INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 0503 Rev.1

English only

Original: English

Question(s): 4/17 Geneva, 16-25 September 2009

TEMPORARY DOCUMENT

Source: Q.4/17 Rapporteur

Title: Proposed initial draft text for Rec. ITU-T X.cybex, Cybersecurity information exchange framework

TSB Note: Please note that further to the SG 17 meeting the acronym for this Recommendation was changed from X.cybief to X.cybex.

Introduction

The annex to this document is the initial draft text that is the culmination of more than six months work by participants in the work of Q.4/17 and its Correspondence Group on Trusted Exchange of Network Digital Forensics that was approved as a new work item by Q.4 and edited at the meeting. The editors designated for the subsequent progress of the Recommendation are (in alphabetical order): Inette Furey (DHS), Youki Kadobayashi (NICT), Bob Martin (Mitre), Angela Mckay (Microsoft), Damir Rajnovic (FIRST), Gavin Reed (Cisco), Tony Rutkowski (Yaana), Gregg Schudel (Cisco), Craig Schultz (LAC). The number and diversity of the editors reflects the importance of this Recommendation. Because of the volume and significance of this work, Q4/17 is also seeking creation of a Correspondence Group for the Coordination of the Cybersecurity Information Exchange Framework Work Items. This will provide an expanded opportunity for interested parties to participate in advancing this work and being aware of all new developments.

This annex was taken from TD0460 - as revised and approved at the meeting.

The international community will gain significantly if the Cybersecurity Information Exchange Framework is adopted as an ITU-T Recommendation by significantly enhancing global cybersecurity.

Contact: Tony Rutkowski Tel: +1 408 854 8041
Q.4/17 Rapporteur Email: tony@yaanatech.com

X.cybex

Recommendation ITU-T X.cybex
Cybersecurity Information Exchange Framework

Summary

This Recommendation addresses an essential cybersecurity capability – a common framework for providers and cybersecurity centers to exchange cybersecurity related information in a structured and trusted way. This exchange may occur locally or globally among all kinds of communities and entities. The framework is shown in the following simple diagram.

This approach enables coherent, comprehensive, global, timely and trusted exchange of cybersecurity information using identified specifications and providing for their global use and information interoperability by

- identifying and incorporating existing significantly used platform standards
- as necessary, making the existing standards more global and interoperable
- providing extensible means for adapting to new exchange requirements and capabilities

In so doing, it moves beyond guidelines and facilitates the scaling and broad implementation, on a potentially measurable basis, of core capabilities already developed within existing insular cybersecurity communities. The framework also includes cloud computing, and can be easily applied to new sectors such as SmartGrid and eHealth cyberecurity.

The Recommendation provides for this objective via a framework that allows for continual evolution to accommodate the significant activities and specification evolution occurring in numerous cybersecurity forums, and consists of a basic exchange framework with three extensible functions:

- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- trusted exchanging of cybersecurity information over networks

The means of initially acquiring this information prior to the actual exchange of that information, as well as the use of this information, are generally out of scope of the Recommendation. The objective of the Recommendation is trusted information exchange. However, the framework does allow for programmatic expressions that request information.

These functions are organized into several exchange “clusters” for distinct cybersecurity user groups and requirements :

- Vulnerability/mitigation exchange
- Event/incident/heuristics exchange
- LEA/evidence exchange
- Cybersecurity organization identity and trust
- Cybersecurity heuristics and information request

This Framework provides an implementation of the many guidelines, practices and requirements found in the Appendix materials, which are included for reference.

X.cybex

Candidate Recommendation ITU-T X.cybex

Cybersecurity Information Exchange Framework

Table of Contents

History

Sep 2009. Initial draft

RECOMMENDATION ITU-T X.cybex

Cybersecurity Information Exchange Framework

1. Scope

Enable coherent, comprehensive, global, timely, and trusted exchange of cybersecurity information, and providing for the structured global discovery and interoperability of that information in a framework that allows for continual evolution to accommodate the significant activities and specification evolution occurring in numerous cybersecurity forums, including cloud computing and new applications such as SmartGrid and eHealth cybersecurity.

Scope of the framework includes an information exchange model with three functions

- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- trusted exchanging of cybersecurity information over networks

The means of initially acquiring this information prior to the actual exchange of that information, as well as the use of this information, are generally out of scope of the Recommendation.

Related guidelines, practices, and similar kinds of material related to the exchange of cybersecurity information are provided for reference.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

3. Definitions

Computer Security Incident Response Team: a team of IT security experts whose main responsibility is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches. In order to mitigate risks and minimise the number of required responses, most CSIRTs also provide preventative and educational services for their constituency. They issue advisories on vulnerabilities in the software and hardware in use, and also inform the users about exploits and viruses taking advantage of these flaws. The term *Computer Emergency Response Team (CERT)* is a precursor synonym for CSIRT.

Cybersecurity entity: any entity possessing or seeking cybersecurity information

Cybersecurity information: structured information or knowledge concerning

1. The “state” of equipment, software or network based systems as related to cybersecurity, especially vulnerabilities
2. Forensics related to incidents or events
3. Heuristics and signatures gained from experienced events
4. Parties who implement cybersecurity information exchange capabilities within the scope of this framework
5. Specifications for the exchange of cybersecurity information, including modules, schemas, and assigned numbers
6. The identities and trust attributes of all of the above
7. Implementation requirements, guidelines and practices

National CERT: a CSIRT operated or designated by and for a national Administration.

Protocol: [ITU-T Rec. X.200]

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

Exchange Protocol: A set of rules and associated behavior governing the exchange of information between two or more computer systems via a network. An Exchange Protocol may employ authentication and/or authentication of authorization during the initiation of the exchange which may allow or disallow the exchange to take place.

Transport Protocol: A set of rules and behavior governing the operation of network elements which allow and support the instantiation and operation of one or more channels of communication between elements.

Security Operations: Methods and processes used to monitor and manage security within defined operational limits including:

- The collection and analysis of behavioral information which may have an effect on security.
- The detection of behavior which adversely effects security or by which the likelihood of a future adverse effect can be determined.
- Action taken in the event of an adverse behavior taking place in order to limit, mitigate and/or prevent future occurrences of the adverse behavior or its effects.
- Security-related communications, whether physical, virtual or otherwise network related concerning the status and condition of systems.

4. Abbreviations and acronyms

BEEP	Blocks Extensible Exchange Protocol
CAPEC	Common Attack Pattern Enumeration and Classification
CCE	Common Configuration Enumeration
CEE	Common Event Expression
CEEE	Common Event Expression Exchange
CERT	Computer Emergency Response Team
CHIRP	Cybersecurity Heuristics and Information Request Protocol
CPE	Common Platform Enumeration
CRF	Common Result Format
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
DEXF	Digital Evidence Exchange File Format
ERDM	Electronic Discovery Reference Model
EVCERT	Extended Validation Certificate Framework
IODEF	Incident Object Description Exchange Format
LEA	Law Enforcement Agency
OVAL	Open Vulnerability and Assessment Language
SCAP	Security Content Automation Protocol

SOAP Simple Object Access Protocol

XCCDF eXensible Configuration Checklist Description Format

5. Conventions

The key words "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this Recommendation are interpreted in accordance with [ITU-T Res. ??].

6. Basic concept of the Cybersecurity Information Exchange Framework

This section describes the basic construct of the framework and the context for its use.

6.1 Description of the Framework

The Cybersecurity Information Exchange Framework (CYBEX) is intended to accomplish a simple, limited objective – namely common global means for cybersecurity entities to exchange cybersecurity information – generally over a network of some kind. Such entities typically consist of organization, persons, objects, or processes possessing or seeking cybersecurity information. Most frequently, these entities are CSIRTs or National CERTs and the operators or vendors of equipment, software or network based systems.

The cybersecurity information exchanged is essential to achieving enhanced cybersecurity and infrastructure protection, as well as accomplishing the principal functions performed by CSIRTS. This information includes:

- 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
- Parties who implement cybersecurity information exchange capabilities within the scope of this framework
- Specifications for the exchange of cybersecurity information, including modules, schemas, and assigned numbers
- The identities and trust attributes of all of the above
- Implementation requirements, guidelines and practices

The exchange of vulnerability information typically occurs within highly compartmentalized trust communities until remedies are devised and available. At such time, knowledge of the vulnerability and the associated remedies is made public. The related specifications included in this framework are intended to facilitate these processes and thereby enhance cybersecurity. Ref. ITU-T Rec. X.1206.

This exchange process is depicted below in Figure 1 as consisting of three functions:

- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- trusted exchanging of cybersecurity information over networks

Sections 7 through 9 of this Recommendation set forth specifications for accomplishing these functions.

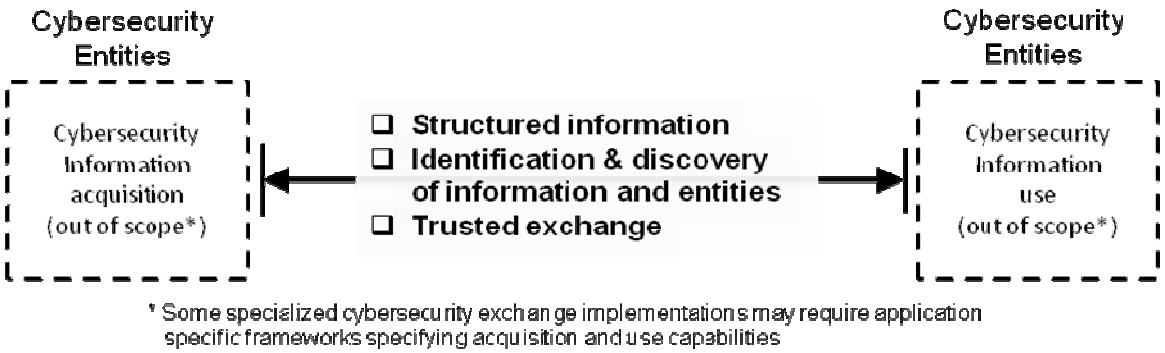

Figure 1 – Framework for the exchange of cybersecurity information

The exchange framework is bi-directional. This bi-directionality allows for both information requests and verifications to facilitate required levels of trust between the parties or provide certification of delivery.

The means of acquiring information as well as the uses made of the information are generally out of scope and not treated in this Recommendation. However, some specialized cybersecurity exchange implementations such as traceback of attack sources may require application specific frameworks specifying acquisition and use capabilities specific to that kind of exchanged information. Such implementations also include making cybersecurity measureable, for example, through the use of security content automation protocols. [ed. Add recursion]

The Framework makes no assumptions about the cybersecurity entities other than an identity – which may be public or private. Entities may also exist entirely within the same organization or cloud.

[ed. This frame work applies to the format for the exchange of this information and does not mandate in any way to exchange the information.]

6.2 Description of the context of the framework

Although specific acquisitions and uses are out of scope, it is useful at the macro level to describe the implementation context of the Framework. The Framework enables exchange capabilities for the entire Cybersecurity Ecosystem, by supporting the dashed exchanges shown in Figure 2, below. In this depiction, Cyber Security is shown as a coherent set of capabilities that include measures to enable protection, threat detection, thwarting and patching, and legal remedies. The trusted exchange of cybersecurity information is essential for enabling this ecosystem.

The Framework is also equally applicable when the ecosystem components are highly distributed, or integrated in the form of Cloud Computing.

[ed. A depiction or description of CSIRTS in Fig. 2 is needed]

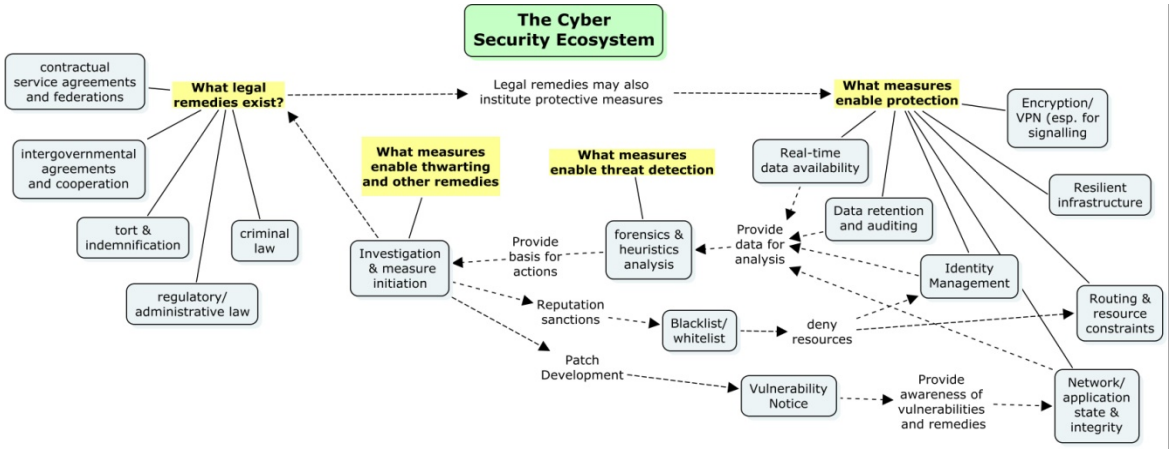

Figure 2 – The Cyber Security Ecosystem supported by the exchange of cybersecurity information

6.3 Elements of the Framework

Due to the speed at which new attack techniques propagate throughout networks as well as the techniques used to hide the actual sources of attacks, i.e. bot-herders and the like, viewing only one type of information, no matter what the one type is, has proven ineffective in countering the threat. However, with a broader view of the network landscape, patterns are easier to see, sources of attacks easier to find and more efficient and effective responses may be made.

However, the current state of security operations is that the sources of information available at any given time lag far behind their effective usefulness and while protective measures are being developed, attacks go unchecked. . Also, the information available is of such a disparate nature that trying to coordinate and correlate available information is a difficult task.

A primary goal of this framework is to increase efficiency and effectiveness of security operations at all levels, from home users to corporate networks, by increasing the ability to collect and analyze information and to correlate a wider

range of information than previously possible. This includes the need to apply automation to a broader range of application and system implementations.

Without a complete understanding of a given situation, security operations is left with isolating, black-holing, or filtering out the offending source or manifestation of incidents and events. While this may appear to improve the situation within a local security island, it frequently leads to an increase in the number of incidents and events.

[ed. A more extensive description of the elements and application of the framework is needed.]

7. Cybersecurity structured information

For the exchange of cybersecurity information to occur as messages between any two entities, it must be structured and described in some consistent manner that is understood by both of those entities. This section describes specifications that enable this exchange. The goal is to make it easier to share cybersecurity information that often 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 to facilitate the cybersecurity related comparisons.

[ed. Some existing specifications are simply identified; while others are being imported as X-series specifications. The choice of treatment has primarily to do with the degree of specialization of the “owning” user community and the globalization benefits derived by the importing. Generic vulnerability and incident specifications, for example, have broad applicability; while LEA information exchange specifications do not.]

These structured information capabilities are organized into several exchange “clusters” for distinct cybersecurity user groups and requirements. Identified needs include:

- Vulnerability/mitigation exchange
- Event/incident/heuristics exchange
- LEA/evidence exchange
- Cybersecurity organization identity and trust
- Cybersecurity heuristics and information request

In addition, these structured information capabilities have dependencies and other kinds of relationships including interoperability, are shown below.

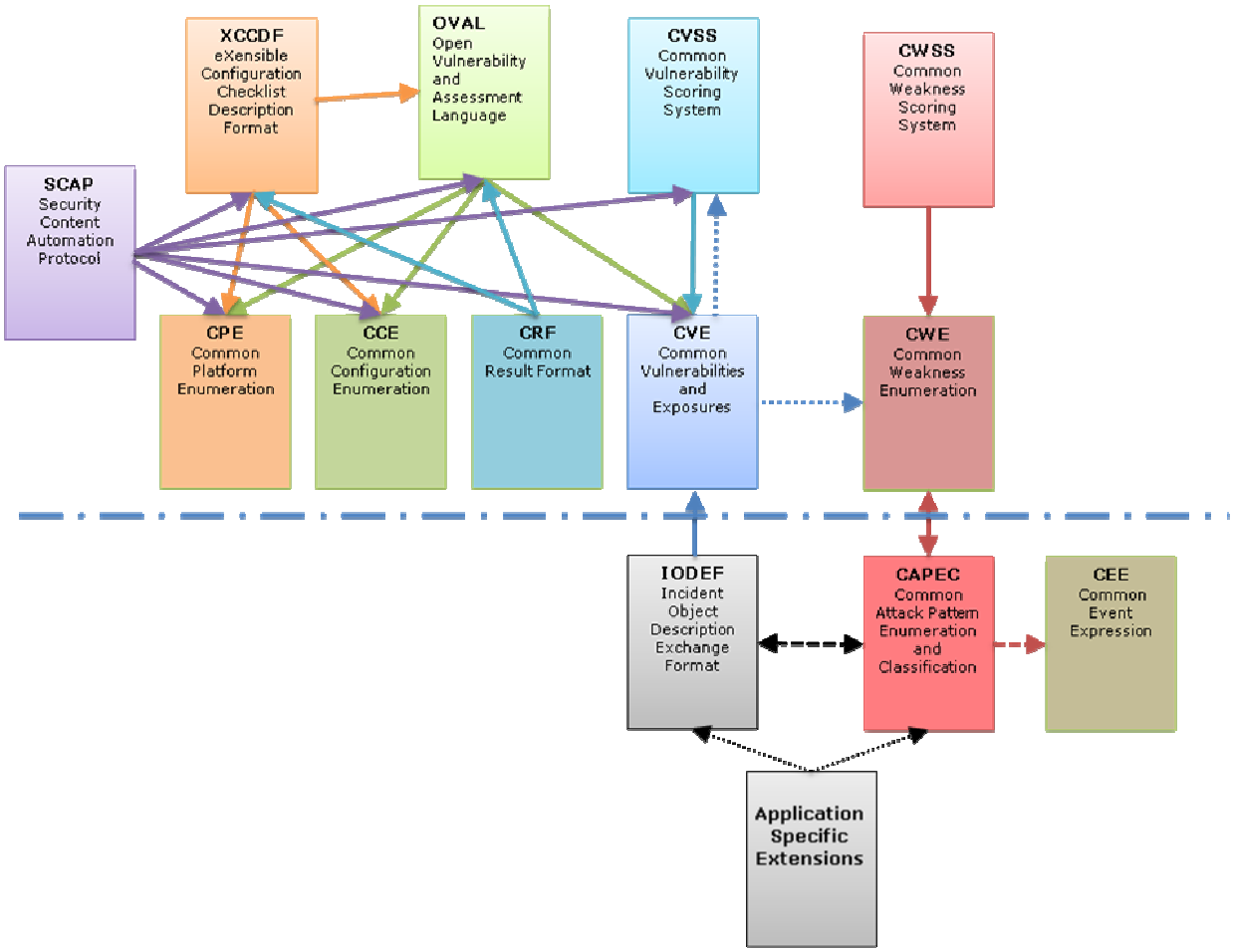

Figure 3 – Relationships and dependencies among structured information exchange capabilities

7.1 Vulnerability/Mitigation Exchange Cluster

The following specifications are included as part of the framework for the purpose of exchanging vulnerability information or mitigating vulnerabilities. The cluster includes extensions of these specifications that are specific to applications such as SmartGrid and eHealth IT cybersecurity.

Rec. ITU-T X.cwe, Common Weakness Enumeration (CWE). Common Weakness Enumeration is an XML/XSD based specification for exchanging unified, measurable sets of software weaknesses that enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Rec. ITU-T X.cwss, Common Weakness Scoring System (CWSS). The Common Weakness Scoring System specification provides for an open framework for communicating the characteristics and impacts of software weakness.

Rec. ITU-T X.cve, Common Vulnerabilities and Exposures (CVE). Common Vulnerabilities and Exposures is an XML based specification for exchanging information security vulnerabilities and exposures that aims to provide common names 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 capabilities 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 and any new problems that become public, and then addressing any older security problems that require validation.

Rec. ITU-T X.cvss, Common Vulnerability Scoring System (CVSS). The Common Vulnerability Scoring System specification provides for an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of 3 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 any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting a common language of scoring IT vulnerabilities.

Rec. ITU-T X.oval, Open Vulnerability and Assessment Language (OVAL). Open Vulnerability and Assessment Language is an international, information security, community standard 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 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 systems for testing; analyzing the system 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.

Three OVAL schemas written in Extensible Markup Language (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 system information, an OVAL Definition schema for expressing a specific machine state, and an OVAL Results schema for reporting the results of an assessment.

Rec. ITU-T X.scap, Security Content Automation Protocol (SCAP). The Security Content Automation Protocol comprises specifications for organizing and expressing security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities. This 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 the six specifications: XCCDF, OVAL, CPE, CCE, CVE, and CVSS. These specifications are grouped into three categories: languages, enumerations, and vulnerability measurement and scoring systems.

Rec. ITU-T X.xccdf, eXensible 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.

Rec. ITU-T X.cpe, Common Platform Enumeration (CPE). Common Platform Enumeration is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

Rec. ITU-T XX.cce, 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.

Rec. ITU-T X.crf, Common Result Format (CRF). Common Result Format is a standardized IT asset assessment result format that facilitates the exchange of assessment results among systems to increase tool interoperability and allow for the aggregation of those results across large enterprises that utilize diverse technologies to detect patch levels, policy compliance, vulnerability, asset inventory, and other tasks. CRF leverages existing standardization efforts for common names and naming schemes to report the findings for assets.

7.2 Event/Incident/Heuristics Exchange Cluster

The following specifications are included as part of the framework for the purpose of exchanging event, incident or heuristic information.

Rec. ITU-T X.cee, 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.

Rec. ITU-T X.iodef, Incident Object Description Exchange Format (IODEF). The Incident Object Description Exchange Format defines a data representation that provides a framework for the exchange of information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. This document describes the information model for the IODEF and provides an associated data model specified with XML Schema.

[ed. Check on IDM work and relevancy to exchange of IODEF messages.]

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

7.2.1 Specific Event/Incident/Heuristics Exchange Cluster

The following specifications are included as part of the framework for the purpose of exchanging specialized event, incident or heuristic information.

Rec. ITU-T X.teef, Cyber Attack Tracing Event Exchange Format. The Cyber Attack Tracing Event Exchange Format defines a data representation that provides a framework for the exchange of information by Computer Security Incident Response Teams (CSIRTs) about the source and path of computer security incidents. This document describes the information model for TEEF and provides an associated data model specified with XML Schema.

Rec. ITU-T X.dpi, Deep Packet Inspection Exchange Format. The Deep Packet Inspection Exchange Format defines a data representation that provides a framework for the exchange of information by Computer Security Incident Response Teams (CSIRTs) about the attributes of packet payloads associated with computer security incidents. This document describes the information model for DPI and provides an associated data model specified with XML Schema.

Rec. ITU-T Xpfoc Phishing, Fraud, and Other Crimeware Exchange Format. The Phishing, Fraud, and Other Crimeware Exchange Format extends the Incident Object Description Exchange Format (IODEF) to support the reporting of phishing, fraud, other types of electronic crime. The extensions also support the exchange on 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.

[ed. Consider if newly created IEEE Computer Security Group (ICSG) for development of a Malware Exchange Format specification should be included in this section of X.cybex.]

Rec. ITU-T X.gridf, SmartGrid Incident Exchange Format. The SmartGrid Incident Exchange Format defines a data representation that provides a framework for the exchange of information by Computer Security Incident Response Teams (CSIRTs) about the attributes of SmartGrid security incidents. This document describes the information model for SmartGrid Security Incident exchanges and provides an associated data model specified with XML Schema.

7.3 LEA/Evidence Exchange Cluster

The following specifications are included as part of the framework for the purpose of exchanging law enforcement authority or juridical evidence information exchange.

ETSI TS102232, Handover Interface and Service-Specific Details (SSD) for IP delivery. The Handover Interface and Service-Specific Details (SSD) for IP delivery specification defines a data representation that provides a framework for the exchange of information between a network mediation point and a law enforcement facility to provide an array of different real time network forensics associated with a designated incident or event. This document describes the information model and provides an associated data model specified with ASN.1 modules.

ETSI TS102657, Handover Interface for the Request and Delivery of Retained Data. The Handover Interface for the Request and Delivery of Retained Data specification defines a data representation that provides a framework for the exchange of information between a network mediation point and a law enforcement facility to provide an array of different stored network forensics associated with a designated incident or event. This document describes the information model and provides an associated data model specified with ASN.1 modules and XML schema.

IETF RFC3924, Architecture for Lawful Intercept in IP Networks

The Architecture for Lawful Intercept in IP Networks specification defines a data representation that provides a framework for the exchange of information between a network access point and a provider mediation facility to provide an array of different real time network forensics associated with a designated incident or event. This document describes the information model and provides an associated data model specified with ASN.1 modules.

3GPP TS23.271, Handover for Location Services. The Handover Interface for Location Services specification defines a data representation that provides a framework for the exchange of information between a network mediation point and an external facility to provide an real-time or stored location forensics associated with a network device. This document describes the information model and provides an associated data model specified with ASN.1 modules and XML schema.

EDRM, Electronic Discovery Reference Model. The Electronic Discovery Reference Model specification defines a data representation that provides a framework for the exchange of information between a network mediation point and a juridical designated party to request and provide an array of different stored network forensics associated with a designated incident or event. This document describes the information model and provides an associated data model specified with XML schema.

Rec. ITU-T X.dexf, Digital Evidence Exchange File Format. The Digital Evidence Exchange File Format specification defines structures and data elements for structured digital evidence exchange file exchange. Electronic evidence means information and data of investigative value that is stored on or transmitted by electronic device. The primary purpose of digital evidence exchange file format is interoperability of digital forensic systems. It does not include any protection scheme.

7.4 Cybersecurity Heuristics and Information Request Cluster

The following specifications are included as part of the framework for the purpose of requesting cybersecurity heuristics and information.

Rec. ITU-T X.chirp, Cybersecurity Heuristics and Information Request Protocol. Cybersecurity Heuristics and Information Request Protocol defines a flexible data representation that provides a framework for requesting information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. This document describes the information model for CHIRP and provides an associated data model specified with XML Schema.

8. Cybersecurity identification and discovery

Different cybersecurity organizations are implementing common cybersecurity protocols for the capture and exchange of system state, vulnerability, incident forensics, and incident heuristics information in operational applications and as specified in this Recommendation. 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.

Any globally unique identifier used for global cybersecurity information exchange must necessarily have the following characteristics:

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

8.1 Common Cybersecurity Identifier (CCI)

Cybersecurity information exchange protocols can be used by anyone, anywhere, at any time. So there is no way to control their use. However, common interests may exist among cybersecurity communities regarding cybersecurity identifiers and their creation, administration, discovery, verification, and use. Some of those interests include:

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

Rec. ITU-T X.cybex.1, Guidelines for Administering the OID arc for cybersecurity information exchange. A common global cybersecurity identifier namespace for these purposes is described in Rec. ITU-T X.cybex.1, together with administrative requirements, as part of a coherent OID arc, and includes:

- Cybersecurity information identifiers
- Cybersecurity organization identifiers
- Cybersecurity policy identifiers

8.2 Discovery

Rec. ITU-T X.cybex-disc, Discovery Mechanisms in the Exchange of Cybersecurity Information. This recommendation provides 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.

9. Cybersecurity trusted exchange

Within the Information Exchange Framework, 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. The latter can have additional requirements imposed if the exchanged information is subsequently used for evidentiary purposes.

9.1 Trust Assurance

Many different trust assurance mechanisms are used in conjunction with the exchange of cybersecurity information. Several are included as part of this framework.

Rec. ITU-T X.eaa, Entity authentication assurance. This Recommendation | International 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.

Rec. ITU-T X.evcert, Extended Validation Certificate Framework. The Extended Validation Certificate Framework consists of an integrated combination of technologies, protocols, identity proofing, lifecycle 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.

ETSI TS102042 V.2.1, Policy requirements for certification authorities issuing public key certificates. The present 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.

9.2 Information Exchange Protocols

This section contains specific exchange protocols that are used in diverse cybersecurity information exchange contexts.

Rec. ITU X.cybex-tp, Transport Protocols supporting Cybersecurity Information Exchange. This recommendation provides an overview of exchange protocols which have been adopted and or adapted for use within the Cybersecurity Information Exchange Framework, Cybex.

Rec. ITU-T X.cybex-beep, Blocks eXtensible eXchange Protocol Framework for CYBEX. RFC3080 describes a generic application protocol kernel for connection-oriented, asynchronous interactions called BEEP. At BEEP's core is a framing mechanism that permits simultaneous and independent exchanges of messages between peers. Messages are arbitrary MIME content, but are usually textual (structured using XML). 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. Implicit in the operation of BEEP is the notion of channel management. In addition to defining BEEP's channel management profile, this document defines: the TLS transport security profile; and, the SASL family of profiles. Other profiles, such as those used for data exchange, are defined by an application protocol designer.

Rec. ITU-T, X.cybex-soap, Simple Object Access Protocol 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.

Transport of Real-time Inter-network Defense (RID) Messages. This specification specifies the transport of RID messages within HTTP [RFC2616] Request and Response messages transported over TLS.

ETSI TS102232-1, Handover Interface and Service-Specific Details (SSD) for IP delivery. The -1 module of the Handover Interface and Service-Specific Details (SSD) for IP delivery specification contains protocols and their implementation for trusted delivery of forensic information to law enforcement and security authorities.

Appendix: compendium of cybersecurity requirements and guidelines

This appendix contains an extensive compendium of existing requirements that provide the basis for the Cybersecurity Information Exchange Framework as well as guidelines for its use.

Generic Cybersecurity

X.1205 Overview of cybersecurity

X.gopw Guideline on preventing malicious code spreading in a data communication network

WD27032 (N7558) Guidelines for cybersecurity

WD27033-1 (N7584) Guidelines for Network security

WD27034 (N7564) Application security

Y.2701 Next Generation Network security

X.tsgf Information security governance framework

WD27014 (N7820) information security governance framework

[ed. The ITU-D Q22/I cybersecurity report seems appropriate here.]

Vulnerability Exchange

X.1206 automatic notification of security related information and dissemination of updates

WD29147 (N7901) Responsible Vulnerability disclosure

Generic Security Information

X.sisfreq Requirement for security information exchange

X.gpn Mechanism and procedure for distributing policies for network security

Incident Forensics

X.1056 Security Incident Management for telecommunications organizations

WD27035 (N7566) Information Security Incident Management

X.bots Framework for botnet detection and response

X.tb-ucc Traceback use cases and capabilities

X.abnot Abnormal traffic detection and control guideline for telecommunication network

X.sips Framework for countering cyber attacks in SIP-based services

Y.dpireq NGN deep packet inspection requirements

WD27037 (N7570) Guidelines for identification, collection and/or acquisition and preservation of digital evidence

LEA Forensics

TS102656 Retained Data Requirements

TS101331 Requirements of Law Enforcement Agencies

_____