SWID Message and Attributes for PA-TNC

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

https://datatracker.ietf.org/doc/draft-coffin-sacm-nea-swid-patnc/

SACM Virtual Interim Meeting

May 17, 2016

Agenda

- Review Consensus from previous meeting
- Open issues

Issues with consensus

- Removal of references to TNC's IF-IMV & IF-IMC
  - Should have no real impact on capabilities
- Retain support for 2009 SWID tags
  - Both 2015 and 2009 tags will remain supported, but language around specific support on each tag version will be clarified
- XML will be a MTI binding in SWID M&A
  - XML is how virtually all SWID tags are expressed today
- Target: have a revised specification incorporating these changes before the next VIM on June 15

Old Semi-open Issues

- SWID tag versions
  - Consensus that product versions need to be tracked, but SWID tag versions are not needed for that
  - Tag version needed if using endpoints as data sources of tag metadata, but has no impact on inventory reporting
    - Example of tag metadata would be Payload fields, which might provide file integrity golden measurements
  - If tag versioning still important, technical mechanism still needs to be developed
- How to mark the binding (XML, CBOR, etc.) of a contained tag
  - Consensus that messages need to indicate the binding, but technical details still open
- Target: Have technical proposals to the group ahead of the next VIM on June 15

New Issue – Software Location

- SWID tags do not necessarily include the location of the software that they report
- Some follow-on activities would need to know software location
- Pros to adding software location
  - Easier to distinguish multiple software instances from double reporting
  - Follow-on activities have more information
- Cons
  - There is not always a mechanical way to determine software location given a SWID tag
- If we want to do this, the SWID Instance Identifier can contain the software location – meet two needs at once
- Meta-question – to what extent should SWID M&A attempt to anticipate the needs of follow-on activities?

New Issue – Source Management

- SWID tags can come from multiple sources
  - E.g., collected from file system, generated from package manager, output from inventory checking tools, etc.
- Currently different sources are not distinguished in SWID M&A
  - All sources combined into the endpoint SWID tag collection
  - Sources are not distinguished when reporting
- Pros to differentiating sources
  - Easier to distinguish multiple software instances from double reporting
  - Not all sources can detect changes at the same rate – clarify reporting
- Cons
  - Increases the size of messages and complexity of endpoint behavior
- Is it worth the trade off? How would knowing this change behavior?

Next Steps

- Integrate consensus changes into the SWID M&A draft by June 15 VIM
  - Remove IF-IMV/IF-IMC references
  - Clarify SWID 2009/2015 usage text
  - State XML binding as MTI
- For more technical changes, develop proposals and socialize them on the mailing list before June 15 VIM
  - Binding identification in SWID messages
  - SWID tag version (if accepted)
  - Application location (if accepted)
  - SWID tag source identification (if accepted)
- Continue to solicit suggestions and proposals