Information Model Update

IETF 97
11/15/2016
Agenda

• Open issues

• Next steps
Issue #68: IM/DM-related questions (1)¹

• At the last two VIMs²³ and on list⁴, there were discussions around how to best focus the IM work around leveraging existing data models (CIM, Configuration Profiles, MIB, YANG, SWID, OVAL, etc.)
  • Experience with OVAL tells us one data model is not enough
  • Seems to be consensus on accommodating multiple data models

• Feedback on IEs is there are too many :). Would like to see it trimmed:
  • Re-introduction of envelope constructs (statement, content element, etc.)
  • Metadata necessary for tasks, enabling provenance, and DM comprehension
  • Core endpoint concepts based on VAS and existing security checklists
  • Guidance and assessment results

1. https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/68
2. https://www.ietf.org/proceedings/interim-2016-sacm-05/minutes/minutes-interim-2016-sacm-05
3. https://www.ietf.org/proceedings/interim-2016-sacm-06/minutes/minutes-interim-2016-sacm-06-201610131400-00
Issue #68: IM/DM-related questions (2)

• SACM End Goal: Using a standardized framework, enable end users to discover, characterize, collect, evaluate, query, and store security automation information independent of the underlying protocols and data models in use

• Just to clarify, by standardized framework, I mean:
  Interfaces, operations, tasks, and information needs

• Does this align with others’ vision for SACM?
Issue #68: IM/DM-related questions (3)

• How do we get there? (note: this doesn’t all belong in the IM)
  • Define the tasks we want to support including inputs and outputs
  • Define the information needs we care about and identify existing data models that support them
  • Determine how to unify data across existing data models. Two approaches:
    • Leverage the IM as the common mapping between data models
    • Provide metadata necessary to enable vendors to transcode data between data models
  • Define the operations and interfaces necessary to standardize the interactions between SACM Components while executing tasks
Issue #68: IM/DM-related questions (4)

• Leverage the IM as the common mapping between data models
  • More work to do on the front end (enumerate needs, define in IM, map DMs to IM)
  • Vendors don’t need to create mappings
  • Should result in improved consistency among tools

• Provide metadata necessary to enable vendors to transcode data between data models
  • Less work to do on the front end
  • Pushes mapping work to each vendor
  • Is there the potential for inconsistencies in vendor-defined mappings?

• Is there a preference on which approach we take?
Issue #67: Uniqueness of attribute and subject names

• Are the names of attributes and subjects unique within the IM or are they unique to the instance of the attribute or subject?

• The IE naming convention states:
  • Names MUST be unique within the SACM registry. Enterprise-specific names SHOULD be prefixed with a Private Enterprise Number [PEN]

• This implies that attribute and subject names are unique within the registry that defines the IM as well as any subsequent extensions

• Is the naming convention sufficient or is explicit text required?

Issue #10: Differentiating classes of software

- The IM includes OS-specific attributes (osName, osType, osVersion, etc.) as well as a generic software subject (softwareInstance)

- It seems the WG would support either software-specific attributes or a generic software subject that includes a classification attribute
  - Installation location of software and privileges are also of interest to the WG
  - CIM SoftwareIdentity and RFC 2790 each provide a list of software classes

- Supporting both options is redundant, is one option more appealing than the other?

Next steps

• Continue resolving open issues on the mailing list