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 5
  - DAEDALUS, NICT (Planned Support)
- Update in Section 6

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) close (IETF93)
- #10: Other implementations (section 6) close (IETF93)

- #11: DAEDALUS (section 5) open (IETF94)
- #12: Other implementations (section 6) open (IETF94)

Section 5.2: DAEDALUS, NICT

- DAEDALUS is a real-time alert system based on a large-scale darknet monitoring facility that has been deployed as a part of the nicter system of NICT, Japan. DAEDALUS consists of an analysis center (i.e., nicter) and several cooperate organizations. Each organization installs a darknet sensor and establishes a secure channel between it and the analysis center, and continuously forwards darknet traffic toward the center. In addition, each organization registers the IP address range of its livenet at the center in advance.

- When these distributed darknet sensors observe malware activities from the IP address of a cooperate organization, then the analysis center sends an alert to the organization.

- The future version of DAEDALUS will support IODEF for sending alert messages to the users.

Section 6.4: TrendMicro Sharing System

- (TBD) in IETF92-93
  - => This section was deleted.

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, DAEDALUS
- Section 6 (Other implementations) : done?
  - CIMS, AirCERT, CyberFed
- 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)
  - Updates in IETF94
    - DAEDALUS (in section 5.2)

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).