SUIT WG at Virtual IETF 110

Thursday, 11 March 2021 at 15:30 UTC

1) Logistics

- Agenda Bashing
  - Roman (Sec AD): The suit-reports document does not require recharter; however, the MUD document does require recharter.
- Minute Taker
  - Dave Thaler, Akira Tsukamoto, and Jessica Fitzgerald-McKay will take notes.
- Jabber Scribe
- Bluesheets

2) SUIT Architecture (draft-ietf-suit-architecture)

- No discussion; the document is with the RFC Editor.

3) SUIT Information Model (draft-ietf-suit-information-model)

- The document has been through IESG review, which raised a few nits as well as three topics that need discussion
- Why are we only using UUIDs for Device ID matching?
  - Should we better explain why UUID and not say delegated IDs?
  - Slide gives Brendan's answer
  - Dave Thaler: other groups had similar questions about other IDs and allowed a delegation because one might need to look up other data from an ID, for example to find the organization that generated it, but here you have the rest of the manifest with such information in it. So, yes, documenting the rationale would be helpful since probably a frequently asked question.
  - Brendan: Text fields tend to get parsed; it rarely stays at string matching. UUIDs encourage people to do the right thing, just matching the ID. UUID is 16 bytes fixed length. Text is for human readable things, and devices don't need that. The vendor and class ID are for testing applicability, not asserting properties, those are different things.
- Delegation mechanism too vague

    - Brendan: Providing context, delegating from one signatory to the next. It was deliberately left vague in information model, with the details being described in manifest document.
    - Russ: Seems desirable to move some of those details to the information model, but leave the bulk of the discussion in the manifest document.
- Requirements on secure time
    - Brendan: The manifest document does not include a reference time source requirement, only that the clock needs to be monotonicly increasing. Probably makes sense to add. You could have a secure relative clock. However, the manifest uses absolute time. So, probably should add a reference time source.
    - David Waltermire: The time source also needs to be verifiable, such as using a signature.
- Adding examples? Maybe adding examples in different document.
    - Roman: There are rumors that IESG does not want informational documents, but I find examples valuable, and I will support.

4) SUIT Manifest Format (draft-ietf-suit-manifest)

- Very few changes to the draft, mainly editorial, and correcting mismatch of CDDL.
- One feature addition requested by TEEP for ability to delete a component. Can cause a lot of dependancy problems, which could end up with broken system. Also, who has authority to delete trusted components? What happens when the component has already been deleted? What happens if a component is used partway through update, then delete the component, and then the update fails? Maybe unlink or garbage-collect would make more sense than deletion.
    - Brendan: Added garbage collection feature to version 12; want WG feedback.
    - Dave T: Think garbage collection will be fine for TEEP. Need to make it clear that TEEP requirement comes from limited storage capacity situations. Need to do garbage collect before an install in newly freed space. One could perhaps bundle SUIT manifests in a strict ordering. That is, first manifest is for deleting a Trusted Application (TA) in a Trusted Execution Environment (TEE) and, then a second manifest installing another TA in the space freed by the deletion. How do we express that? Maybe bundle two manifests into another manifest, with an ordering requirement?
    - Brendan: Yes, garbage collection of a component should not impact that. May need a special case for the situation where there are no references to a component to start with.
    - Dave T: SUIT or TEEP could implement this approach. TEEP could pass two manifests and use them sequentially. But, prefer a solution in the SUIT manifest.
    - David Brown: Is the reference count ephemeral or persistent?
    - Brendan: It has to be persistent. Only relevant when you have multiple non-interdependant components.
    - David B: Okay, need to be clear on that.
    - Dave T: A TEEP TA is basically a type of shared library, the deletion of a component with a non-zero reference use case in general is any shared library.

- Hannes Tschofenig: Encryption in SUIT. There are two mechanisms: symmetric key (AES 128 Key Wrap) or ECDH Ephemeral-Static + AES KW. When firmware image is stored on external flash, need to decrypt to execute on internal flash. When image is decrypted, it can be put in RAM for execution. With AES 128 KW, symmetric Key Encryption Key (KEK) used to encrypt randomly generated Content Encryption Key (CEK). With ECDH Ephemeral-Static, sender creates ephemeral ECDH key pair, receiver uses static key pair, and ECDH produces shared secret, HKDF produces the KEK from shared secret, creates random CEK, encrypts CEK with KEK.
  AES-128 in COSE-provides worked example in slides.
    - David B: Question regarding use cases. Third one has not been implemented in MCUboot. Microcontrollers doing decrypt in hardware rather than in software, and they are able to execute the encrypted binary directly.
    - Hannes: AES KW need additional data structure, defined in COSE. Hannes suggests external additional data (external_aad) defined as null. Would like clarification on COSE requirements. ECDH is more complicated, but it is better from a security perspective. Inner "box" (on slides) that carries public key and key ID referring to the sender. What curve recommendations should be defined by SUIT? What would we use for PartyUInfo.Identity in the key derivation? Should we include nonces in this structure? What algorithm parameters should be stored in SuppPubInfo?
    - Russ: The nonce makes sure that a unique KEK is produced, even if the ephemeral key gets used more than once. If you are sure the ephemeral key will only be used once, you can skip the nonce.
    - Hannes: What if we are using the static key for the recipient?
    - Russ: That is okay as long as the sender key is ephemeral. The nonce is a "belts and suspenders" approach.
    - David B: Patches in MCUboot use nonces. But, some users feel more comfortable including the nonce.
    - Chris Inacio (in Jabber): Is cost of using the nonce high enough to worry about this?
    - David W: Doing this in manifest will delay manifest publication. And we keep delaying publication to add new features. Can we split this work to allow manifest publication, while continuing to work on encryption?
    - Brendan: That is what I recommend. With examples, we can keep existing ones in manifest document, but put additional ones in new examples document. We can consider informational profiles. Minimum device features, minimum device with encryption, and so on.
    - Russ: Profiles are inevitable, given algorithm choices. The needed features are already in the manifest document.
    - David W: Worth spending time to move this forward. Mandatory-to-implement decisions can do in another document to support algorithm agility.
    - Hannes: Would that include key exchange algorithms?
    - David W: We need to work that out.
    - Hannes: Maybe we can have AES KW in the base manifest document, and then cover ECDH separately. Selecting on elliptic curve scheme is tricky. Recent work in CFRG on hybrid public key encryption schemes that might be useful.

    - Dave T: Propose to push encrypted binaries details into separate document. Put as much of the discussion to a new document, making sure manifest is extendable. Prefer this approach to including AES KW in manifest document.
    - Roman (in jabber): What are the new milestones for manifest, then?
    - Russ: We will need interim meeting to sort this out.
    - David W: We should factor this into a charter update.
    - Brendan: Should we factor out all examples in manifest, or just new ones? Implementers might need some examples.
    - Dave T and Hannes (in chat): Leave examples that are already present in manifest document, just add new ones in additional doc.
    - David W and Russ: We need to take that discussion to the mail list.

5) Secure Reporting of Update Status (draft-moran-suit-report)

- Out of time; move discussion to interim.

6) Strong Assertions of IoT Network Access Requirements (draft-moran-suit-mud)

- Out of time; move discussion to interim.