X.1500 - Cybersecurity Information Exchange Framework (CYBEX)
(draft-takahashi-cybex-intro-00.txt)

Takeshi Takahashi, Youki Kadobayashi

ITU-T Study Group 17 Question 4
(ITU-T Q.4/17)
Messages of this presentation

• We would like to support your SCAP activities in IETF

• Our works are strongly related though they are not overlapping

• We believe we can collaborate, complement each other, and enjoy synergies
On behalf of ITU-T Q.4/17, we would like to introduce CYBEX in this presentation.

Contributors to X.1500 (CYBEX)*

Anthony Rutokowski
Rapporteur

S. Adegbite
I. Furey
M. Hird
R. Martin
A. McKay

Youki Kadobayashi
Associate Rapporteur

D. Rajnovic
G. Reid
G. Schudel
T. Takahashi
M. Terada

* Contributors include editors, but not limited to them
What is CYBEX?

- CYBEX is cybersecurity information exchange framework
- It structures cybersecurity information, and then, enables assured exchange of the information
- For that purpose it gathers all the professional works related to this and orchestrates them
We would like to provide outreach among standards bodies.
ITU-T is building X.1500, which provides the cybersecurity information exchange framework, known as CYBEX.
CYBEX consists of 5 functional blocks

Five functional blocks of CYBEX

1. **Information Description block**: This block structures and describes cybersecurity information.
2. **Information Discovery block**: This block identifies and discovers cybersecurity information and entities.
3. **Information Query block**: This block requests and responds with cybersecurity information.
4. **Information Validation block**: This block ensures the validity of the information.
5. **Information Transport block**: This block exchanges cybersecurity information over networks.

Focus of today’s presentation
This block uses the cybersecurity ontology to identify what kind of information needs to be exchanged

Cybersecurity Operational Information Information Ontology

- **IT Asset Management Domain**
  - IT Infra. Prvdr
  - Administrator
  - Provider Resource DB
  - User Resource DB

- **Incident Handling Domain**
  - Res. Team
  - Coordinator
  - Incident DB
  - Warning DB
  - Evidence DB

- **Forensics Domain**
  - Inspector
  - Evidence DB

- **Knowledge Accumulation Domain**
  - Researcher
  - Registrar
  - Product & Service KB
    - Version KB
    - Configuration KB
  - Countermeasure KB
    - Assessment Rule
    - Detection / Protection Rule
  - Cyber Risk KB
    - Vulnerability KB
    - Threat KB

Cybersecurity Information Description block

draft-takahashi-cybex-intro-00.txt
The ontology orchestrates specifications, with which various types of cybersecurity information can be described.
Standardization activities in IETF are essential for the purpose of enabling such functional blocks.

IETF standardization activities

IODEF

SCAP

Some other activities

Essential inputs

CYBEX (X.1500)
Following the philosophy of CYBEX, we would like to utilize IETF standards

Summary text from draft Rec. ITU-T X.1500 (CYBEX)

• This Recommendation
  – describes a framework and general principles for coherent, comprehensive, global, timely and assured exchange of cybersecurity information, and
  – enables this exchange by
    – identifying and incorporating existing capability specifications implemented in various environments
    – as necessary, making the existing standards more global and interoperable
    – providing extensible means for adapting to new exchange requirements and capabilities.
We believe we share the same philosophy, and we would like to support your IETF activities

- Historically, IETF and ITU-T SG17 have established close collaborative relationship

- Important specifications such as PKIX (X.509), ASN.1 (X.680) were build based on the close collaboration

- We believe we share the same philosophy - building charge-free, practical and effective standard

- We believe SCAP is a key use case of the needed capabilities for the ICT security toolkit, and it is synergistic and interoperable with other components of the CYBEX ensemble
CYBEX is a substantive ongoing global Cyber/ICT security initiative

- CYBEX structures cybersecurity information, and then enables assured exchange of the information

- The CYBEX initiative aimed at identifying the emerging set of specifications for the global platforms for achieving these trusted exchanges

- Most of the work has been accomplished within existing systems assurance, incident response, and intelligence/surveillance communities

- Pro-active outreach is part of the initiative
  - Constant attempt to survey what is occurring in all other forums and bringing important capabilities into the framework
  - Constant analysis of what is missing or needed

- Unique – no comparable activity exists
Please refer to the following articles and tools for further information, or feel free to contact us

• cg-cybex: correspondence group regarding cybex. It holds telephone conferences bi-weekly. Subscription to the mailing list is warmly welcomed

• “Cybersecurity Information Exchange Framework”, draft-takahashi-cybex-intro-00.txt, IETF, Oct. 2010


• Cybex Information Exchange Tool (cybiet) -- A Cybex Discovery and Cybex BEEP profile implementation, http://cybiet.sourceforge.net/
Messages of this presentation

- We would like to support your SCAP activities in IETF
- Our works are strongly related though they are not overlapping
- We believe we can collaborate, complement each other, and enjoy synergies