Software Message and Attributes for PA-TNC

draft-coffin-sacm-nea-swid-patnc-02

SACM Virtual Interim Meeting – IETF 95
October 13, 2016
Status

• Delivered version -02 on Sept 12
• Recently updated GitHub repository
  • https://github.com/sacmwg/software-identification
  • Currently 7 tracked issues
Issue #7: Nature of reported software

• Mailing list discussion in August identified 3 classes of endpoint software
  • Installed
  • Running
  • Installation packages
• All three classes are of interest to SACM
  • Question is which should be reported in SW M&A
• Currently (-02) SW M&A reports only installed software
Issue #2 – Include Software ID in all messages

• Currently, Software ID is not included if the full record is delivered
  • Software ID is derived from the full record
  • Doing so requires recipient to be able to parse full record

• Proposal to include Software ID as a separate field for each reported software (even if full record is delivered)
  • Redundant in company of a full record, but recipient no longer needs to parse the record.
Issue #3 – Include Installation Location in all messages

• Installation location might or might not appear in a full record
  • Even if present, message recipient needs to be able to parse to discover

• Statement made that location (+ Software Identifier) are necessary for many use cases
  • E.g., patching – Software ID = “whether to patch”; location = “where to patch”

• Proposal is to have a designated Installation Location field for each reported piece of software
Issue #6: MTI Data Models

• Currently SW M&A identifies 2 data models
  • ISO SWID 2015 XML
  • ISO SWID 2009 XML
  • Other data models can be added

• Should there be one or more MTI data models?

• What does MTI mean here?
  • We cannot necessarily control how data sources will report
  • Only technical dependency is that endpoints need to be able to derive a Software ID from the full record (expressed in a recognized data model)
Issue #4: User-defined data models

- The current design does not support identification of data models except through references defined in an IANA table
- Proposal: add way to support vendor/user-defined data models

- One proposal: currently, Data Model Type is 8 bits
  - Most Significant Bit $\rightarrow$ 0 = IANA table, 1 = non-standardized
  - $2^{\text{nd}}$ Most Significant Bit $\rightarrow$ 0 = User-defined, 1 = Vendor defined
  - Vendor, and user can each define 64 data models; IANA can define 128
  - Agreement on meaning of non-standardized data models left to implementers
Issue #1: Identification of data sources

• Issue #1
  • In IETF 94 there were many in favor of adding a field to track the source of reported information

• Issue #5
  • SW M&A servers have no requirement to be able to parse delivered records
  • Proposal: explicitly state that SW M&A servers MUST accept any data model received without error
Next Steps

• Any other issues?

• -03 by 10/31 (pending consensus on open issues)
BACKUP
NEA Architecture

* Not currently part of NEA, but part of the compatible TNC architecture
Change Tracking in SW M&A

- Posture Collectors MUST monitor their software information sources for changes
  - Can be real-time or periodic monitoring
- Each change is assigned a unique, sequential “event number”
- All event numbers have an associated “event epoch”
- Within an epoch, event numbers fully order all change events
- All inventories are reported along with the event number and epoch of the last recorded event at time of inventory
  - Given this and a list of subsequent events, one can track all changes just using deltas
  - Epoch changes represent discontinuities – no way to track across
SW M&A Message Flows: Demand-Driven (Pull)

- 4 types of Response attributes depending on Request parameters
  - SW Inventory – Complete or targeted inventory expressed in data model
  - SW Identifier Inventory – Complete or targeted inventory using software IDs
  - SW Events – Changes since a given event number using in data model
  - SW Identifier Events – Changes since a event number using software IDs
SW M&A Message Flows: Event-Driven (Push)

Subscription Established

Change Event

Posture Collector

Posture Validator

SW Request

SW Response

SW Response

SW Response

...