MILE Implementation Report

Chris Inacio, Carnegie Mellon University
Daisuke Miyamoto, The University of Tokyo
daisu-mi@nc.u-tokyo.ac.jp

Overview

- Updates in Section 2
  - Information Sharing and Analysis Centers (ISAC) supports
  - APWG, ACDC, and REN-ISAC
- Updates in Section 6
  - Other implementations
  - AirCERT, CyberFed, TrendMicro Sharing System

Issues

- #1: MANTIS framework (section 4) close (IETF90)
- #2: Implementation Guide (section 6/7) close (IETF90)
- #3: CIMS (section 4) close (IETF91)
- #4: n6 (section 4) close (IETF91)
- #5: updates* close (IETF91)
  - Added new section, "other implementations"
- #6: iodeflib (section 7) close (IETF92)
- #7: iodef.pm (section 7) close (IETF92)
- #8: updates* close (IETF92)
  - Moved n6 from other implementation to open source

- #9: ISAC supports (section 2) open (IETF93)
- #10: Other implementations (section 6) open (IETF93)

Section 2.1: Anti Phishing Working Group

- Anti-Phishing Working Group (APWG) is one of the biggest coalition against cybercrime, especially phishing.

- In order to collect threat information in a structured format, APWG provides a phishing and cybercrime reporting tool which sends threat information to APWG by tailoring information with IODEF format, based on RFC5070 and RFC5901.

Section 2.2: Advanced Cyber Defence Centre

- The Advanced Cyber Defense Centre (ACDC), is EU-wide activity to fight against botnets. ACDC provides a solutions to mitigate on-going attacks, as well as consolidating information provided by various stakeholders into a pool of knowledge.

- Within ACDC, IODEF is one of the supported schema for exchanging the information.

Section 2.3: REN-ISAC

- Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) is a private community of the research and higher education members fro sharing threat information, and employs IODEF formatted-message to exchange information.
- REN-ISAC also recommends to use of the IODEF attachment provided with the notification email be processed rather than relying on parsing of the email body text. The interface provided by REN-ISAC are designed for dealing with such email.
- http://www.ren-isac.net/notifications/using_iodef.html

Section 6.2: Automated Incident Reporting: AirCERT

- AirCERT (by CERT/CC of Carnegie Mellon's SEI CERT division)
  - was designed to be an Internet-scalable distributed system for sharing security event data.
  - was designed to be an automated collector of flow and IDS alerts.
  - would collect that information into a relational database and be able to share reporting using IODEF and IDMEF.
  - used SNML to exchange information about the network.
  - was implemented in a combination of C and perl modules and included periodic graphing capabilities leveraging RRDTool.

Section 6.2: (cont)

- AirCERT was intended for large scale distributed deployment and eventually the ability to sanitize data to be shared across administrative domains.

- The architecture was designed to allow collection of data at a per site basis and to allow each site to create data sharing based on its own particular trust relationships.

Section 6.3: US Department of Energy CyberFed

- The CyberFed (by Argonne National Laboratory)
  - The system automates the detection and response of attack activity against Department of Energy (DoE) computer networks.
  - automates the collection of network alerting activity from various perimeter network defenses and logs those events into its database.
  - automatically converts that information into blocking information transmitted to all participants.
  - used IODEF messages wrapped in an XML extension to manage a large array of indicators.
  - was not designed to describe a particular incident as much as to describe a set of current network blocking indicators that can be generated and deployed machine-to-machine.

Section 6.3: (cont)

- CyberFed is primarily implemented in Perl. Included as part of the CyberFed system are scripts which interact with a large number of firewalls, IDS/IPS devices, DNS systems, and proxies which operate to implement both the automated collection of events as well as the automated deployment of blacking.

- Currently CyberFed supports multiple exchange formats including IODEF and STIX. OpenIOC is also a potential exchange format that DoE is considering.

Section 6.4: TrendMicro Sharing System

- TBD

Progress

- Section 2 (ISAC Support) : done?
  - APWG, ACDC, REN-ISAC
- Section 3 (Open Source Implementations) : done?
  - EMC/RSA RID Agent, NICT IODEF-SCI, NASK n6
- Section 4 (Vendor Implementations) : done?
  - Deep Secure, IncMan, Surevine PoC, MANTIS
- Section 5 (Vendor with planned support) : done?
  - Threat Central
- Section 6 (Other implementations) : ongoing
  - CIMS, AirCERT, CyberFed, TrendMicro(TBD)
- Section 7 (Implementation Guide) : done?
  - Code generators, libraries, usability tips

Summary

- Update status and progress
  - Base: draft-moriarty-mile-implementation-report-00
  - Updates in IETF90
    - MANTIS (in section 4.4)
    - Implementation Guide (draft-daisuke-iodef-experiment-00, in section 7.1, 7.4)
  - Updates in IETF91
    - CIMS (in Section 6.1), n6 (in section 3.3), and updates* (added new section)
  - Updates in IETF92
    - Iodelib amd iodef.pm (in section 7.2 and 7.3) and updates* (status updates)
  - Updates in IETF93
    - APWG, ACDC, and REN-ISAC (in section 2.1, 2.2 and 2.3)
    - AirCERT, CyberFed (in section 6.2 and 6.3)
  - Envisioned updates in IETF94
    - TrendMicro Sharing System

Acknowledgement

This work is materially supported by the Ministry of Internal Affairs and Communication, Japan, and by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 608533 (NECOMA).