabilities that are representative of the types of exchange protocols that may be used as an information exchange.

Appendix I

Structured cybersecurity information exchange techniques

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

Table I.1 – Techniques in the weakness, vulnerability and state exchange cluster

Technique	Description	References
Common vulnerabilities and exposures (CVE)	Common vulnerabilities and exposures is a method for identifying and exchanging information security vulnerabilities and exposures, and provides common identifiers for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration." CVE is designed to allow vulnerability databases and other resources to be linked together, and to facilitate the comparison of security tools and services. As such, 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 intention of CVE 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, as well as identifying any new problems that become public, and then addressing any older security problems that require validation.	[b–ITU-T X.1520]
Common vulnerability scoring system (CVSS)	The common vulnerability scoring system process provides for an open framework for communicating the characteristics and impacts of ICT vulnerabilities. CVSS consists of three groups: base, temporal and environmental. Each group produces a numeric score ranging from 0 to 10, and a vector, a compressed textual representation that reflects the values used to derive the score. The base group represents the intrinsic qualities of a vulnerability. The temporal group reflects the characteristics of a vulnerability that change over time. The environmental group represents the characteristics of a vulnerability that are unique to the environment of the user. CVSS enables ICT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting a common language of scoring ICT vulnerabilities.	[b–ITU-T X.1521]

Table I.1 – Techniques in the weakness, vulnerability and state exchange cluster

Technique	Description	References
Common weakness enumeration (CWE)	Common weakness enumeration is a process for identifying and exchanging unified, measurable sets of software weaknesses. CWE enables more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems. It also provides for better understanding and management of software weaknesses related to architecture and design. CWE implementations are compiled and updated by a diverse, international group of experts from business, academia and government agencies, ensuring breadth and depth of content. CWE provides standardized terminology, allows service providers to inform users of specific potential weaknesses and proposed resolutions, and allows software buyers to compare similar products offered by multiple vendors.	[b-ITU-T X.1524CWE]
Common weakness scoring system (CWSS)	The common weakness scoring system (CWSS) provides for an open framework for communicating the characteristics and impacts of software information and communication technology (ICT) weaknesses during development of software capabilities. The goal of CWSS is to enable ICT software developers, managers, testers, security vendors and service suppliers, buyers, application vendors and researchers to speak from a common language of scoring ICT weaknesses that could manifest as vulnerabilities when the software is used.	[b-ITU-T X.1525CWSS]
Critical security controls for effective cyber defence (CSC)	The critical security controls and associated compendiums describe a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks. The measures reflect the combined knowledge of actual attacks and effective defences.	[b-CSC]
Open vulnerability and assessment language (OVAL)	The language for the open definition of vulnerabilities and for the assessment of a system state (also known as Open vulnerability and assessment language) is an international specification effort to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system endpoint details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of endpoints systems for testing, analysing the endpointsystem for the presence of the specified machine state (vulnerability, configuration, patch state, etc.), and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language. OVAL schemas written in XML have been developed to serve as the framework and vocabulary of the OVAL	[b- ITU-T X.1526OVAL]

Table I.1 – Techniques in the weakness, vulnerability and state exchange cluster

Technique	Description	References
	language. These schemas correspond to the three steps of the assessment process: an OVAL system characteristics schema for representing endpointsystem information, an OVAL definition schema for expressing a specific machine state, and an OVAL results schema for reporting the results of an assessment.	
eXtensible configuration checklist description format (XCCDF)	The eXtensible configuration checklist description format is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices. XCCDF documents are expressed in XML.	[b-XCCDF]
Common platform enumeration (CPE)	Common platform enumeration (CPE) is a standardized method to identify and describe the software systems and hardware devices present in an enterprise's computing asset inventory. CPE provides: a naming specification, including the logical structure of well-formed CPE names and the procedures for binding and unbinding these names with machine-readable encodings,; a matching specification, which defines procedures for comparing CPE names to determine whether they refer to some or all of the same products or platforms,; and a dictionary specification, which defines the concept of a dictionary of identifiers and prescribes high-level rules for dictionary curators.	[b-ITU-T X.1528] [b-ITU-T X.1528.1] [b-ITU-T X.1528.2] [b-ITU-T X.1528.3] [b-ITU-T X.1528.4][b-CPE]
Software identification tag	Software identification tags (SWID tags) record unique information about an installed software application, including its name, edition, version, whether it is part of a bundle, etc. SWID tags support software inventory and asset management initiatives.	[b-ISO/IEC 19770-2]
Common configuration enumeration (CCE)	Common configuration enumeration provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, CCE identifiers can be used to associate checks in configuration assessment tools with statements in configuration best-practice documents.	[b-CCE]
Assessment results format (ARF)	Assessment results format (ARF) is an open specification that provides a structured language for exchanging per-device assessment results data between assessment tools, asset databases, and other products that manage asset	[b-ARF]

Table I.1 – Techniques in the weakness, vulnerability and state exchange cluster

Technique	Description	References
	information. It is intended to be used by tools that collect detailed configuration data about IT assets. ARF also includes an aggregate reporting specification to enable reporting on information across multiple assets and a tasking and query language to enable requesting assessment results. The security automation specifications describe an end-to-end process for delivering assessment content to data stores, requesting assessments against that content, reporting on the results of those assessments, and aggregating assessment results to an enterprise level.	

Table I.2 – Techniques relevant to the event, incident, and heuristics exchange cluster

Technique	Description	References
Common event expression (CEE)	Common event expression standardizes the way computer events are described, logged, and exchanged. By using CEE's common language and syntax, enterprise-wide log management, correlation, aggregation, auditing, and incident handling can be performed more efficiently and produce better results. The primary goal of the effort is to standardize the representation and exchange of logs from electronic systems. CEE breaks the recording and exchanging of logs into four (4) components: the event taxonomy, log syntax, log transport, and logging recommendations.	[b-CEE]
Incident object description exchange format (IODEF)	The incident object description exchange format defines a data representation that provides a standard format for the exchange of information commonly exchanged information by CIRTs about computer security incidents. IODEF describes an information model and provides an associated data model specified with XML schema.	[b-ITU-T X.1541][b-IETF RFC 5070]
Extensions to IODEF for reporting Phishing	This extends the incident object description exchange format to support the reporting of phishing events. Recommendation ITU-T X.1500 is intended to only describe techniques for commonly understood, assured means for cybersecurity entities to exchange cybersecurity information, and does not include the uses of that information.	[b-IETF RFC 5901]
An IODEF extension for structured cybersecurity information	This document extends the IODEF defined in RFC 5070 to exchange enriched cybersecurity information among security experts at organizations and to facilitate their operations. It provides a well-defined pattern to consistently embed structured information, such as identifier- and XML-based information.	[b-IETF RFC 7203]

Table I.2 – Techniques relevant to the event, incident, and heuristics exchange cluster

Technique	Description	References
Common attack pattern enumeration and classification (CAPEC)	CAPEC is a specification method 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 XML schema and classification taxonomy.	[b-ITU-T X.1544]
Cyber observable eXpression (CybOX)	Cyber observable eXpression (CybOX) is a structured language for the specification, capture, characterization and communication of cyber observables. A wide variety of high-level cyber security use cases rely on such information. CybOX provides a common mechanism (structure and content) for addressing cyber observables across and among this full range of use cases improving consistency, efficiency, interoperability and overall situational awareness.	[b-CybOX]
Malware attribute enumeration and characterization format	The malware attribute enumeration and characterization (MAEC) is a standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviours, artefacts and attack patterns.	[b-ITU-T X.1546]
Structured threat information eXpression (STIX)	Structured threat information expression (STIX) is a structured language for describing cyber threat information so that it can be shared, stored and analysed in a consistent manner. The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible and automatable.	[b-STIX]
Malware metadata exchange format (MMDEF)	The malware metadata exchange format (MMDEF) is a collaborative effort with industry to capture and share information about malware in a standardized fashion. The initial MMDEF schema, which is currently in use by AV vendors, has been augmented to include attributes and metadata specific to the characterization of clean (benign) files, thus supporting the exchange of information on such files and datasets. The MMDEF schema has been enhanced with additional attributes, such as a digital signature object for characterizing digitally signed binaries, as well as a software package object for the linking of files with the software packages that they may belong to. Along with these new types, many tool-extractable elements, such as the version and internal name, were added to the existing file object for their utility in whitelisting. Current enhancements under way include additions for capturing blackbox behavioural metadata, such as the type of information captured by dynamic malware analysis tools. This allows for the creation of a standardized format for such data, permitting correlation and clustering based on shared	[b-MMDEF]

Table I.2 – Techniques relevant to the event, incident, and heuristics exchange cluster

Technique	Description	References
	behavioural functionality, as well as facilitating the exchange of such information across various entities.	
Phishing, fraud, and misuse format	The phishing, fraud, and misuse exchange format extends the incident object description exchange format (IODEF) to support the reporting of phishing, fraud, and other types of misuse. The extensions also provide a standard format for exchanging information about widespread spam incidents. These extensions are flexible enough to support information gleaned from activities throughout the entire electronic fraud or spam cycle. Both simple reporting and complete forensic reporting are possible, as is consolidating multiple incidents. NOTE – This Recommendation only describes techniques for commonly understood, assured means for cybersecurity entities to exchange cybersecurity information, and does not include the uses of that information.	[b-IETF RFC 5901]
Common attack pattern enumeration and classification (CAPEC)	CAPEC is a specification method 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 XML schema and classification taxonomy.	[b-CAPEC]
Malware attribute enumeration and characterization format	The malware attribute enumeration and characterization format (MAEC) is a formal language that includes a schema to provide both a syntax for the common vocabulary of enumerated attributes and behaviours, and an interchange format for structured information about these data elements. The enumerations are at different levels of abstraction: low-level actions, mid-level behaviours and high-level mechanisms. At the lowest level, MAEC describes attributes tied to the basic functionality and low-level operation of malware. At the middle level, MAEC language organizes the aforementioned low-level actions into groups for the purpose of defining mid-level behaviours. At the more conceptual and high level, MAEC's vocabulary allows for the construction of mechanisms that abstract clusters of mid-level malware behaviours based upon the achievement of a higher order classification.	[b-MAEC]

Table I.3 – Techniques relevant to the policy exchange cluster

Technique	Description	References
Traffic light protocol (TLP)	The traffic light protocol (TLP) was created to encourage greater sharing of sensitive information. The originator signals how widely they want their information to be circulated beyond the immediate recipient. The TLP provides a simple method to achieve this. It is designed to improve the flow of information between individuals, organizations or communities in a controlled and trusted way. The TLP is based on the concept of the originator labelling information with one of four colours to indicate what further dissemination, if any, the recipient can undertake. The recipient must consult the originator if wider dissemination is required. The TLP is accepted as a model for trusted information exchange among security communities in over 30 countries. The four "information sharing levels" for the handling of sensitive information are: RED – Personal. This information is for named recipients only. In the context of a meeting, for example, RED information is limited to those present. In most circumstances RED information will be passed verbally or in person. AMBER – Limited distribution. The recipient may share AMBER information with others within their organization, but only on a "need-to-know" basis. GREEN – Community wide. Information in this category can be circulated widely within a particular community. However, the information may not be published or posted on the Internet, nor released outside of the community. WHITE – Unlimited. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.	[b-TLP]

Table I.4 – Techniques relevant to the identification, discovery, and query cluster

Technique	Description	References
Discovery mechanisms in the exchange of cybersecurity information	These techniques include methods and mechanisms which can be used to identify and locate sources of cybersecurity information, types of cybersecurity information, specific instances of cybersecurity information, methods available for access of cybersecurity information as well as policies which may apply to the access of cybersecurity information.	[b-ITU-T X.1570]
Guidelines for administering the OID arc for cybersecurity information exchange	A common global cybersecurity identifier namespace is described, together with administrative requirements, as part of a coherent OID arc, and includes identifiers for: • cybersecurity information; • cybersecurity organizations; • cybersecurity policy.	[b-ITU-T X.1500.1]
Resource-oriented lightweight information exchange	The resource-oriented lightweight indicator exchange (ROLIE) defines a resource-oriented approach for security automation information publication, discovery, and sharing. Using this approach, producers may publish, share, and exchange representations of security incidents, attack indicators, software vulnerabilities, configuration checklists, and other security automation information as web-addressable	[b-IETF RFC 8322]

Technique	Description	References
	resources. Furthermore, consumers and other stakeholders may access and search this security information as needed, establishing a rapid and on-demand information exchange network for restricted internal use or public access repositories. This specification extends the Atom Publishing Protocol and Atom Syndication Format to transport and share security automation resource representations.	
XMPP protocol extension for generic publish-subscribe functionality	This specification defines an XMPP protocol extension for generic publish-subscribe functionality. The protocol enables XMPP entities to create nodes (topics) at a pubsub service and publish information at those nodes; an event notification (with or without payload) is then broadcasted to all entities that have subscribed to the node. Pubsub therefore adheres to the classic Observer design pattern and can serve as the foundation for a wide variety of applications, including news feeds, content syndication, rich presence, geolocation, workflow systems, network management systems, and any other application that requires event notifications.	[b-XEP-0060]
Cybersecurity information query language	The cybersecurity information query language (CYIQL) defines a flexible data representation that provides a framework for requesting information commonly exchanged by computer incident response teams (CIRTs) about computer security incidents. This specification describes the information model for CYIQL and provides an associated data model specified with XML schema.	

Table I.5 – Techniques relevant to the identity assurance cluster

Technique	Description	References
Trusted platforms	Computing and communications products with embedded trusted platform modules (TPMs) advance the ability of businesses, institutions, government agencies, and consumers to conduct trustworthy information exchange; therefore, TPMs are relevant to most CYBEX implementations. TPMs are special-purpose integrated circuits (ICs) built into a variety of platforms to enable strong user authentication and machine attestation – essential to prevent inappropriate access to confidential and sensitive information and to protect against compromised networks.	[b-TPM]
	Trusted platform module technology is based on open standards to ensure interoperability of diverse products in mixed-vendor environments. The prevalent TPM standard consists of a set of specifications developed and maintained by the Trusted Computing Group (TCG), alongside with a protection profile for security evaluation against the common criteria.	
	The design principles give the basic concepts of the TPM and generic information relative to TPM functionality. A TPM designer must review and implement the information in the TPM main specification (parts 1-3) and review the platform-specific document for the intended platform. The platform-specific document contains normative statements that affect the design and implementation of a TPM. A TPM designer must review and implement the requirements, including	

Table I.5 – Techniques relevant to the identity assurance cluster

Technique	Description	References
	testing and evaluation, as set by the TCG conformance workgroup. The TPM must comply with the requirements and pass any evaluations set by the conformance workgroup. The TPM may undergo more stringent testing and evaluation.	
Trusted execution environment	Trusted execution environment (TEE) defines a standardized isolation environment for systems on chip (SoC) in which sensitive code, data and resources are processed away from the main operating environment, software and memory on the device. This isolation is enforced by hardware architecture and the boot sequence uses a hardware root of trust in the SoC package making it highly robust against software and probing attacks. In addition, code running in the TEE and using protected resources (known as 'Trusted Applications') is cryptographically verified prior to execution, leading to high integrity assurance.	[b-TEE]
Trusted network connect	ICT security operations often desire to discover the state of operating system (OS)-level and the application software used by the supporting network. For example, when systems lack OS security patches or antivirus signatures, reliable notification is crucial to containing the damage associated with network-based attacks. Making this appraisal requires reliable information that a connected system is in a particular state. In order to prevent systems (e.g., hacked systems) from falsifying information, successful appraisal requires a hardware basis on the system to be appraised. Trusted platforms are embedded in the hardware to record certain facts about the boot process and deliver them in digitally signed form. Furthermore, major chip manufacturers are now supplementing the trusted platforms with a "late launch" capability that allows for execution of trusted code later in the boot sequence. This, in turn, allows events to be reliably recorded after the hardware-specific boot process.	[b-TNC]

Table I.5 – Techniques relevant to the identity assurance cluster

Technique	Description	References
	Network configuration management is effectively a deployment of system attestation: software agents on enterprise machines that periodically send configuration reports to a central repository, which evaluates and flags non-compliant systems. Data from these software agents, while valuable, is easily modified by an attacker. Using the widespread deployment of trusted platforms to enable a more trustworthy evaluation of system state would greatly increase an enterprise's confidence in its configuration management data. Trusted network connect (TNC) is an open architecture for network access control. Its aim is to enable network operators to provide endpoint integrity at every network connection, thus enabling interoperability among multi-vendor network endpoints.	
Entity authentication assurance	This standard provides an authentication life cycle framework for managing the assurance of an entity's identity and its associated identity information in a given context. Specifically it provides methods to 1) qualitatively measure and assign relative assurance levels to the authentication of an entity's identities and its associated identity information, and 2) communicate relative authentication assurance levels.	[b-ITU-T X.1254][b-NIST EAA]
The DNS-based authentication of named entities (DANE) transport layer security (TLS) Protocol: TLSA	Encrypted communication on the Internet often uses transport layer security (TLS), which depends on third parties to certify the keys used. This document improves on that situation by enabling the administrators of domain names to specify the keys used in that domain's TLS servers. This requires matching improvements in TLS client software, but no change in TLS server software.	[b-IETF RFC 6698]
Extended validation certificate framework	The extended validation certificate framework consists of an integrated combination of technologies, protocols, identity proofing, life cycle management, and auditing practices that describe the minimum requirements that must be met in order to issue and maintain extended validation certificates ("EV Certificates") concerning a subject organization. The framework accommodates a wide range of security, localization and notification requirements.	[b-EVCERT]
Policy requirements for certification authorities issuing public key certificates	The specified document specifies policy requirements relating to certification authorities (CAs) issuing public key certificates, including extended validation certificates (EVC). It defines policy requirements on the operation and management practices of certification authorities issuing and managing certificates such that subscribers, subjects certified by the CA and relying parties may have confidence in the applicability of the certificate in support of cryptographic mechanisms.	[b-ETSI TS 102 042]

Table I.6 – Techniques relevant to the exchange protocol cluster

Technique	Description	References
Real-time inter-network defense (RID)	Real-time inter-network defense (RID) provides a framework for the exchange of incident information. The RID standard provides the set of incident coordination messages necessary to communicate IODEF documents securely between entities. RID is a wrapper for IODEF documents, including any extensions of IODEF. The standard messages and exchange formats include security, privacy and policy options/considerations that are necessary in a global incident coordination scheme. RID is the security layer between IODEF documents and the transport protocol. The transport selected is decided upon by the entities communicating incident information. The transport may be the specified RID transport (HTTP/TLS), BEEP, SOAP, or a protocol specified in the future.	[b-ITU-T X.1580][b-IETF RFC 6045]
Transport of real-time inter-network defense (RID) messages	This mechanism specifies the transport of real-time inter-network defense (RID) messages within HTTP Request and Response messages transported over TLS.	[b-ITU-T X.1581][b-IETF RFC 6046]
Trusted automated exchange of indicator information	Trusted automated exchange of indicator information (TAXII) enables sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols and messages to exchange cyber threat information for the detection, prevention and mitigation of cyber threats.	[b-TAXII]
~~Blocks extensible exchange protocol (BEEP) profile for CYBEX~~	~~A BEEP profile for cybersecurity information exchange techniques specifies the BEEP profile for use within CYBEX. BEEP is a generic application protocol kernel for connection-oriented, asynchronous interactions described in [b-IETF RFC 3080]. At BEEP's core is a framing mechanism that permits simultaneous and independent exchanges of messages between peers. All exchanges occur in the context of a channel – a binding to a well-defined aspect of the application, such as transport security, user authentication, or data exchange. Each channel has an associated "profile" that defines the syntax and semantics of the messages exchanged.~~	~~[b-IETF RFC 3080]~~
~~Simple object access protocol (SOAP) for CYBEX~~	~~SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML-based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. SOAP can potentially be used in combination with a variety of other protocols; however, the only bindings defined in this document describe how to use SOAP in combination with HTTP and HTTP extension framework.~~	~~[b-W3C SOAP]~~

Appendix II

A cybersecurity information exchange ontology

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

Appendix II provides a cybersecurity information exchange ontology. This illustrates an operational context for CYBEX, and results in an effective cybersecurity ecosystem where knowledge derived from reports, testing, and experience is used to create and evolve the weakness and vulnerability information that in turn can be used, together with system state information, to measure and enhance security.

The CYBEX ontology defines the following terms:

1) **Cybersecurity operations**: Methods and processes used to monitor and manage security within defined operational limits, including:

    • the collection and analysis of information that may have an effect on security;

    • the detection of behaviour or events which adversely affect security or by which the likelihood of a future adverse effect can be determined;

    • action taken as a result of adverse behaviour or event taking place in order to limit, mitigate and/or prevent future incidents;

    • security-related communications concerning the status and condition of systems.

2) **Cybersecurity entity**: Any entity that is part of an exchange of cybersecurity information, including the information object itself.

3) **Cybersecurity operational information**: Any information that is needed for cybersecurity entities to run cybersecurity operations

The cybersecurity techniques described in CYBEX are usefully described further within this CYBEX ontology; that is, a model for describing the abstracted world of cybersecurity operations. The ontology consists of a set of types, properties, and relationships. See Figure II.1. The solid lines indicate the relationship of the information types, while arrows indicate information input from a functional entity to a knowledge base/database. The functional entities shown on the right are generic and entities such as CIRTs may encompass one or more of these functions.
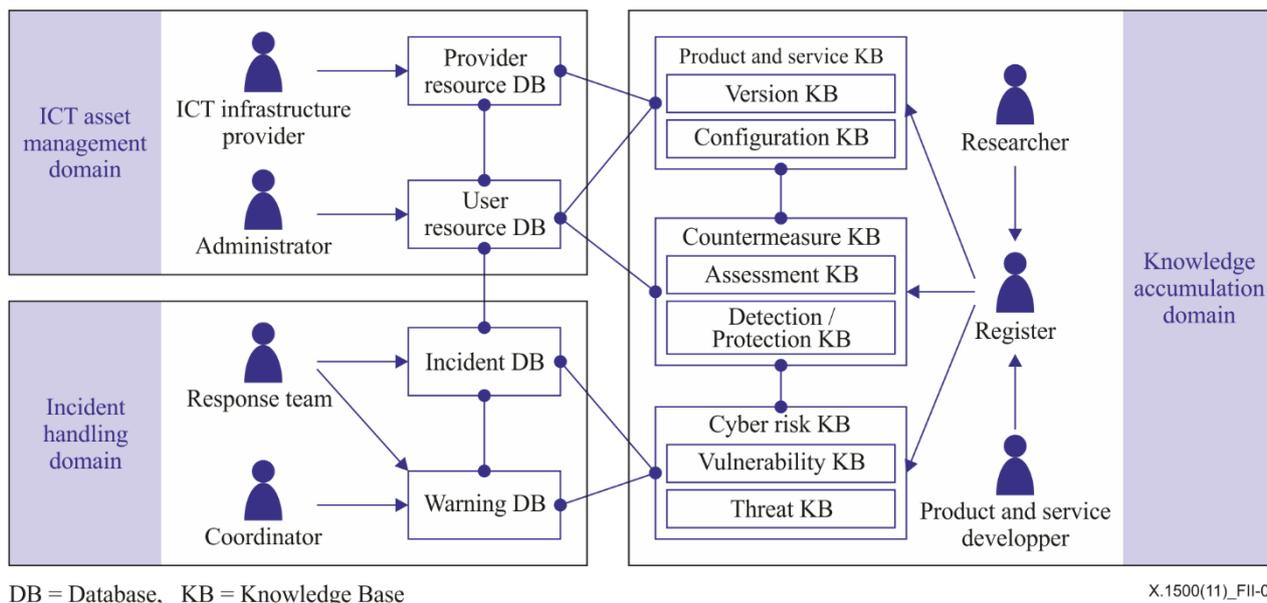
Figure II.1 – CYBEX ontology model

In this ontology, a model is used to define domains for cybersecurity operations, which is then used to identify required cybersecurity entities to support the operations in each domain. In the following clauses, a detailed ontology is derived. This illustrates how the CYBEX techniques can be used to support this ontology.

II.1 Operation domains

Cybersecurity operations principally consist of three domains: incident handling, ICT asset management and knowledge accumulation.

The incident handling domain includes detection and response to cybersecurity incidents by monitoring incidents, computer events that constitute the incidents, and attack behaviour identified in the incidents. For instance, it detects anomalies through alarms from detectors, and then assembles details by collecting various logs. Sometimes it provides alerts and advisories, e.g., early warnings against candidate threats to user organizations.

The ICT asset management domain includes cybersecurity operations within each user organization such as installing, configuring, and managing ICT assets in the organization. It includes both incident preventive operations and damage controlling operations in each organization.

The knowledge accumulation domain includes cybersecurity-related information. Reusable knowledge for other organizations is generated and accumulated.

II.2 Cybersecurity entities

Based on the operation domains described above, the cybersecurity functional entities that are necessary to run cybersecurity operations in each domain can be identified.

Within the incident handling domain, two entities exist for its operations: the response team, and the coordinator. The response team is an entity that monitors and analyses various kinds of incidents, e.g., unauthorized access, DDoS attacks and phishing, and accumulates incident information. Based on this information, a response team may implement countermeasures, e.g., register phishing site addresses on black lists. A coordinator is an entity that coordinates with the other entities and addresses potential threats based on known incident information.

In the ICT asset management domain, two operation entities exist: administrator and ICT infrastructure provider. The administrator administers the system of its organization and possesses information on its own ICT assets. An ICT administrator inside each organization is a typical instance. The ICT infrastructure provider provides each organization with ICT infrastructures, which includes the network connectivity, cloud computing services such as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), and identity services. An Internet service provider (ISP) and an application service provider (ASP) are typical instances.

In the knowledge accumulation domain, three operation entities exist: researcher, product and service developer, and registrar. A researcher researches cybersecurity information, extracting and accumulating knowledge. A product and service developer possesses information on products and services, e.g., naming, versions, their vulnerabilities, their patches and configuration information. Software vendors, ASPs and individual software programers are typical instances. A registrar is an entity that classifies and organizes cybersecurity knowledge provided by researchers, developers, and vendors so that knowledge can be used by another organization.

II.3 Cybersecurity operational information

Based on the operation domains and entities, this clause elaborates on cybersecurity operational information provided by the functional entities for each operation domain.

II.3.1 Incident handling domain

In the incident handling domain, there exist an incident database and a warning database. An incident database contains information on incidents provided by a response team. It includes three kinds of records: event, incident, and attack. An event record includes computer events such as privileged users logging into a system. It also includes information on packets, files and transactions related to incidents. Usually, most of the records are provided by computers automatically. An incident record includes events that are incident candidates. This record is usually derived from several event records and their conjectures, which are created automatically and/or manually. An attack record is based on the analyses of incidents and includes the precise date and time of the attacks as well as their sequences.

A warning database includes information on cybersecurity warnings provided by a response team and coordinator. The warnings are based on the incident database as well as the cyber risk knowledge base.

II.3.2 ICT asset management domain

In the ICT asset management domain, there are two databases: a user resource database and a provider resource database.

The user resource database accumulates information on assets within an individual organization and contains information such as the list of software, hardware, their configurations, status of resource usage, security policies including access control policies, security level assessment results, and intranet topology. The information is provided by the administrator.

The provider resource database accumulates information on assets outside the individual organization. It mainly contains external resource information and external network information. External resource information consists of information on resources that each organization is utilizing outside their organization such as the list and status of external cloud services (e.g., data centre and SaaS). The external network information consists of information on networks that connect each organization to other organizations such as their topology, routing information, access control policy, traffic status and the security level. The information is provided by the ICT infrastructure provider.

II.3.3   Knowledge accumulation domain

Three knowledge bases exist in the knowledge accumulation domain: cyber risk, countermeasure, and product and service. They accumulate knowledge on cybersecurity provided by the researcher and product and service developer, which is then organized and classified by the registrar.

The cyber risk knowledge base accumulates cybersecurity risk information and includes vulnerability knowledge and threat knowledge. The vulnerability knowledge base accumulates known vulnerability information, including naming, taxonomy and enumeration of known vulnerabilities. It also includes human vulnerabilities exposed by human ICT users. The threat knowledge base accumulates known threat information that includes attack knowledge and misuse knowledge. Attack knowledge includes information on attack patterns, attack tools (e.g., malware) and their trends such as the information on past attack trends in terms of geography and attack target. It also includes statistical information about past attacks. Misuse knowledge includes information about misuses of ICT caused by human users without any malicious intention. Information of mistyping, being caught by phishing traps, and compliance violations are included.

The countermeasure knowledge base accumulates information on countermeasures to cybersecurity risks and contains two knowledge bases: assessment and detection/protection. The assessment knowledge base accumulates known rules and criteria for assessing the security level of ICT assets as well as the checklist of configurations. The detection/protection knowledge base accumulates known rules and criteria for detecting/protecting security threats, for example, IDS/IPS signatures and related detection/protection rules.

The product and service knowledge base accumulates information on products and services. It includes two knowledge bases: version knowledge and configuration knowledge. The version knowledge base accumulates version information on products and services, including naming and enumeration of their versions. Regarding product version, security patches are also included within the knowledge base. The configuration knowledge base accumulates configuration information on products and services. Regarding product configuration, it includes naming, taxonomy and enumeration of known configurations.

Each of the databases and knowledge bases mentioned above may utilize various information description techniques as shown in Figure II.2.
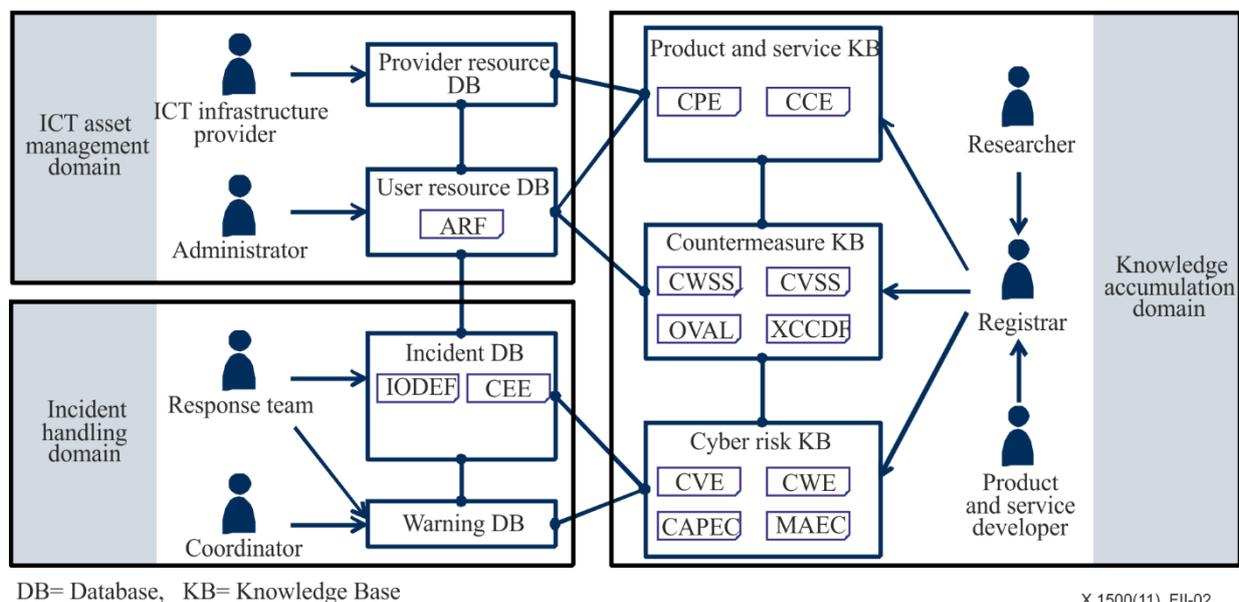

Figure II.2 – Detailed view of the CYBEX ontology model with techniques shown

For further information on CYBEX ontology, see [b-Takahashi].

Appendix III

CYBEX examples of security automation schemas

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

Appendix III provides two examples of security automation schemas. These capabilities can be used for creating specific CYBEX instantiations that include automating known secure or trusted "states" of software, services, and systems, detecting malware, capturing incident and heuristics information.

It is expected that a large number of implementations will emerge – particularly a security automation schema for ensuring that ICT systems are properly configured and patched. Two initial prominent examples include:

1)   The USA National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) for implementing the Desktop Core Configuration (FDCC) and its replacement, the United States Government Configuration Baseline (USGCB), and

2)   The Japan JVN Security Content Automation Framework.

Each of these is briefly described in this appendix. In general, these security automation tool implementations take the form shown in Figure III.1, and include various numbers of the CYBEX information exchange platforms represented by the overlay pointers in the diagram.
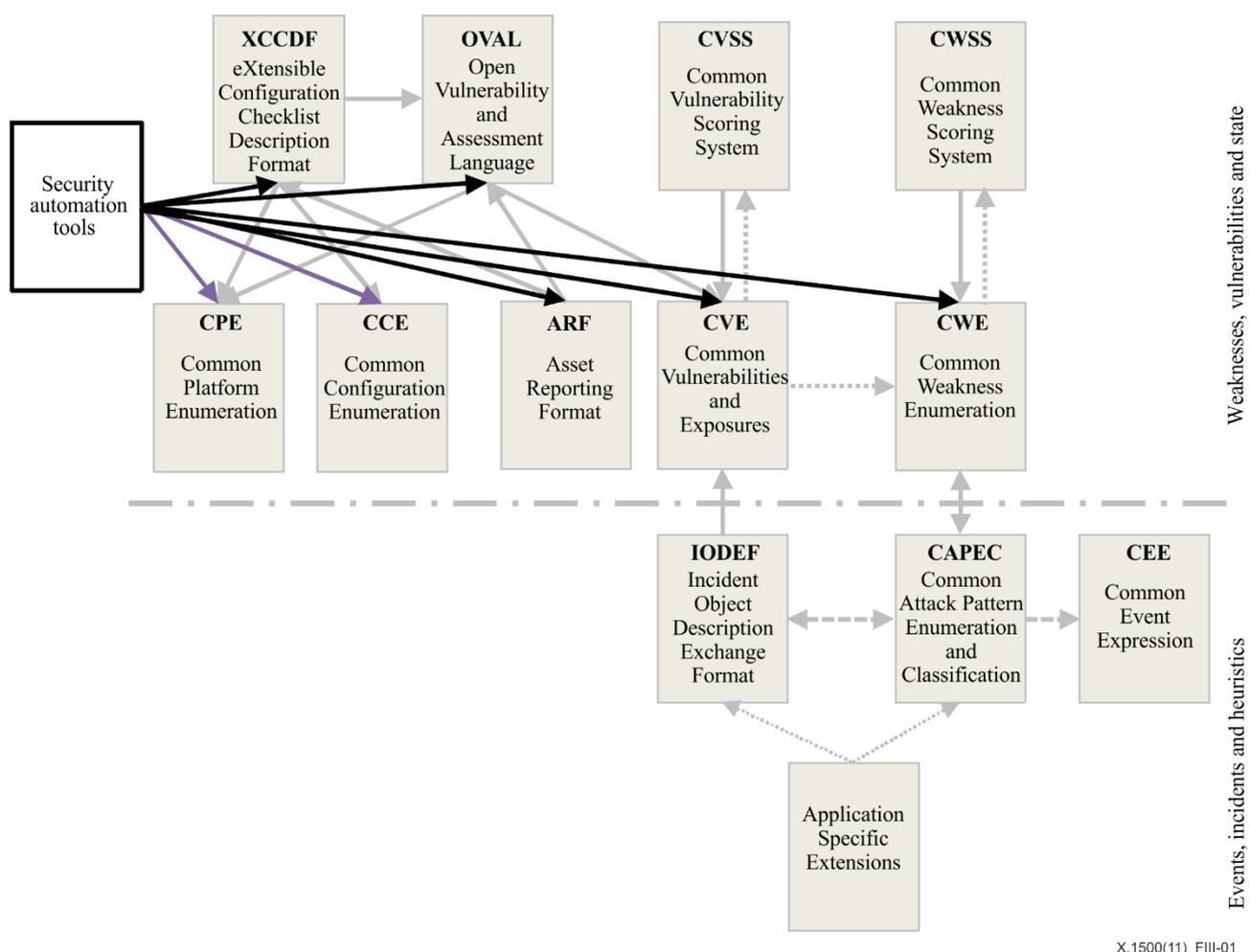

Figure III.1 – Cybersecurity assurance and integrity automation

III.1 Example: USA Federal Desktop Core Configuration/United States Government Configuration Baseline

The Federal Desktop Core Configuration (FDCC) and its replacement, the United States Government Configuration Baseline (USGCB), using the NIST Security Content Automation Protocol (SCAP) comprises specifications for organizing and expressing security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities. The purpose of these two initiatives is to create security configuration baselines for ICT products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain effective configuration settings focusing primarily on security.

The USGCB technical specification describes the requirements and conventions that are to be employed to ensure the consistent and accurate exchange of SCAP content and the ability of the content to reliably operate on SCAP validated tools. The initial version is comprised of six specifications: XCCDF, OVAL, CPE, CCE, CVE, and CVSS. These specifications are grouped into three categories: languages, enumerations, and vulnerability measurement and scoring systems.

SCAP implements 1) a specified format and nomenclature by which security software products communicate software flaw and security configuration information, and 2) specific software flaw and security configuration standard reference data known as SCAP content. Goals for SCAP include standardizing system security management, promoting interoperability of security products, and fostering the use of standard expressions of security content. Because many different SCAP contents are likely to emerge for diverse systems and levels of security, the structured tagging, discovery, and assurance verification of current schema are important requirements. The USGCB initiative creates content and guidance based on the SCAP specifications.

### III.2 Example: Japan vulnerability information portal site, JVN

JVN stands for "Japan Vulnerability Notes" and provides vulnerability and related information on software used in Japan, with which it intends to contribute to the countermeasure to cyber threats. In order to enable application developers to use data through an open interface, JVN has adopted SCAP and contains local (domestic) information and international information, resulting in the JVN security content automation framework. Just like the National Vulnerability Database (NVD), each of the vulnerability information contains a CVE number, provides a CVSS score, and a CWS number. Moreover, the CPE name of the affected product is also provided.

The framework consists of three components: MyJVN, JVN, and JVN iPedia (see Figure III.2), each of which is elaborated below.

MyJVN provides vulnerability countermeasure information via MyJVN API, a machine-readable interface including web APIs, and the MyJVN tools such as the Version Checker. It improves the usage of vulnerability countermeasure information stored in JVN and JVN iPedia by making it easier and more efficient for users to collect their target information through services such as customized filtering, auto searching and checklist creation. Also, "MyJVN Version Checker," a tool based on SCAP, allows people to easily check whether the software installed on their PC is the latest version.

JVN provides vulnerability countermeasure information and Japanese vendor status for reported vulnerabilities by the "Information Security Early Warning Partnership", which is a public-private partnership framework that has been established to promote software product and website security, and prevent damage to spread to the vast range of computers due to computer viruses or unauthorized access. When the vulnerability information is reported to IPA (Information-technology Promotion Agency, Japan) as the recipient body of this partnership, it is passed to the JPCERT/CC as a coordination body. JPCERT/CC specifies the affected software products and coordinates with developers. When solutions for vulnerabilities such as patches or software updates are available for users, the vulnerability details with developers' statements are published on JVN.

JVN iPedia provides vulnerability countermeasure information collected on software products, such as operating systems, applications, libraries and embedded systems, used in Japan. JVN aims to offer the vulnerability and countermeasure information to the public as soon as possible. A coordination body interacts with the vendors regarding when to disclose new reported vulnerabilities. The JVN iPedia mission, on the other hand, aims to collect additional vulnerability and countermeasure information found on a daily basis on Japanese software products that are not released on JVN.
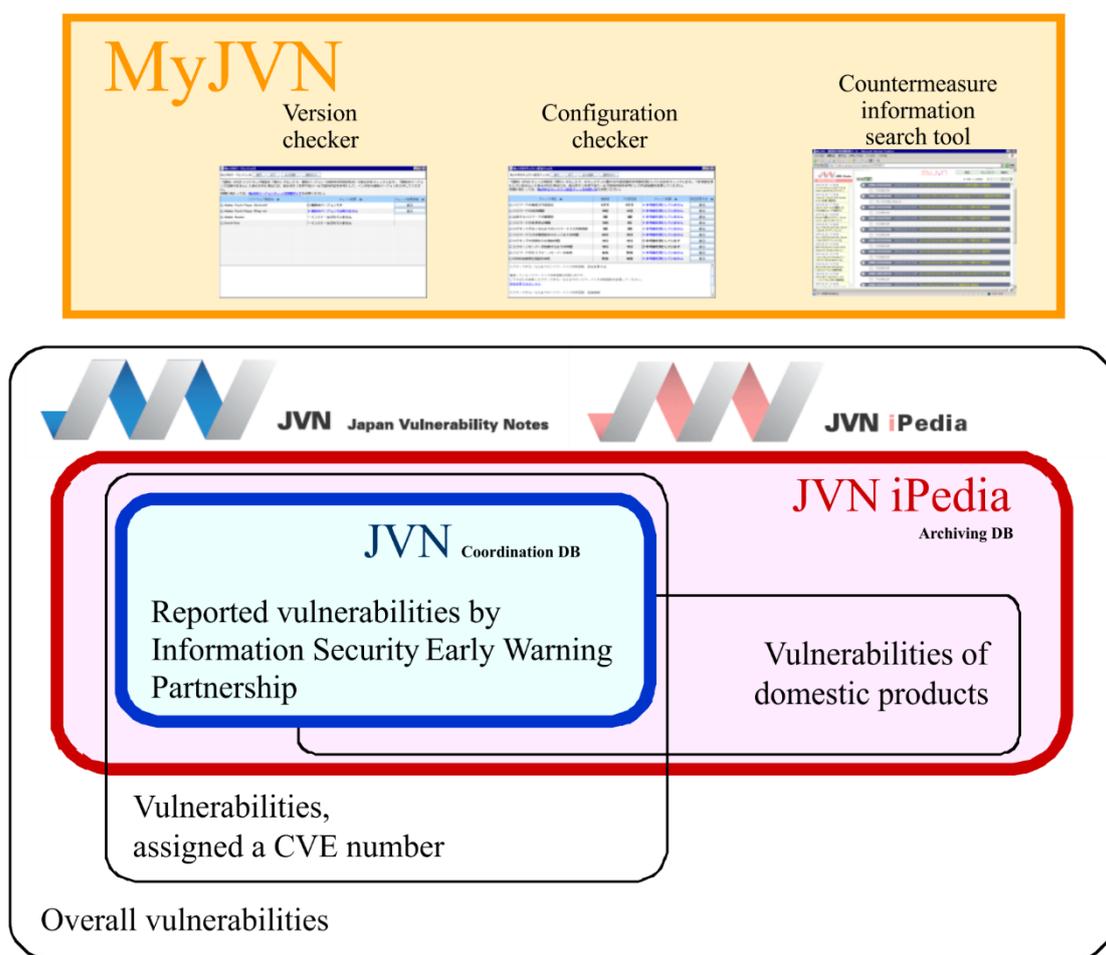
X.1500(11)_FIII-02

Figure III.2 – Concept of the JVN security content automation framework
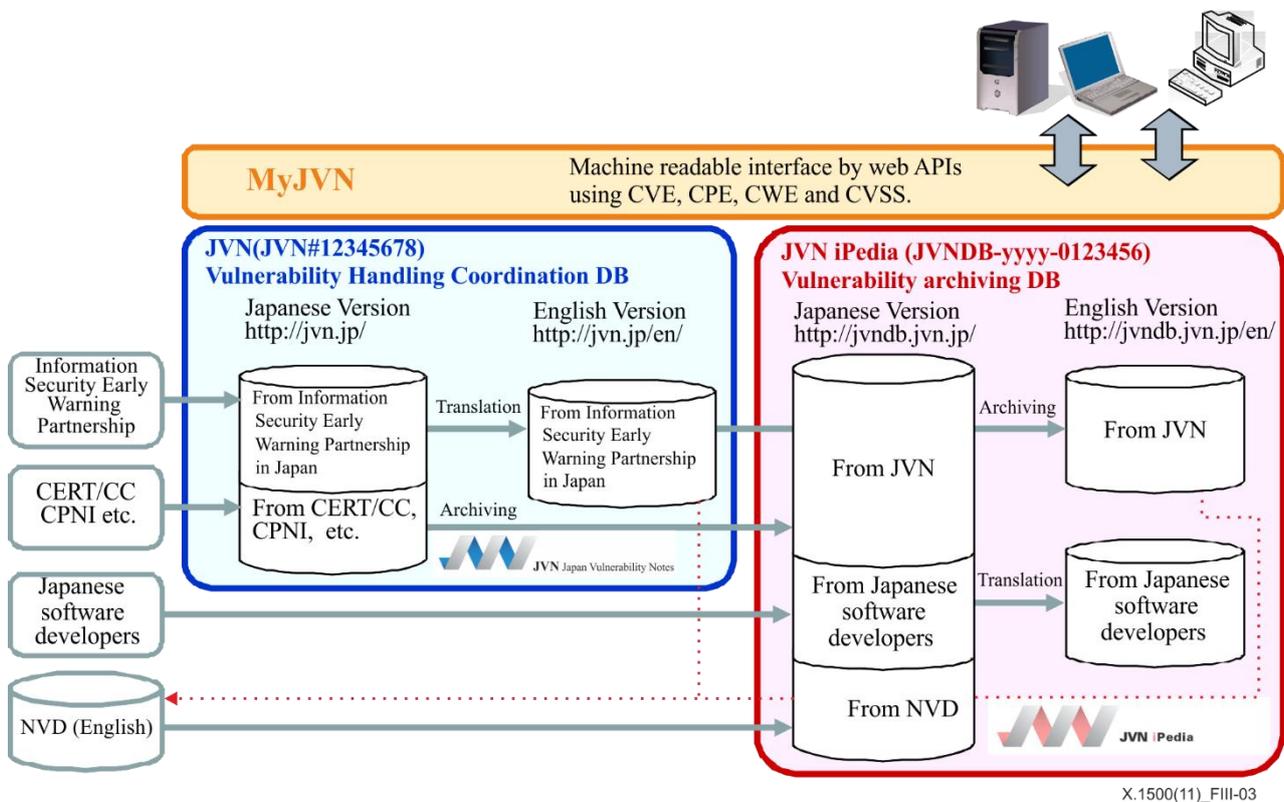
Figure III.3 – Database with international and local information

Users adopting standard formats such as RSS may enjoy a database that contains international and local information (see Figure III.3). Among the three components, MyJVN works as a user interface, whose usability is facilitated with the following tools and APIs.

MyJVN tools and API

The MyJVN tools are security tools based on SCAP that improve the usage of vulnerability countermeasure and information exchange environment for users. The major tools currently offered are:

- **Filtered Vulnerability Countermeasure Information Tool** – This tool improves the usage of vulnerability countermeasure information stored in JVN and JVN iPedia by making it easier and more efficient for users to collect their target information through services such as customized filtering by CPE.

- **Version Checker** – Version checker is an OVAL based online scanner that allows people to easily check whether the software installed on their PC is the latest version. With just one mouse click, people can check the versions of several software modules. The results are easy to understand: a tick mark signifies the latest version and a cross mark signifies an obsolete version. If the software is not the latest version, users can easily access the vendor's download website with just a few clicks. MyJVN version checker supports Internet-related software products that were selected seeking cooperation from software vendors.

- **MyJVN Security Configuration Checker** – This is an XCCDF and OVAL based online scanner. It is a free, easy-to-use tool to assess the Windows security configuration, including account policies such as the minimum password length, password expiration period, automatic turn-on of screensaver, the USB autorun feature, etc.

- **MyJVN API** – This API is a software interface to access and utilize vulnerability countermeasure information stored in JVN and JVN iPedia. To enable application developers to use data through an open interface, JVN iPedia has adopted SCAP, a set of standards for describing vulnerability countermeasure information. By using MyJVN API, any custom applications can access the data in JVN iPedia and various vulnerability management services can now efficiently utilize vulnerability countermeasure information.

  Basic functions of MyJVN API are a filtered information service API and SCAP collaboration service API. The former API supports "Get list of products", "Get list of vulnerability overviews" etc., which are used by the Filtered Vulnerability Countermeasure Information Tool. The latter API supports "Get list of OVAL definitions", "Get data of OVAL definition", etc., which are used by the MyJVN Version Checker and the MyJVN Security Configuration Checker.

  For further information on JVN, please refer to the article [b-Terada].

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework*.

[b-ITU-T X.1500.1] Recommendation ITU-T X.1500.1 (2012), *Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange*

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (20112004), *Common vulnerabilities and exposures (CVE)*.

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (20112016), *Common vulnerability scoring system 3.0*.

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

[b-ITU-T X.1525] Recommendation ITU-T X.1525 (2015), *Common weakness scoring system*.

[b-ITU-T X.1526] Recommendation ITU-T X.1526 (2014), *Language for the open definition of vulnerabilities and for the assessment of a system state*.

[b-ITU-T X.1528] Recommendation ITU-T X.1528 (2012), *Common platform enumeration*.

[b-ITU-T X.1528.1] Recommendation ITU-T X.1528.1 (2012), *Common platform enumeration naming*.

[b-ITU-T X.1528.2] Recommendation ITU-T X.1528.2 (2012), *Common platform enumeration matching*.

[b-ITU-T X.1528.3] Recommendation ITU-T X.1528.3 (2012), *Common platform enumeration dictionary*.

[b-ITU-T X.1528.4] Recommendation ITU-T X.1528.4 (2012), *Common platform enumeration applicability language*.

[b-ITU-T X.1541] Recommendation ITU-T X.1541 (2012), *Incident object description exchange format*.

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

[b-ITU-T X.1546] Recommendation ITU-T X.1546 (2014), *Malware attribute enumeration and characterization*.

[b-ITU-T X.1570] Recommendation ITU-T X.1570 (2011), *Discovery mechanisms in the exchange of cybersecurity information*.

[b-ITU-T X.1580] Recommendation ITU-T X.1580 (2012), *Real-time inter-network defense*.

[b-ITU-T X.1581] Recommendation ITU-T X.1581 (2012), *Transport of real-time inter-network defense messages*.

[b-ETSI TS 102 042] ETSI TS 102 042 (2011), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*.

[b-IETF RFC 3080]   IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*.
http://datatracker.ietf.org/doc/rfc3080/

[b-IETF RFC 5070]   IETF RFC 5070 (2007), *The Incident Object Description Exchange Format*.
http://datatracker.ietf.org/doc/rfc5070/

[b-IETF RFC 5901]   IETF RFC 5901 (2010), *Extensions to the IODEF-Document Class for Reporting Phishing*.
http://datatracker.ietf.org/doc/rfc5901/

[b-IETF RFC 6045]   IETF RFC 6045 (2010), *Real-time Inter-network Defense (RID)*.
http://datatracker.ietf.org/doc/rfc6045/

[b-IETF RFC 6046]   IETF RFC 6046 (2010), *Transport of Real-time Inter-network Defense (RID) Messages*.
http://datatracker.ietf.org/doc/rfc6046/

[b-IETF RFC 6120]   IETF RFC 6120 (2011), *Extensible Messaging and Presence Protocol (XMPP): Core*.
http://datatracker.ietf.org/doc/rfc6120/

[b-IETF RFC 6698]   IETF RFC 6698 (2012), T*he DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA*.
https://datatracker.ietf.org/doc/rfc6698/

[b-IETF RFC 7203]   IETF RFC 7203 (2014), *An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information*.
https://datatracker.ietf.org/doc/rfc7203/

[b-IETF RFC 8322]   IETF RFC 8322 (2018), Resource-Oriented Lightweight Information Exchange (ROLIE).
https://datatracker.ietf.org/doc/rfc8322/

[b-ISO/IEC 15026]   ISO/IEC 15026-2:2011, *Systems and software engineering – Systems and software assurance – Part 2: Assurance case*.

[b-ISO/IEC 19770-2] ISO/IEC 19770-2:2015, *Information technology – Software asset management – Part 2: Software identification tag*.

[b-ISO/IEC 20004]   ISO/IEC TR 20004:2015, *Information Technology – Security Techniques – Refining Software Vulnerability Analysis under ISO/IEC 15408 and ISO/IEC 18045*.

[b-ISO/IEC 24772]   ISO/IEC TR 24772:2013, *Information technology – Programming languages – Guidance to avoiding vulnerabilities in programming languages through language selection and use*.

[b-ISO/IEC 27034]   ISO/IEC 27034-1:2011, *Information Technology – Security Techniques – Application security – Part 1: Overview and concepts*.

[b-ISO/IEC 27036]   ISO/IEC 27036-1:2014, *Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts*.

[b-ISO/IEC 29147]   ISO/IEC 29147:2014, *Information Technology – Security Techniques – Vulnerability Disclosure*.

[b-A2]   Terada, M. et al. (2009), *Proposal of MyJVN (Web Service APIs) for Security Information Exchange infrastructure*, 21st Annual FIRST Conference, June 2009.
http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/21thFirstConference_paper.pdf

[b-ARF]   Assessment Results Format. https://measurablesecurity.mitre.org/incubator/arf/

[b-CAPEC]   Common Attack Pattern Enumeration and Classification.
https://capec.mitre.org/

[b-CCE]	Common Configuration Enumeration. https://cce.mitre.org/
[b-CSC]	ETSI TR 103 305 (2016), *CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls.* http://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/02.01.01_60/tr_10330501v020101p.pdf
[b-CybOX]	Cyber Observable eXpression. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
[b-EVCERT]	CA/Browser Forum (2018), *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* Version 1.5.6. https://cabforum.org/baseline-requirements-documents/
[b-MMDEF]	*Malware Metadata Exchange Format*, IEEE ICSG Malware Metadata Exchange Format Working Group, https://standards.ieee.org/develop/indconn/icsg/mmdef.html
[b-NIST 800-53]	National Institute of Standards and Technology, Special Publication 800-53 Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*", Joint Task Force Transformation Initiative, Computer Security Division Information Technology Laboratory, January 2015. http://csrc.nist.gov/publications/PubsSPs.html. See also, https://web.nvd.nist.gov/view/800-53/home
[b-OMG ASCSM]	OMG Specification ASCSM 1.0 (12/14), *Automated Source Code Security Measure*. OMG, 2014.
[b-OG O-DA]	Open Group O-DA, *Dependability through Assuredness (O-DA) Framework*, Open Group. ISBN 1-937218-36-2, July 2013.
[b-OG O-TTPS]	Open Group O-TTPS, Version 1.1 *Mitigating Maliciously Tainted and Counterfeit Products – Open Trusted Technology Provider Standard*, Open Group. ISBN 1-937218-55-3, July 2014.
[b-OMG SACM]	OMG Specification SACM 2.0 (06/16), *Structured Assurance Case Metamodel*. OMG, 2016.
[b-OMG SMM]	OMG Specification SMM 1.1.1 (04/16), *Structured Metrics Meta-Model*. OMG, 2016.
[b-OMG SPMS]	OMG Specification SPMS 1.1 (06/16), *Structured Patterns Metamodel Standard*. OMG, 2016.
[b-STIX]	Structured Threat Information eXpression. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
[b-Takahashi]	Takahashi, T., Kadobayashi, Y. Reference Ontology for Cybersecurity Operational Information, *The Computer Journal*, doi: 10.1093/comjnl/bxu101, October, 2014
[b-TAXII]	Trusted Automated eXchange of Indicator Information. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
[b-TEE]	Trusted Execution Environment (TEE) Specifications, GlobalPlatform. https://www.globalplatform.org/specificationsdevice.asp
[b-TLP]	Traffic Light Protocol (TLP), Forum of Incident Response and Security Teams. https://www.first.org/tlp
[b-TNC]	Trusted Computing Group. Network Equipment http://www.trustedcomputinggroup.org/developers/trusted_network_communications.
[b-TPM]	Trusted Platform Module Specifications. Trusted Computing Group. http://www.trustedcomputinggroup.org/developers/trusted_platform_module

[b-XCCDF]	XCCDF – The Extensible Configuration Checklist Description Format, http://scap.nist.gov/specifications/xccdf/. XCCDF has also been adopted as, ISO/IEC 18180 (2013), *Information technology – Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2.*

[b-XEP-0060]	XMPP Standards Foundation, XEP-0060 (2010), *Publish-Subscribe.*

[b-CEE]	Common Event Expression. https://cee.mitre.org/

[b-CPE]	Common Platform Enumeration. https://cpe.mitre.org/

[b-CWE]	Common Weakness Enumeration. https://cwe.mitre.org/

[b-CWSS]	Common Weakness Scoring System. https://cwe.mitre.org/cwss/

[b-EVCERT]	CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3

[b-MAEC]	Malware Attribute Enumeration and Characterization. https://maec.mitre.org/

[b-NIST EAA]	*Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.2, April 2006

[b-OVAL]	Open Vulnerability and Assessment Language. https://oval.mitre.org/

[b-Takahashi]	Takahashi, T., Kadobayashi, Y., and Fujiwara, H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks, September.

[b-Terada]	Terada, Masato, et al. (2009), *Proposal of MyJVN (Web Service APIs) for Security Information Exchange infrastructure*, 21st Annual FIRST Conference on Computer Security Incident Handling, June. http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/21thFirstConference_paper.pdf

[b-TLP]	*CPNI Traffic Light Protocol* (2010), Information Sharing Levels, CPNI Information Exchange, UK, April.

[b-TNC]	Trusted Computing Group, *Trusted Network Connect.*

	Integrity Measurement Collectors – TCG Version (IF-IMC, Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)

	Integrity Measurement Verifiers – TCG Version (IF-IMV Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)

	Trusted Network Connect Client-Server – TCG Version (IF-TNCCS TLV Binding Specification Ver. 2.0 Rev. 16, 22 Jan. 2010)

	Trusted Network Connect Client-Server Statement of Health – TCG Version (IF-TNCCS-SOH TLV Binding Specification Ver. 2.0 Rev. 10, 23 Jan. 2008)

	Policy Enforcement Point – TCG Version (IF-PEP Protocol Bindings for RADIUS Specification Ver. 1.1 Rev. 0.7, 5 Feb. 2007)

	Binding for SOAP – TCG Version (IF-MAP Specification Ver. 2.0 Rev. 36, 30 July 2010)

	Platform Trust Services Interface – TCG Version (IF-PTS Specification Ver. 1.0 Rev. 1.0, 17 Nov. 2006)

	Clientless Endpoint Support Profile – TCG Version (CESP Specification Ver. 1.0 Rev. 13, 18 May 2009)

[b-TPM]   Trusted Computing Group, *Trusted Platform Modules*.

Design Principles – TCG Version (TPM Main, Part 1, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-2, 2009-05-15, Information technology – TPM – Part 2)

TPM Structures – TCG Version (TPM Main, Part 2. Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-3, 2009-05-15, Information technology – TPM – Part 3)

Commands – TCG Version (TPM Main, Part 3, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-4, 2009-05-15, Information technology – TPM – Part 4)

The TPM 1.2 specifications have also been adopted as ISO/IEC 11889. Overview – TCG Version (N/A), ISO/IEC Version (11889-1, 2009-05-15, Information technology – TPM – Part 1)

[b-W3C SOAP]   W3C Recommendation Simple Object Access Protocol (SOAP), 2007.

SOAP Version 1.2 Part 1: Messaging Framework.

SOAP Version 1.2 Part 2: Adjuncts.

[b-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