MILE Implementation Report

Chris Inacio, Carnegie Mellon University
Daisuke Miyamoto, The University of Tokyo

Overview

- This is …
  - draft-mile-implementationreport-00 (IETF90)
- Related drafts are…
  - draft-moriarty-mile-implementationreport-00 (IETF89)
  - draft-daisuke-iodef-experiment-00 (IETF89)
- Two updates are …
  - #1: Update for vendor implementations
    - 4.4. MANTIS Cyber-Intelligence Management Framework
  - #2: Update for implementation guide
    - 6. Implementation Guide

#1: Vendor implementation…

- 4.4. MANTIS Cyber-Intelligence Management Framework
  - MANTIS provides an example implementation of a framework for managing cyber threat intelligence expressed in standards such as STIX, CybOX, IODEF, etc.

#1: …Vendor implementation

- To aide discussions about emerging standards such as STIX, CybOX et al. with respect to questions regarding tooling: how would certain aspect be implemented, how do changes affect an implementation? Such discussions become much easier and have a better basis if they can be lead in the context of example tooling that is known to the community.
- To lower the entrance barrier for organizations and teams (esp. CERT teams) in using emerging standards for cyber-threat intelligence management and exchange.
- To provide a platform on the basis of which research and community-driven development in the area of cyber-threat intelligence management can occur.

#2 Implementation Guide…

- 6.1 Code Generators
  - Tips for generating native class files from IODEF XSD (in RFC 5070)
  - In cases of Perl, Ruby, Python, Java, C++, and C#

#2 ···Implementation Guide

- 6.2 Usability
  - Here notes some tips to avoid problems.
  - IODEF has category attribute for NodeRole class. Though various categories are described, they are not enough. For example, the case of web mail servers, you should choose either "www" or "mail". One suggestion is selecting "mail" as the category attribute and adding "www" for another attribute.
  - The numbering of Incident ID needs to be considered. Otherwise, information, such as the number of incidents within certain period could be observed by document receivers. For instance, we could randomize the assignment of the numbers.

Summary

- Update Status
  - Base: draft-moriarty-mileimplementation-report-00
  - Update
    - 1. Vendor implementation (MANTIS in section 4.4)
    - 2. Implementation Guide (draft-daisuke-iodef-experiment-00, in section 6.1, 6.2)

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).