Software Inventory Message and Attributes for PA-TNC

IETF 97

11/15/2016

draft-coffin-sacm-nea-swid-patnc-03

Agenda

- Status

- Open issues

- Next steps

Status

- Discussed during the SACM WG Virtual Interim Meeting on 10/13[1]
- Submitted revision -03 on 10/31[2] which addresses:
  - Issue #2: include software identifiers in all reports[3]
  - Issue #7: focus on the collection of installed software only[4,5]
- Plan to update the name of the I-D from "SWID M&A" to "Software Inventory M&A"

[1] https://www.ietf.org/proceedings/interim-2016-sacm-06/minutes/minutes-interim-2016-sacm-06-201610131400-00

[2] https://github.com/sacmwg/software-identification/blob/master/draft-coffin-sacm-nea-swid-patnc-03.xml

[3] https://github.com/sacmwg/software-identification/issues/2

[4] https://github.com/sacmwg/software-identification/issues/7

[5] https://www.ietf.org/mail-archive/web/sacm/current/msg04476.html

Issue #3: Include the installation location of software[1] (1 of 3)

- General WG consensus for adding a software installation location field to the software inventory message[2].
- Text was included in -03[3] adding a "Software Locator" to the software inventory message.
- "Software Locator" contains a single URI to represent the installation location.
- The I-D defines two schemes, but these can be extended:
  - file: the location is relative to the endpoint's local file system
  - unknown: the location cannot be determined with any reasonable degree of confidence
- Location SHOULD be the "root directory" of the software's executables
  - The location SHOULD be the location of the primary executable

[1] https://github.com/sacmwg/software-identification/issues/3

[2] https://www.ietf.org/mail-archive/web/sacm/current/msg04008.html

[3] https://tools.ietf.org/html/draft-coffin-sacm-nea-swid-patnc-03#section-3.2.1.2

Issue #3: Include the installation location of software[1] (2 of 3)

```
                      1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Flags         |             Record Count                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Request ID Copy / Subscription ID              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            EID Epoch                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Last EID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Record ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Software Identifier Length      |  Software Locator Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Record Length                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Data Model Type|       Software Identifier (variable length)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Software Locator (Variable length)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Record (Variable length)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Issue #3: Include the installation location of software[1] (3 of 3)

- There was a concern that in some cases it may be difficult to determine the location (e.g. on RAM, on remote file systems, may change over time, etc.)
    - Does the proposed solution address this concern?
- “unknown” is not an IANA registered URI scheme[2]
- Another option for handling the “unknown” scenario
    - Use a 0 byte length for the “Software Locator”?
    - Any preference?

[1] https://github.com/sacmwg/software-identification/issues/3
[2] http://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml

Issue #4: Support user/vendor-defined data models[1]

- Currently, the I-D only supports the use of data models identified in the proposed IANA registry. It does not permit user/vendor extensions.

- One proposal to support user/vendor extensions:
  - Current Data Model Type is 8 bits
  - Most Significant Bit → 0 = IANA registry, 1 = non-standardized
  - 2nd Most Significant Bit → 0 = User-defined, 1 = Vendor-defined
  - Vendor and user can each define 64 data models; IANA can define 128 data models
  - Agreement on meaning of non-standardized data models left to implementers

- Do we want to support user/vendor extensions? Do we like this proposal?

1. https://github.com/sacmwg/software-identification/issues/4

Issue #1: Identification of data sources[1]

- WG interest around including the data source of each software record[2,3]. Useful because data sources may have:
    - Different degrees of trust
    - Varying rates of change detection

- Possible data sources include: file system, package managers, software discovery tools, etc.

- Do we want to add a data source field to the software inventory message?

[1] https://github.com/sacmwg/software-identification/issues/1

[2] https://www.ietf.org/proceedings/95/minutes/minutes-95-sacm

[3] https://www.ietf.org/mail-archive/web/sacm/current/msg04038.html

Issue #5: Clarify that SW M&A servers must accept all data models[1]

- SW M&A does not impose any requirements that would require a SW M&A server to be able to parse or understand a data model payload

- As a result, it has been recommended that the I-D be explicit about SW M&A servers being able to accept all data models delivered to them without error or complaint

- Is there WG consensus to make this change?

[1] https://github.com/sacmwg/software-identification/issues/6

Issue #6: MTI data models[1]

- The I-D currently supports two data models:
  - ISO 2009 SWID Tags (XML)[2]
  - ISO 2015 SWID Tags (XML)[3][4]
- Concise Software Identifiers[5] is another option, but, not currently supported in the I-D
  - ISO 2015 SWID Tags (CBOR)
- Which of these data models should be MTI?
  - Are there other data models that need to be considered?
  - Do MTI data model requirements belong in this I-D or in another I-D?
  - Still need to define the process by which an endpoint derives a software identifier from a data model instance. Do we want this to be a SHOULD requirement?

[1] https://github.com/sacmwg/software-identification/issues/6

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

[3] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=65666

[4] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf

[5] https://datatracker.ietf.org/doc/draft-birkholz-sacm-coswid/

Next steps

- Resolve remaining issues on the mailing list

- Post next draft as draft-ietf-sacm-nea-patnc-swima-00

- Work towards a WGLC early next year (January-February timeframe)