CYBEX – The Cybersecurity Information Exchange Framework (X.1500)

Anthony Rutkowski*
Yaana Technologies, USA
tony@yaanatech.com

Youki Kadobayashi†
NAIST, Japan
youki-k@is.naist.jp

Inette Furey
DHS, USA
Inette.Furey@dhs.gov

Damir Rajnovic
FIRST, USA
gaus@cisco.com

Robert Martin
MITRE, USA
ramartin@mitre.org

Takeshi Takahashi‡
NICT, Japan
takeshi_takahashi@nict.go.jp

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article's technical content. Comments can be posted through CCR Online.

ABSTRACT

The cybersecurity information exchange framework, known as CYBEX, is currently undergoing its first iteration of standardization efforts within ITU-T. The framework describes how cybersecurity information is exchanged between cybersecurity entities on a global scale and how the exchange is assured. The worldwide implementation of the framework will eventually minimize the disparate availability of cybersecurity information. This paper provides a specification overview, use cases, and the current status of CYBEX.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and Protection*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Standardization, Security, Design

Keywords

CYBEX, cybersecurity, security, information exchange

1. INTRODUCTION

Wide proliferation of the Internet is bolstering the immense development of cyber society, where diverse communications including sharing of private information and business transactions are taking place. In cyber society, malware such as viruses may attack any computer beyond the borders of the country of its origin or target, and an attacker can attack computers all over the world by running other hackers' pre-packaged attack software. Sources of threats cross borders of countries and even continents. It is also possible for an attacker to attack computers in country A by controlling computers in country B while physically residing in country C. Moreover, a system's vulnerability may be exposed to any attackers across the globe. The number of attacks is increasing drastically each year. From the viewpoint of new malicious code signatures, Symantec created 2,895,802 such signatures in 2009, a 71 percent increase over 2008; the 2009 figure represents 51 percent of all such signatures ever created by Symantec [7].

Countermeasures against these cybersecurity threats, however, are most frequently implemented by individual organizations in isolation. Consequently, an organization in one country may be attacked by malware whose countermeasures are already known and implemented within another organization in another country. Such incidents occur due to the lack of sharing of information among organizations. One of the biggest factors preventing organizations from sharing information with each other is the absence of a globally common format and framework for cybersecurity information exchange. Albeit some countries such as the United States possess domestic standards for approaching this problem, most other countries have no such standards. Another such factor is the absence of assured information exchange framework, without which no organization will exchange information.

To cope with this problem, ITU-T is now building an emerging standard – The Cybersecurity Information Exchange Framework (CYBEX). CYBEX provides a globally common format and framework for assured cybersecurity information exchange, which will eventually minimize the disparity of cybersecurity information availability on a global scale. Since cybersecurity information can be shared worldwide, no country or organization implementing CYBEX will be left behind in terms of its availability. Consequently, developing countries, which currently have fewer resources to put towards cybersecurity, can become equal partners with developed countries with appropriate investments. Therefore countermeasures will be implemented through global collaboration. The framework will also advance the development of automating cybersecurity information exchange. Most cybersecurity information exchange within organizations are not currently automated and depend largely on human intervention. Email, telephone calls and even face-to-face meetings are still the primary method for information exchange. The need for and reliance on human interaction

*This author is the Rapporteur of ITU-T Q.4/17.

†This author is the Associate Rapporteur of ITU-T Q.4/17.

‡This author is the main editor of this article.

Table 1: CYBEX family specifications

Functional blocks	CYBEX family specifications	
	imported specifications	newly built specifications
Information Description block	CPE, CCE, CVE, CWE, CAPEC, MAEC, CVSS, CWSS, OVAL, XCCDF, ARF, IODEF, CEE, TS102232, TS102667, TS23.271, RFC3924, EDRM,	X.dexf, X.pfoc
Information Discovery block		X.cybex.1, X.cybex-disc
Information Query block		X.chirp
Information Assurance block	EVCERT, TS102042 V2.0	X.eaa
Information Transport block	TS102232-1	X.cybex-tp, X.cybex-beep

vspace-2mm

consumes a great deal of time. By advancing automation of cybersecurity information exchange, the costs (e.g., personnel costs) within each organization will be significantly reduced and the operation will be more efficient. At the same time, human-operation-based mistakes such as miscommunication can be avoided; thus the quality of operations can be improved.

The rest of this paper is organized as follows: Section 2 explains the scope of CYBEX, Section 3 describes the overview of CYBEX specification, Section 4 describes the use cases of CYBEX, Section 5 describes the current status of CYBEX, and Section 6 concludes the paper.

2. SCOPE OF CYBEX

CYBEX focuses on cybersecurity information exchange between cybersecurity organizations as shown in Figure 1. Cybersecurity information is information required for cybersecurity operations such as on a vulnerability, and a cybersecurity organization is an organization running cybersecurity operations such as CERTs of countries and private companies. How to acquire/use cybersecurity information is outside the scope of CYBEX.

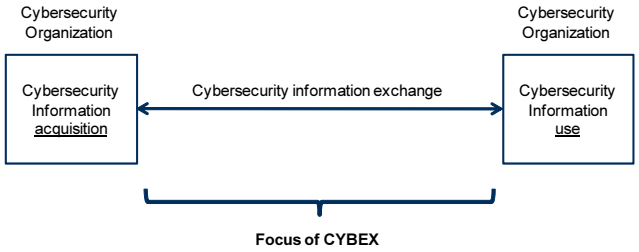

Figure 1: Scope of CYBEX

The cybersecurity information exchange provides an effective cybersecurity ecosystem where knowledge derived from reports, testing, experience, and experience are 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. These building blocks can also be used for creating extension capabilities that include detection of malware or automating known secure states of software, services, and systems. This cybersecurity ecosystem enabled by CYBEX is shown in Figure 2. Evidence is produced when required by authorities for wrongdoing.

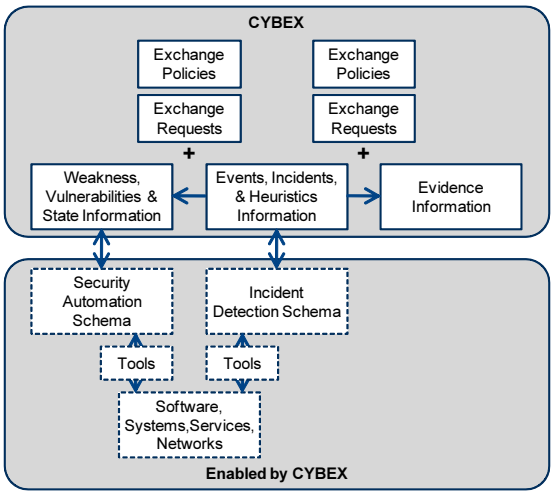

Figure 2: Cybersecurity ecosystem enabled by CYBEX

3. OVERVIEW OF CYBEX SPECIFICATIONS

Considering the cybersecurity information life cycle, we concluded that five functional blocks are needed for CYBEX: Information Description, Information Discovery, Information Query, Information Assurance and Information Transport, as are shown in Figure 3. The Information Description block structures cybersecurity information for exchange purposes, the Information Discovery block identifies and discovers cybersecurity information and entities, the Information Query block requests and responds with cybersecurity information, the Information Assurance block ensures the validity of the information, and Information Transport block exchanges cybersecurity information over networks.

Each functional block consists of assorted specifications[1] as are shown in Table 1. As can be seen, one important characteristics of CYBEX is that this de jure standard is based on current de facto standards, and that by creating CYBEX in cooperation with the creators of each de facto standards we can increase the utility and compatibility of CYBEX with these standards, so users will be able to use CYBEX

[1]The term "specification" in this paper includes draft Recommendations that are not completed yet or that are still in its initial phase of development though it usually refers to a detailed description of the design and materials that is ready for use.

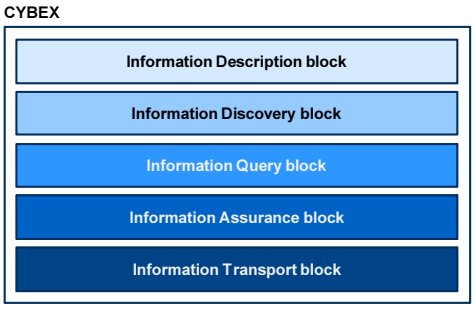

Figure 3: Five functional blocks of CYBEX

seamlessly with available products, making CYBEX more practical and deployable.

Each of the functional blocks are elaborated on in the following subsections.

3.1 Information Description Block

This functional block structures cybersecurity information for exchange purposes and provides the formats and languages to describe it. These formats and languages are depicted through the introduction of 18 existing specifications and three newly created ones.

From the viewpoint of the cybersecurity operational information ontology that is modified from the one in [11] to accommodate forensic aspects, these specifications are classified as shown in Figure 4. The following subsections provide the details of the introduced specifications following the operation domains defined by the ontology.

3.1.1 Knowledge Accumulation Domain

Knowledge Accumulation domain is an operation domain that accumulates knowledge on cybersecurity, which will be then shared and reused by other organizations. The National Vulnerability Database [10], for instance, is providing practical facilitation for such operations. The information required for this operation is stored in either of the three knowledge bases: Product & Service, Cyber Risk or Countermeasure.

The Cyber Risk Knowledge Base accumulates information on cyber risks including that on vulnerabilities and threats. To describe information in the knowledge base, CYBEX introduces Common Vulnerabilities and Exposures (CVE) [9, 13], Common Weakness Enumeration (CWE) [9, 13], Common Attack Pattern Enumeration and Classification (CAPEC) [9, 13], and Malware Attribute Enumeration and Characterization (MAEC) [9, 13]. CVE provides unique identifiers for publicly known vulnerabilities in commercial and open source software to facilitate rapid and accurate correlation of vulnerability data across multiple information sources and tools. CWE is an XML/XSD-based specification that provides unique identifiers for the weaknesses in software code, design, architecture, or implementation as well as a rich body of knowledge about the cause, impact, and mitigations of these weaknesses to include code examples. CAPEC is an XML/XSD-based specification that provides unique identifiers for the patterns of attack against software as well as a rich body of knowledge about the attack steps, impact, and mitigations of these attack patterns to include observable attributes. MAEC provides a language and format for characterizing the behaviors and actions of malware with two core components consisting of enumerated elements (vocabulary) and schema (grammar).

The Countermeasure Knowledge Base accumulates information on countermeasures that corresponds to cyber risks. To describe information in the knowledge base, CYBEX introduces the Common Vulnerability Scoring System (CVSS) [9, 13], Common Weakness Scoring System (CWSS) [12], Open Vulnerability and Assessment Language (OVAL) [9, 13], and eXtensible Configuration Checklist Description Format (XCCDF) [9, 13]. CVSS provides for an open framework for communicating the characteristics and impacts of IT vulnerabilities, while CWSS provides that for software weaknesses. OVAL provides a language used to encode system details and an assortment of content repositories held throughout the community, and XCCDF provides a language for writing security checklists, benchmarks, and related kinds of documents.

The Product & Service Knowledge Base accumulates information on products and services. To describe information in this knowledge base, CYBEX introduces Common Platform Enumeration (CPE) [9, 13] and Common Configuration Enumeration (CCE) [9, 13]. CPE provides a structured naming scheme for information technology systems, platforms, and packages, while CCE provides unique identifiers to system configuration issues to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. Note that knowledge on cyber risks and countermeasures are often linked to specific products and services. For instance, a CVE is linked to CPE identifiers and CVSS scores in NVD. Hence the Product & Service Knowledge Base is linked to Cyber Risk Knowledge Base and Countermeasure Knowledge Base as is shown in Figure 4.

3.1.2 IT Asset Management Domain

IT Asset Management domain is an operation domain that administrates and protects IT assets of user organizations. The necessary information for this operation is stored in the User Resource Database and Provider Resource Database. To describe information in the User Resource Database, CYBEX introduces the Assessment Result Format (ARF) [13], which provides a standardized IT asset assessment result format that facilitates the exchange of such results among systems.

3.1.3 Incident Handling Domain

Incident Handling domain is an operation domain that monitors and responds to cyber-incidents. The necessary information for this operation is stored in the Incident Database and Warning Database. To describe information in the Incident Database, CYBEX introduces the Incident Object Description Exchange Format (IODEF) [6], X.pfoc, and Common Event Expression (CEE) [9, 13]. IODEF defines a data representation that provides a framework for exchange of information about computer security incidents. X.pfoc (Phishing, Fraud, and Other Crimeware Exchange Format) extends IODEF to support the reporting of phishing, fraud, and other types of electronic crime. The extensions also support exchange of information about widespread spam incidents. CEE defines a common language and syntax for expressing how events are described, logged, and exchanged.

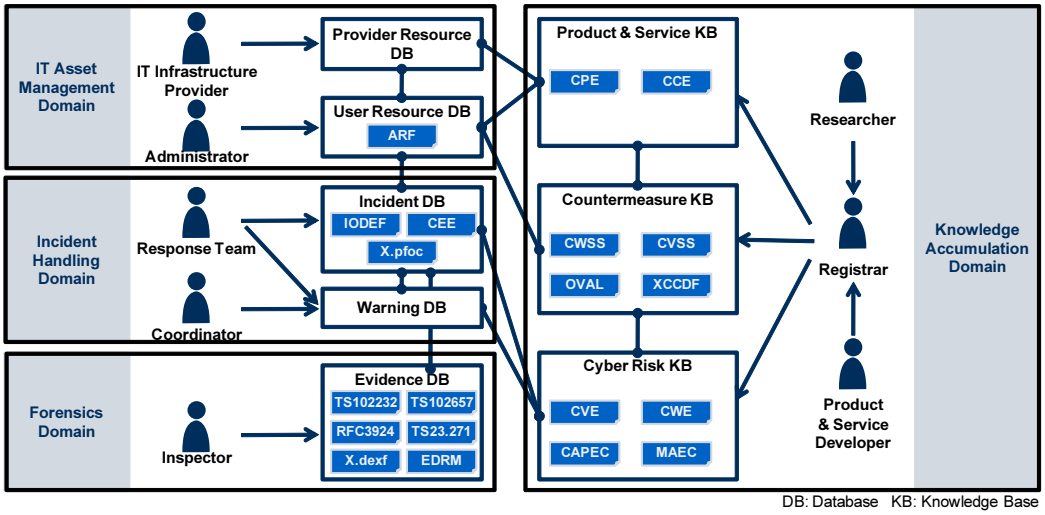

Figure 4: Cybersecurity information specifications in CYBEX

3.1.4 Forensics Domain

Forensics domain is an operation domain that supports law enforcement operations by collecting evidences. The necessary information for this operation is stored in the Evidence Database. To describe information in the database, CYBEX introduces six forensics specifications: ETSI TS102232 [2], ETSI TS102657 [3], ETSI TS23.271 [1], RFC3924 [5], Electronic Discovery Reference Model (EDRM) [4] and X.dexf. ETSI TS102232 defines a data representation that provides a framework for 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. ETSI TS102657 defines the same but with stored network forensics. ETSI TS23.271 defines a data representation that provides a framework for 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. RFC 3924 defines a data representation that provides a framework for 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. EDRM defines a data representation that provides a framework for 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. X.dexf (Digital Evidence Exchange Format) defines structures and data elements for structured digital evidence exchange.

3.2 Information Discovery Block

This functional block identifies and discovers cybersecurity information and entities. X.cybex-disc provides such methods and mechanisms, and provides two paradigms for service and information discovery in common use: centralized discovery and de-centralized discovery.

Centralized discovery can best be explained by pointing to the OID [8] as an example of how one or more hierarchical registries are used by information providers as a means of

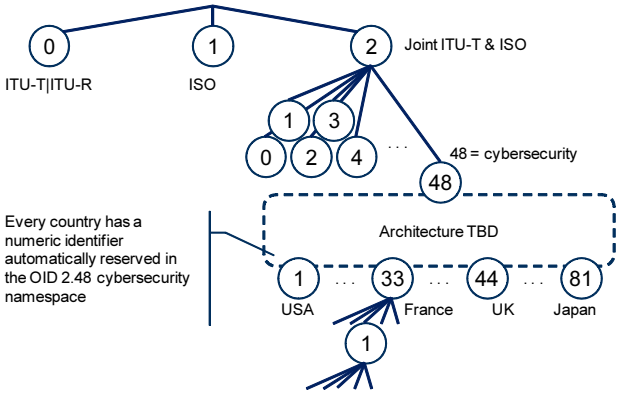

Figure 5: OID-based discovery

making their services known, and by those seeking sources for the information they require. Figure 5 depicts the concept of identifying cybersecurity information in OID-based discovery. Cybersecurity information is hierarchically indexed in a tree, so that any information can be traceable by following the tree. Note that the OID space and namespace are defined by X.cybex.1, which also provides a guideline for administrating the OID arc for cybersecurity information exchange. Central registries have many advantages in that users can easily know where to go and quickly find what they are looking for. Their main disadvantage is that users need to know of the existence of a given registry in the first place before using it, either as an information provider or the one seeking information. In addition, the different resources and costs involved in maintaining a central repository can also make it prohibitive for those with limited resources.

A common example of decentralized discovery is the RDF [14] of the World Wide Web Consortium (W3C). RDF is a syntactic and semantic language for representing information describing available resources. Figure 6 depicts the concept of identifying cybersecurity information in RDF-based discovery. A user wishing to access such information uses

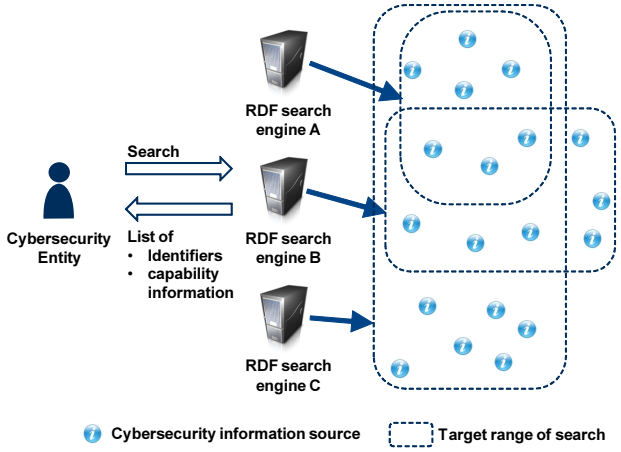

Figure 6: RDF-based discovery

an RDF search engine, which has its own list of indices to the assorted cybersecurity information in the network. Note that the search ranges of each RDF search engine are different. Then the search engine replies to the cybersecurity entity with the list of identities and capability information of candidate cybersecurity information sources. RDF's main advantage is that resources and costs associated with making RDF information available are minimal, and those providing information and those seeking information need not know of each other's existence beforehand. RDF's main disadvantage is that in order for users to find the information they seek, starting from zero-knowledge, they literally need to crawl the entire Internet. However, aggregations of RDF-formatted information can provide a useful compromise between centralized and decentralized discovery mechanisms in some applications.

3.3 Information Query Block

This functional block requests and responds with cybersecurity information. CYBEX introduces X.chirp, which provides secure access, including management and maintenance of cybersecurity information through a common set of interfaces. X.chirp is a query language that is an extension of SQL.

3.4 Information Assurance Block

This functional block ensures the validity of the information. CYBEX introduces three standards: X.evcert, X.eaa and ETSI TS 102042 V2.0. X.evcert is a draft recommendation for digital certificates. It provides a framework for EV Certificates, which describes the minimum requirements that must be met in order to issue and maintain EV Certificates concerning a subject organization. X.eaa is a draft recommendation for identity assurance. It provides an authentication life cycle framework for managing the assurance of an entity's identity and associated identity information in a given context. ETSI TS102042 V.2.0 is a draft recommendation for policy requirement for certification authorities (CA). It describes these requirements for certification authorities issuing public key certificates.

3.5 Information Transport Block

This functional block exchanges cybersecurity information over networks. The overview of such a function is described in X.cybex-tp. This describes the overview of transport protocols for cybersecurity information exchange. Based on the general overview, protocol specific features are described in the X.cybex-beep draft recommendation, which describes a transport protocol based on BEEP. Albeit other protocols can be used for this transport, currently only the BEEP protocols are being investigated. Other candidate protocols, such as SOAP, exist but no draft recommendation for such protocols have been presented yet. From the viewpoint of forensics, ETSI TS102232-1 is also introduced here. This provides assurance of forensics information delivery to law enforcement and security authorities.

4. USE CASES

CYBEX provides the framework for exchanging cybersecurity information between cybersecurity entities. The usage of the standard is up to users. Nevertheless, to demonstrate the usability of CYBEX, this section describes two use cases of CYBEX.

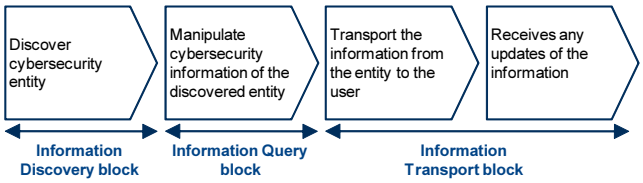

Figure 7: Cybersecurity information acquisition

A user may wish to know the vulnerabilities on a particular computer and to keep updated about them and their related information. In this case, CYBEX is one of the most feasible options for the user, which may use CYBEX as shown in Figure 7. First, the user identifies a cybersecurity issue on a specific computer that they are interested in, and they want to find out more about the issue from an appropriate repository that knows about this cybersecurity issue by using either OID-based discovery or RDF-based discovery (the Information Discovery block). The user sends queries to the repository to obtain and retrieve the desired information about the cybersecurity issue that is stored within the repository using X.chirp (the Information Query block). The information can then be transferred to the user using BEEP with a CYBEX profile (the Information Transport block) or some other transfer mechanism. The user now has the desired information about the cybersecurity issue on the specific computer using the various components of CYBEX. Since the connection state is preserved in the case of BEEP, if there is a change in the repository information about the cybersecurity issue, the user can be notified. This allows the user to acquire updated and current information about the cybersecurity issues on the computer systems they care about.

Another use case is when CERT A finds an incident in CERT B, then wishes to convey the incident information to CERT B. In this case, CERT A searches CERT B using RDF-based discovery (the Information Discovery block) and receives the candidate list of CERT B with the description of capabilities. Based on the capability information, CERT A chooses the entity that seems most likely to be CERT B according to its capability description, and connects with

the entity via SSL. CERT A then receives EVSSL from the entity, with which it can ensure that the entity is CERT B (the Information Assurance block). CERT A thus sends the incident information following the IODEF format to CERT B, which sends back another IODEF message to report the completion of implementing countermeasures later (Information Description block). The procedure is depicted in Figure 8.

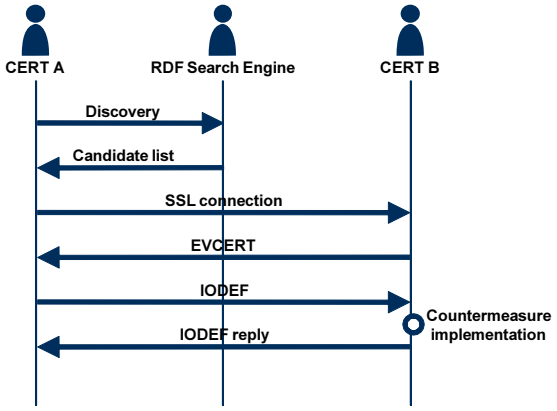

Figure 8: IODEF information notification

5. CURRENT STATUS OF CYBEX

CYBEX is expected to be standardized in December 2010. By this time, the structure of CYBEX ensembles will be determined. Nevertheless, each of the specifications that form CYBEX needs to be discussed and advanced further for their determination. This December, only CVE and CVSS are expected to be standardized as imported specifications in ITU-T. The other specifications are expected to be finalized by the end of 2013.

CYBEX is, nevertheless, still evolving and developing. For instance, it has yet to be adapted to cloud computing. As discussed in [11], the existing cybersecurity information standards are designed for current, non-cloud computing and need to be modified to accommodate cloud computing. CVSS, for instance, assumes a single computer as their evaluation target and cannot cope with virtual machines. Moreover, in the case of cloud computing, data separated from an IT asset need to be protected. This could be done, for instance, by implementing data provenance technologies.

As mentioned, CYBEX is designed to be highly practical and deployable. Many of the imported standards are de facto standards for specific purposes in specific regions. Moreover, partial implementation of CYBEX is performed by several organizations. Toward the dissemination of CYBEX, even more implementation will be provided.

6. CONCLUSION

This paper introduced CYBEX, a new cybersecurity standard that will be finalized in December 2010. CYBEX provides a framework for assured cybersecurity information exchange between cybersecurity entities and minimizes the disparity of cybersecurity information availability among cybersecurity entities. The challenge is finding a means of permitting wide usage of CYBEX. Without global and widespread usage, CYBEX will not be able to provide its true value or contribute to cybersecurity. In order to advance cybersecurity, the effectiveness of CYBEX needs to be globally and widely recognized.

7. ADDITIONAL AUTHORS

Additional authors: Craig Schultz (Multimedia Architectures, email: `craig@cass-hacks.com`) and Gavin Reid (Cisco, email: `gavreid@cisco.com`) and Gregg Schudel (Cisco, email: `gschudel@cisco.com`) and Mike Hird (BIS, email: `mike.hird@talktalk.net`) and Stephen Adegbite (FIRST, email: `sadegbit@adobe.com`).

8. REFERENCES

[1] TS23.271 : Handover for Location Services. *European Telecommunications Standards Institute*, March 2001.

[2] TS102232 : Handover Interface and Service-Specific Details (SSD) for IP delivery. *European Telecommunications Standards Institute*, December 2006.

[3] TS102657 : Handover interface for the request and delivery of retained data. *European Telecommunications Standards Institute*, December 2009.

[4] The Electronic Discovery Reference Model. *URL http://edrm.net*, August 2010.

[5] F. Baker, B. Foster, and C. Sharp. Cisco Architecture for Lawful Intercept in IP Networks. *IETF RFC 3924*, October 2004.

[6] R. Danyliw, J. Meijer, and Y. Demchenko. The Incident Object Description Exchange Format. *IETF Request For Comments 5070*, December 2007.

[7] M. Fossi, D. Turner, E. Johnson, T. Mack, T. Adams, J. Blackbird, S. Entwisle, B. Graveland, D. McKinney, J. Mulcahy, and C. Wueest. Symantec Global Internet Security Threat Report. XV, April 2010.

[8] International Telecommunication Union. Information technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree. *X.660*, August 2008.

[9] R. A. Martin. Making Security Measurable and Manageable. *CrossTalk, the Journal of Defense Software Engineering*, September/October 2009.

[10] National Institute of Standards and Technology. National Vulnerability Database (NVD). *http://nvd.nist.gov/*, August 2010.

[11] T. Takahashi, Y. Kadobayashi, and H. Fujiwara. Ontological approach toward cybersecurity in cloud computing. *International Conference on Security of Information and Networks*, 2010.

[12] The MITRE Corporation. Common Weakness Scoring System (CWSS). *URL http://cwe.mitre.org/cwss/*, August 2010.

[13] The MITRE Corporation. Making Security Measurable. *URL http://msm.mitre.org/*, August 2010.

[14] The World Wide Web Consortium (W3C). Resource Description Framework (RDF). *URL http://www.w3.org/RDF/*, August 2010.