A Proposed SACM Information Model

with implications to a SACM Data Model

Henk Birkholz

Nancy Cam-Winget

Proposal

- SACM Information Model
  - Defines structure for Data Models guidance
  - Defines guidance on SACM interfaces
    - Can include Data Model Guidance
    - Can include inference to Data Model operations

Proposed Information Model

- Intention is to provide structure to SACM information layout
- Structure is a container that includes:
  - Description of the SACM information (metadata)
  - The content itself
- The Structure allows for different Data Models

Information Model Abstract

- Highest level ➔ SACM statement
  - Statement Metadata
    - Globally Unique ID (of Statement)
    - Data Origin (of Statement)
    - Data Source (of Content)
    - Creation Timestamp (of Statement & Content)
    - Publication Timestamp (of Statement)
    - Type (of Content)
  - Statement Content
    - The Proposed DM
    - Additional DMs OVAL, SCAP(-AI), DMTF CIM, etc.

Structure of the DM Content Format provided by the IM

- IM MUST define elements to proof inter-operability and use-cases
  - Being too abstract is (probably) bad
  - BUT some abstraction is needed to allow agility
- Should the elements be abstract, e.g. by defining semantic structures that provide guidance to DM defintions?
- Example: What is the “atomic leaf“ for: Address, IPAddress, IPv6Address
  - DM decision? Probably varies from DM to DM

Structure of SACM Content

- Statement Content includes one or more:
  - Atomic Elements
  - Grouped Elements
  - Categorized Elements

- Statements can be Categorized Elements themselves
  - “recursive“ nesting to facilitate correlation, relay, etc.

Structure of the DM Content Format provided by the IM

- Grouping (has_a)
    - Example: NETWORK
        - IPAddress
        - SubnetMask
- Categorizing (is_a)
    - Example: Address
        - IPAddress
            - IPv6Address

SACM defines a MUST set of elements

- A set of Elements will be defined and (most?) identified as MUST to ensure interoperability

- Elements have clear semantic understanding to allow DMs to map to SACM’s intent

Element sample

- Atomic Elements:
  - IPv4Address
  - IPv6Address
- Grouped Element:
  - Endpoint
    - Endpoint Identifier
    - <other elements that can identify the Endpoint>

- Categorized Element
  - Software Asset
    - Software Identifier
    - Software version
    - <other elements to identify the asset>

Next steps

- Is there enough interest in this approach for presenters to generate draft text and detail the structure and elements?

Comments?

Terms and Mapping of Terms

- One set of IM Terms for Atomic Elements (Canon)
- Various sets of DM terms (already existing and future ones)
- A mapping/dictionary is required that should be part of each DM
  - Mapping DM Terms with IM Terms
- The atomic elements included in the DM content format are intented to be 100% in sync with the IM Terms