SWID Message and Attributes for PA-TNC

draft-coffin-sacm-nea-swid-patnc-00

SACM WG Meeting – IETF 95
April 6, 2016
Agenda

• Overview

• Role in SACM

• Questions and Open Issues

• Next Steps
Overview

• Standardizes reporting of endpoint software inventory information
• Uses SWID tag (ISO/IEC 19770-2:2015)\(^1\) information
• Utilizes NEA (RFC 5209)\(^2\) PA-TNC (RFC 5792)\(^3\) for messaging

• Capabilities
  • Report full inventories or targeted inventories (only report items of interest)
  • Report inventories or list of change events (deltas)
  • Can identify software using full SWID tag or just the unique tag identifier
  • Supports demand-driven (pull) and event-driven (push) delivery

2. [https://datatracker.ietf.org/doc/rfc5209/](https://datatracker.ietf.org/doc/rfc5209/)
Role in SACM

• Endpoint Identification and Assessment Planning use case (section 2.1.2 of Endpoint Security Posture Assessment: Enterprise Use Cases\(^1\))
  • Help understand software inventory of endpoints
  • Can direct further assessment/actions based on vulnerabilities present, application-specific policy, etc.

• Endpoint Posture Attribute Value Collection use case (section 2.1.3 of Endpoint Security Posture Assessment: Enterprise Use Cases\(^1\))
  • Provides details about endpoint software inventory
  • Can produce real-time updates as this inventory changes

• An endpoint’s collected SWID tags can be used by other security tools to make further assessments without additional contact with the endpoint

SWID M&A in the NEA Architecture

Endpoint
+-------------------------+
|                         |
| +-------------------------+ |
| | SWID                    |
| | SWID M&A                |
| | Posture                 |
| | Collector               |
| +-------------------------+ |
|                         |
| +-------------------------+ |
| | IF-IMC*                 |
| +-------------------------+ |
| | PB Client               |
| +-------------------------+ |
| | PT Client               |
| +-------------------------+ |

Server
+-------------------------+
|                         |
| +-------------------------+ |
| | SWID                    |
| | SWID M&A                |
| | Posture                 |
| | Collector               |
| +-------------------------+ |
|                         |
| +-------------------------+ |
| | IF-IMV*                 |
| +-------------------------+ |
| | PB Server               |
| +-------------------------+ |
|                         |
| +-------------------------+ |
| | PT Server               |
| +-------------------------+ |

* Not currently part of NEA, but part of the compatible TNC architecture
SWID M&A Message Flows: Demand-Driven (Pull)

- 4 types of Response attributes depending on Request parameters
  - SWID Tag Inventory – Complete or targeted inventory expressed in SWID tags
  - SWID Tag Identifier Inventory – Complete or targeted inventory using tag IDs
  - SWID Tag Events – Changes since a given event number using in SWID tags
  - SWID Tag Identifier Events – Changes since a event number using tag IDs
Change Tracking in SWID M&A

• Posture Collectors MUST monitor their SWID tag collection 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, can track all changes just using deltas
  • Epoch changes represent discontinuities – no way to track across
SWID M&A Message Flows: Event-Driven (Push)
Issue 1: Removal of IF-IMV/IF-IMC references

- SWID M&A includes normative references to IF-IMC\(^1\) & IF-IMV\(^2\)
  - TNC standards that we plan to (and have TCG permission to) submit to SACM but have not yet finished the conversion
  - Given the current document load on SACM, we are thinking of delaying submission
- IF-IMC & IF-IMV references detail use of specific functions to collect unique identifiers for Posture Collectors (IMCs) and Posture Validators (IMVs) (in addition to endpoint IDs)
- Unique IDs for Posture Collectors and Posture Validators are provided in PB-TNC messages\(^3\)
  - Can just say these IDs SHOULD be recorded and used when possible
  - Only difference is that we no longer name specific functions by which these IDs get from the PB to the PA layer of NEA

---

1. [http://www.trustedcomputinggroup.org/resources/tnc_ifimc_specification](http://www.trustedcomputinggroup.org/resources/tnc_ifimc_specification)
2. [http://www.trustedcomputinggroup.org/resources/tnc_ifimv_specification](http://www.trustedcomputinggroup.org/resources/tnc_ifimv_specification)
Issue 2: Support for SWID 2009

• There are two versions of the SWID standard: 2009 and 2015
  • Currently SWID M&A supports both

• Could drop the requirement to support 2009 SWID tags
  • Simplifies procedure for collecting unique SWID identifiers (one method instead of multiple)
  • Removes the need to monitor and report changes to tags (2015 tags cannot be edited – only replaced)
  • Simplifies interoperability since recipients only need to parse one type of tag

• Downside: Lose support for existing 2009 tags, but those should be a small minority in the near future
Issue 3: Report SWID tag versions

• There can be revisions of tags, tracked by the tagVersion field
  • A tag can be revised to fix errors and to add new metadata
  • Tag Identifiers are the same for all revisions of a tag (Unique tag identifiers correspond to the associated software product, not to the tag itself)

• Currently, when reporting tag identifiers SWID M&A doesn’t mention version
  • Tag identifiers for different versions of the same tag look the same

• Is there a need to track new versions of a tag?
Issue 4: Denoting Tag Bindings

• Assuming multiple tag bindings are supported (regardless of whether one or more are MTI)...

• Currently SWID M&A does not identify the binding of contained tags

• Is it important to identify the binding of a tag in the message?
  • If so, what is the best way to do so?
  • What about multiple bindings in the same exchange?
Issue 5: MTI Tag Bindings

• The ISO SWID specification defines a normative XML schema for SWIDs
  • However, other bindings are possible. See recent I-D for a CBOR SWID binding (draft-birkholz-sacm-coswid-00)

• Should there be an MTI binding for SWID tags (XML? CBOR? JSON?)
  • If so, should that be specified in SWID M&A?
    • Currently, SWID M&A is agnostic to the bindings it conveys?
  • Or, should the MTI SWID binding be identified in a higher-level spec? (E.g., the ECP?)

Next Steps

• Would like to adopt the SWID messaging concept as a WG draft
  • Continue to work on this draft within the working group

• Identify other people (beyond current authors) who can provide input/feedback
  • We need more review
  • Could also use help with authoring the draft

• Ultimately would like to see this published as a standards-track RFC