draft-moran-suit-manifest-03

Brendan Moran
Hannes Tschofenig
2018-11-08
Changes from draft-moran-suit-manifest-02

• Many changes due to input from mailing list, meetings, and hackathons
• New COSE_Digest
• Severable fields—similar to COSE’s detached payload
Agenda

• COSE_Digest
• draft-moran-suit-manifest-03 examples
• Summary of changes from draft-moran-suit-manifest-02
COSE_Digest

• COSE_Digest identical to COSE_Mac0
• Digest is used instead of MAC (key ID is irrelevant)
• Context is “Digest” instead of “MAC0”
COSE_Digest CDDL

COSE_Mac0 = [  
    Headers,
    payload : bstr / nil,
    tag : bstr,
  ]
COSE_Digest = COSE_Mac0  
COSE_Digest_Tagged =  
#6.19(COSE_Digest)

Digest_structure = [  
    context : "Digest",
    protected :  
        empty_or_serialized_map,
    external_aad : bstr,
    payload : bstr,
  ]
COSE_Digest Algorithm Identifiers

• Initial algorithms defined:
  • SHA-224
  • SHA-256
  • SHA-384
  • SHA-512
  • SHA3-224
  • SHA3-256
  • SHA3-384
  • SHA3-512

• Proposed Algorithm IDs: 40 to 47
• Unsigned manifest, no installation information, 1 payload

• Information to encode (37 bytes):
  • Sequence Number : 1 (1 byte)
  • Payload component : [h’30’] (2 bytes)
  • Payload size : 94430 (2 bytes)
  • Payload digest : (32 bytes)

• Encoded size: 67 bytes
• No authentication object provided
draft-moran-suit-manifest-03 example 1 (3/3)

{  
  1: null,  
  2: manifest (bstr)  
}

(1) Version 1  
(2) Sequence Number 1  
(5) 1 payload:  
  (1) Component: [‘0’]  
  (2) Size: 94430  
  (3) COSE_Digest:  
      Algorithm: SHA-256  
      digest
• Signed manifest, no installation information, 1 payload

• Information to encode (140 bytes):
  • Example 1 (37 bytes)
  • Key ID: (32 bytes)
  • Signature : (71 bytes) (DER-encoded secp256r1 signature)

• Encoded size: 191 bytes
{ 1: 98(COSE_Sign),  2: Manifest }  

[ 
  h'A103182A',
  {},
  null,
  [
    h'A10126',
    { 4: key id },
    signature
  ]
]

Protected:  
Content type: octet-stream  
Unprotected: none  
Payload: detached

COSE_Signature

Protected:
  Algorithm ID: ES256
Unprotected:
  key ID (digest of public key)
Signature
(1) Version 1
(2) Sequence Number 2
(5) 1 payload:
   (1) Component: ['0']
   (2) Size: 94430
   (3) COSE_Digest
• Signed manifest, no installation information, 1 payload
• Information to encode (428 bytes):
  • Example 2 (140 bytes)
  • Preconditions:
    • Vendor ID: 16 bytes
    • Class ID: 16 bytes
  • Payload URI: https://tools.ietf.org/html/draft-moran-suit-manifest-03 (56 bytes)
  • Text description: 200 bytes
• Encoded size: 605 bytes
• Encoded size with text pruned: 398 bytes
• Encoded size with text and installation info pruned: 319 bytes
(1) Version 1
(2) Sequence Number 2
(3) preinstall Info
   (1) Preconditions
       Vendor ID
       Class ID
(5) 1 payload:
   (1) Component: ['0']
   (2) Size: 94430
   (3) COSE_Digest
(6) Install Reference (COSE_Digest)
(8) Text Reference (COSE_Digest)
draft-moran-suit-manifest-03 example 3 (2/4)

{  
  1: 98(COSE_Sign),  
  2: Manifest,  
  4: InstallInfo,  
  6: TextInfo,  
}

(1) InstallationInfo
(1) Component ID: ['0']
(2) Processors
(1) Processor ID: Remote Resource
(2) Inputs:
   (1) 0 => URI

draft-moran-suit-manifest-03 example 3 (4/4)

{ 1: 98(COSE_Sign), 1: 200 bytes of Lorem Ipsum
  2: Manifest
  4: InstallInfo
  6: TextInfo
}

(1) Update Description

{ 1: 200 bytes of Lorem Ipsum
   1: 200 bytes of Lorem Ipsum
}

16
• Signed manifest, no installation information, 1 payload

• Information to encode (430 bytes):
  • Example 3 (428 bytes)
  • Source of reference material for bsdiff: ['0'] (2 bytes)

• Encoded size: 624 bytes
• Encoded size with text pruned: 417 bytes
• Encoded size with text and installation info pruned: 318 bytes
(1) InstallationInfo
   (1) Component ID: [‘0’]
(2) Processors
   (0) Remote resource
      1 URI
(1) Local resource
    component ID [“1”]
(2) Bsdiff unpack
    Diff stream => 0
    Local reference => 1
Summary of changes from 02 draft 1/2

• draft-moran-suit-manifest-02 was the starting place
• An outer container is expanded
• All COSE objects are used in detached payload mode
• A COSE_Digest structure is defined and used for all digests
• Most structures are constructed using CBOR Maps
• A manifest lifecycle is defined
  • Large manifest content can be pruned when not needed
Summary of changes from 02 draft 2/2

• More preconditions and predirecives are defined
• The processing graph is replaced with processing trees
• More processors are defined
• ResourceInfo and Processor are combined into a single structure
• Storagelentifier is absorbed into the ComponentIdentifier list