International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1500
Amendment 8
(09/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Overview of cybersecurity

---

Overview of cybersecurity information exchange

Amendment 8: Revised structured cybersecurity information exchange techniques

Recommendation ITU-T X.1500 (2011) – Amendment 8

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
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 8

Revised structured cybersecurity information exchange techniques

Summary

Amendment 8 to Recommendation ITU-T X.1500 (2011) 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 September 2015, 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

* 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/.

Recommendation ITU-T X.1500

Overview of cybersecurity information exchange

Amendment 8

Revised structured cybersecurity information exchange techniques

1) *Replace Appendix I with the appendix below.*

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	[b-ITU-T X.1521]

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

Technique	Description	References
	vendors and researchers to all benefit by adopting a common language of scoring ICT vulnerabilities.	
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.1524]
Common weakness scoring system (CWSS)	The common weakness scoring system (CWSS) provides an open framework for communicating the characteristics and impacts of 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.1525]
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 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 for testing, analysing the endpoint 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 language. These schemas correspond to the three steps of the assessment process: an OVAL system characteristics schema for representing endpoint information, an OVAL definition schema for expressing a specific machine state and an OVAL results schema for reporting the results of an assessment.	[b-ITU-T X.1526]

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

Technique	Description	References
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]
Software identification tag	Software identification tags (SWID tags) record unique information about an installed software application, including its name, edition, version, whether it's part of a bundle and more. 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]

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

Technique	Description	References
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 commonly exchanged information about computer security incidents. IODEF describes an information model and provides an associated data model specified with XML schema.	[b-ITU-T X.1541]

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

Technique	Description	References
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 Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information	This document extends the Incident Object Description Exchange Format (IODEF) defined in RFC 5070 to exchange enriched cybersecurity information among security experts at organizations and 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]
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 standardized schema for the specification, capture, characterization and communication of events or stateful properties that are observable in the operational domain. 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) language includes enumerations of malware attributes and behaviour that provide a common vocabulary. These enumerations are at different levels of abstraction: low-level observables, mid-level behaviours and high-level taxonomies. MAEC focuses on the creation of the enumeration of low-level malware attributes, and leverages the few instances of similar work already done in this area. Thus it will initially be capable of characterizing the most common malware types, including Trojans, worms and rootkits, but will ultimately be applicable to more esoteric malware types.	[b-ITU-T X.1546]

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

Technique	Description	References
Structured Threat Information eXpression (STIX)	STIX is a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information. The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable and as human-readable as possible.	[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 behavioural functionality, as well as facilitating the exchange of such information across various entities.	[b-MMDEF]

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]

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

Technique	Description	References
Resource-oriented lightweight indicator exchange	The resource-oriented lightweight indicator exchange (ROLIE) defines a resource-oriented approach to cyber security information sharing. Using this approach, a CSIRT or other stakeholder may share and exchange representations of cyber security incidents, indicators and other related information as web-addressable resources. The transport protocol binding is specified as HTTP(S) with a MIME media type of Atom+XML. An appropriate set of link relation types specific to cyber security information sharing is defined.	[b-ROLIE]
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]

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. 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,	[b-TPM]

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

Technique	Description	References
	including 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]
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]
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]
Trusted automated exchange of indicator information	Trusted Automated eXchange of Indicator Information (TAXII) defines a set of services and message exchanges that, when implemented, enable 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]

2) *Replace the bibliography with the bibliography below*:

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 (2014), *Common vulnerabilities and exposures.*

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system.*

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

[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-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 (2009), *Information technology – Software asset management – Part 2: Software identification tag.*

[b-ISO/IEC 20004] ISO/IEC TR 20004-1:2012, *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-CCE] Common Configuration Enumeration.
https://cce.mitre.org/

[b-CybOX] Cyber Observable eXpression.
<https://cybox.mitre.org/>

[b-EVCERT] CA/Browser Forum (2011), *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* Version 1.0.
http://www.cabforum.org/Baseline_Requirements_V1.pdf

[b-MMDEF] *Malware Metadata Exchange Format*, IEEE ICSG Malware Metadata Exchange Format Working Group.

[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, April 2013.

[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 1.0 (02/13), *Structured Assurance Case Metamodel*. OMG, 2013.

[b-OMG SMM] OMG Specification SMM 1.0 (01/12), *Structured Metrics Meta-Model*. OMG, 2012.

[b-OMG SPMS] OMG Specification SPMS 1.0 (09/14), *Structured Patterns Metamodel Standard*. OMG, 2014.

[b-ROLIE] IETF Internet Draft, *Resource-Oriented Lightweight Indicator Exchange* (2014), draft-ietf-mile-rolie-00.txt.

[b-STIX] Structured Threat Information eXpression.
<https://stix.mitre.org/>

[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://taxii.mitre.org/

[b-TEE] Trusted Execution Environment (TEE) Specifications, GlobalPlatform.
https://www.globalplatform.org/specificationsdevice.asp

[b-TLP] Traffic Light Protocol (TLP), United States Computer Emergency Readiness Team (US-CERT).
http://www.us-cert.gov/tlp/

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

Clientless Endpoint Support Profile (2009), TCG Trusted Network Connect, Clientless Endpoint Support Profile: *Specification ver. 1.0, Rev. 13.*

Federated TNC (2009), TCG Trusted Network Connect, Federated TNC: *Specification ver. 1.0, Rev. 26*.

Integrity Measurement Collector Interface (2013), TCG Trusted Network Connect, *IF-IMC: Specification ver. 1.3, Rev. 18.*

Integrity Measurement Verifier Interface (2013), TCG Trusted Network Connect, *IF-IMV: Specification ver. 1.4, Rev. 10.*

Metadata for Network Security (2012), TCG Trusted Network Connect, *TNC IF-MAP Metadata for Network Security, Specification ver. 1.1, Rev. 8.*

Network Authorization Transport Interface (2009), TCG Trusted Network Connect, *TNC IF-T: Binding to TLS, Specification ver. 1.0, Rev. 16.*

Policy Enforcement Point Interface (2007), TCG Trusted Network Connect, *IF-PEP: Protocol Bindings for RADIUS, Specification ver. 1.1, Rev. 0.7.*

TNC Architecture for Interoperability (2012), TCG Trusted Network Connect, *TNC Architecture for Interoperability, Specification Version 1.5, Rev. 3.*

Trusted Network Connect Client-Server Interface (2010), TCG Trusted Network Connect, *IF-TNCCS TLV: Binding, Specification ver. 2.0, Rev. 20.*

Vendor-Specific IMC/IMV Messages Interface (2010), TCG Trusted Network Connect, *TNC IF-M: TLV Binding, Specification ver. 1.0, Rev. 40.*

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

Commands (2007), TCG Version: TPM Main, Part 3, Specification ver. 1.2, Level 2 Rev. 116.
ISO/IEC 11889-4:2009, *Information technology – Trusted Platform Module – Part 4: Commands*.

Design Principles (2007), TCG Version: TPM Main, Part 1, Specification ver. 1.2, Level 2 Rev. 103.
ISO/IEC 11889-2:2009 *Information technology – Trusted Platform Module – Part 2: Design principles*.

The TPM 1.2 specifications have also been adopted as:
ISO/IEC 11889-1:2009, *Information technology – Trusted Platform Module – Part 1: Overview*.

TPM Structures (2007), TCG Version: TPM Main, Part 2. Specification ver. 1.2, Level 2 Rev. 116.
ISO/IEC 11889-3:2009, *Information technology – Trusted Platform Module – Part 3: Structures*.

[b-XCCDF] 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.

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	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015