Concise Software Identities

Henk Birkholz henk.birkholz@sit.fraunhofer.de

Jessica Fitzgerald-McKay jmfitz2@nsa.gov

Charles Schmidt cmschmidt@mitre.org

David Waltermire david.waltermire@nist.gov

"IETF 107", 1st Virtual Session, May 1st , SACM WG

I-D Status (Change Log)

- Moved key identifier to protected COSE header

- Fixed index reference for hash

- Removed indirection of CDDL type definition for filesystem-item

- Fixed quantity of resource and process

- Updated resource-collection

- Renamed socket name in software-meta to be consistent in naming

- Aligned excerpt examples in I-D text with full CDDL

- Fixed titles where title was referring to group instead of map

- Added missing date in SEMVER

- Fixed root cardinality for file and directory, etc.

- Transformed path-elements-entry from map to group for re-usability

- Scrubbed IANA section

- Removed redundant supplemental rule

Signed CoSWID & Hash Digests

- CoSWID effectively "uses" two IANA algorithm registries:

  - the "Named Information Hash Algorithm Registry" for hash values inside the CoSWID structure, and

  - the "COSE Algorithms Registry" for signing the CoSWID structure via a COSE container.

- The discussion on the list ended in a proposal to proceed as illustrated above.

- Is this the WG consensus?

Implementation Status

- Java-based SWID tools:
  https://github.com/usnistgov/swid-tools/tree/master

- Documentation/Overview:
  https://pages.nist.gov/swid-tools/

- Maven Build-Management-Tool support:
  https://search.maven.org/search?q=g:gov.nist.secauto.swid

WG Status

- I-D is in WGLC status, but does not have an Shepard assigned.

- Next steps?
  - Shepard
  - WG Consensus

- And then the is a potentially open topic related to CoSWID (on the next slide).

CWT & CoSWID

- Both signed and unsigned CoSWID tags are required in the field.
- As work on Unprotected CWT Claims Sets (UCCS) has started, the topic of using CWT as a CoSWID flavor could be revisited.
- Is there still an interest in pursuing this?
  - CoSWID RIM – reference integrity measurements / reference values – could benefit from Claims "surrounding" a RIM tag to express semantics, such as "iat", or "exp"/"bbf".
  - Maybe UCCS is a good place to discuss this more?

Questions?