MILE Implementation Report

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

Overview

- Updates for Implementation Guide (Section 7)

- Update for some implementations

Issues

- #1: MANTIS framework (section 4) close (IETF90)

- #2: Implementation Guide (section 6) close (IETF90)

- #3: CIMS (section 4) close (IETF91)

- #4: n6 (section 4) close (IETF91)

- #5: section title close (IETF91)

- #6: iodeflib (open)

- #7: iodef.pm (open)

- #8: updates for implementation (open)

#6: iodeflib

- Iodeflib
  - is an open source modules written in Python
  - parses and edits IODEF documents
  - is designed as simple as possible
    - PYX can generate such module from IODEF XSD, however, the generated module tends to inherit the complexity of XSD.

- Section 7.2 (Implementation Guide)

#7: iodef.pm

- Iodef.pm
  - is an open source module written in Perl
  - parses and edits IODEF documents
  - provides a simplified interface
    - translate key-value pairs to IODEF representations

- Section 7.3 (Implementation Guide)

#8: updates for implementation

- Done
  - Other implementations => Open source
    - n6SDK: "Other implementations" -> "Open source" https://github.com/CERT-Polska/n6sdk

- Envisioned updates
  - Community support
    - APWG: "planned to support" -> "supported"
      - eCRISP-X (APWG) http://docs.apwg.org/iodefFormat.html
    - REN-ISAC: "supported"
      - RINO-IODEF (REN-ISAC) http://www.ren-isac.net/notifications/using_iodef.html

Summary

- Update Status
  - Base: draft-moriarty-mileimplementation-report-00
  - Update in IETF90
    - 1. Vendor implementation (MANTIS in section 4.4)
    - 2. Implementation Guide (draft-daisuke-iodef-experiment-00, in section 6.1, 6.2)
  - Update in IETF91
    - 3. CIMS (in section 4.5)
    - 4: n6 (in section 4.6)
    - 5: section category
  - (Envisioned) Updates in IETF92
    - 6: iodefIf.lib (in section 7.2)
    - 7: iodef.pm (in section 7.3)
    - 8: updates for implementations

Acknowledgement

- This work is materially supported by NICT and 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).