Information Model Update

SACM WG Virtual Interim Meeting

03/09/2016

Agenda

- Status
- Discussion
- Next steps

Status

- Integrated IPFIX syntax[1] into the IM
  - Expanded the framework to show how the IPFIX syntax should be used
  - Converted many of the existing SACM IEs to the IPFIX syntax
- Reviewed and reused existing IPFIX IEs and data types[2]
- Removed sections related to reports[3]
- Cleaned up other text throughout the document

1. https://tools.ietf.org/rfc/rfc7012.txt
2. http://www.iana.org/assignments/ipfix/ipfix.xhtml
3. http://www.ietf.org/mail-archive/web/sacm/current/msg03813.html

High-level list of things we reused

IEs

- Protocol identifier
- Src/dest IP address, prefix, port
- Exporter/collector IP address
- Interface name, description, index, etc.
- Application identifier, name, etc.
- MIB

Data Types

- Integer, float
- String
- MAC address
- IPv4 address, IPv6 address
- Boolean
- Date/time

How to indicate special things about an IE?

- Want to use IEs to represent objects, attributes, and metadata
  - Is the IE metadata?
  - Is the IE mandatory-to-implement for designation purposes?
  - Are there privacy concerns associated with the IE?

- A few options:
  - We could add properties for all these things
  - We could group the IEs in certain sections
  - Add a new property for this (or possibly generalize data type semantics)

Next steps

- Finish updating the IM
- Post the updated IM by the end of next week (possibly sooner)
- Solicit WG for feedback on mandatory-to-implement IEs
  - Architecture and Requirements
  - Vulnerability Assessment Scenario
  - Existing data models (SCAP, CIM, SWID, APP-ID, etc.)