SWID Message and Attributes for PA-TNC

SACM WG Virtual Interim Meeting

03/09/16

Agenda

- Overview
- Alignment with SACM
- Next steps

Overview

- Extension to NEA PA-TNC[1] to support the collection and exchange of software inventory data using ISO Software Identification (SWID)[2] tags

- SWID PCs are required to monitor all tag data stores
    - Natively stored
    - Generated

- Collection can be driven by the endpoint, a server, or an event
    - Creation
    - Deletion
    - Alteration

[1] https://datatracker.ietf.org/doc/rfc5792/

[2] http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670

Alignment with SACM Use Cases[1]

- Define, publish, query, and retrieve security automation data
  - Provides very basic guidance for collectors
  - Provides a data model for representing software inventory data

- Endpoint identification and assessment planning
  - Software inventory data, expressed as SWID tags, supports endpoint discovery and characterization

- Endpoint posture attribute collection and evaluation
  - Informs the acquisition of collection and evaluation guidance
  - Collects and evaluates posture attribute values expressed as SWID tags
  - Supports change detection as well as other collection and evaluation triggers

[1] https://datatracker.ietf.org/doc/rfc7632/

Alignment with SACM Architecture[1]

- PVs may subscribe to PCs and receive updates to SWID tag data stores
  - Change detection subscription
  - Inventory subscription
  - Event record subscription
  - Targeted subscription
  - Delayed subscription

[1] https://datatracker.ietf.org/doc/draft-ietf-sacm-architecture/

Alignment with the SACM Information Model[1]

- Provides a data model by which to express software inventory data which is represented in the IM as a software instance

```
elementId: 15
name: softwareInstance
dataType: subTemplateMultiList
status: current
description: Information about an instance of software
             installed on an endpoint. The following
             high-level digram describes the structure of
             softwareInstance information element.

            softwareInstance = (subTemplateMultiList, allof,
                softwareIdentifier,
                title,
                creator,
                softwareVersion,
                lastUpdated
            )
```

[1] https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/

Alignment with SACM Vulnerability Assessment Scenario[1]

- Provides a mechanism by which NEA can be leveraged to collect software inventory data using SWID tags
  - Endpoint characterization
  - Guidance applicability
  - Vulnerability status

- Makes this information available to other SACM Components

[1] https://datatracker.ietf.org/doc/draft-coffin-sacm-vuln-scenario/

Next steps

- Update this I-D based on feedback

- Request a call for adoption