SUITable CoSWID Tags

Henk Birkholz (FhG SIT)

Jessica Fitzgerald-McKay (DoD)

Charles Schmidt (MITRE)

David Waltermire (NIST)

IETF SUIT Virtual Interim Feb 26th 2018

Synergy between SUIT & CoSWID

- Software Asset Management (SAM, e.g. ISO/IEC 19770-5:2013) is a common basis for Vulnerability Management (VM).
- ISO/IEC 19770-2:2015 Software Identification Tags documents are an established interoperable format to support the domains of SAM & VM.
- Concise Software Identifier (CoSWID):
  - are based on a well-know information model / semantic (e.g. NISTIR 8060)
  - revise some of the ambiguity found in 19770-2:2015, thereby improving interoperability
  - Employ CBOR/CDDL, thereby supporting lightweight transfer protocols (e.g. LwM2M)

Contributions to SUIT

- Concise Software Identification Tags:
  - are created to convey meta-data about software components
  - can include the actual software (“within reason”)
    - the intend is to include distinguishable binary blobs associated with a (composite) thing
  - Inherit the small CBOR “footprint”
    - Library, Stack & Data in Motion
  - inherit the “noise-less” efficiency CDDL
    - extensibility (e.g. extension points) and
    - guidance features (.within control)

SWID Capabilities

- Support of software enrollment pipeline en large
  - packaging (corpus tags)
  - distribution (counter signed tags)
  - deployment/drop-shipping (payload tags)
  - measurement (evidence tags)
  - modification (update/supplemental tags)
- Vendor specific extensions
  - part of the standard
  - CDDL mechanic soon to be in last call (finally…)

Semantic Interconnected Relationships

- Always assume that software is a composite
  - In consequence, if it is actually a monolithic/atomic piece of firmware: the software is a composite with only a single component
- Same concept is applied to firmware and the thing firmware is running on
  - there will always be dependencies between hardware components and software components – and between different software components / firmware components
- Current information elements included in CoSWID tags are based on RFC4108

Example Simple CoSWID Tag for Firmware

```
{
     15: "en-US",                                                         # language identifier
     0: "d16915af-8449-40ba-ad59-43ddf36280df",                           # tag id (UUID)
     12: 1,                                                               # tag version
     1: "Bootloader",                                                     # software name
     13: "1.0.0",                                                         # software version
     14: "multipartnumeric",                                              # software version scheme
     2: {                                                                 # entity object
          31: "Internet Engineering Task Force SUIT WG",                  # entity name
          32: "org.ietf",                                                 # entity id (a reversed domain name)
          33: ["tagCreator", "softwareCreator"]                            # entity roles indicating the entity
                                                                          # that created the tag and software
     },
     6: {                                                                 # a collection of resources related
                                                                          # to the software
          59: {                                                           # a firmware resource
               60: "firmware.bin",                                        # the name of the firmware resource
               58: [1, h'78338 ..snip.. AC4ED’]                           # A SHA-256 hash
          }
     }
}
```

Next Steps

- Future refinement of these basic information elements will be continued in I-D in succession of the initial CoSWID I-D
- Once SUIT requirements are better defined, firmware support can be expanded
  - Device identification (e.g., device-group-id, device-id)
  - Directives / conditions
  - Refinement of COSE use
  - etc.