SUIT WG at Virtual IETF 112

1) Logistics

- Agenda Bashing
- Minute Taker: Hannes Tschofenig, Russ Housley, Dave Thaler
- Jabber Scribe: Michael Richardson
- Bluesheets (automatic in Meetecho)

Agenda bash: Neither draft-ietf-suit-report nor draft-moran-suit-mud will not be discussed. These document have seems little change since IETF 111.

2) Status in WG Re-charter

GOAL: Share status; resolve any issues raised by the IESG

There has been a long delay in the re-chartering process.

Roman Danyliw: Suggested to put a milestone in the proposed charter about the interaction with RATS WG in the style of: "XXX-2022 Decide with RATS WG on where the 'set of claims for attesting to firmware update status' document should be produced".

Russ Housley: Believes that RATS defines the claims.

Dave Thaler: You want a milestone for deciding which WG will handle the document.

Roman: If we decide that it goes to RATS, the we should update the charter text. If it is still undecided right now, thene there should be a milestone for that decision. March 2022?

Dave Waltermire: What actions do we need to take to make a decision?

DaveT: At the previous meeting we talked about having a document for SUIT-specific claims. Does that document belong in the SUIT WG or the RATS WG?

Henk Berkholz: My preference would be RATS.

Russ: I think RATS is the right home, but we want to make sure that SUIT also reviews the document.

Michael Richardson: It would be good to have a 20 minute joint virtual interim meeting of SUIT and RATS to have a longer conversation on this topic among the all people involved.

Russ: Good suggestion. We will coordinate with the RATS WG Chairs.

Brendan Moran: Does RATS want to deal with every claim? Or, does RATS want the groups to deal with claim registrations? Why are we having this discussion? RATS sets up the base document, and then the rest is handled via the IANA registry.

DaveT: There is an Internet-Draft written by Henk in SUIT that handles the SUIT claims. From a process perspective, this would be similar to how the DHC group works. There is indeed a discussion about where this should/could happen.

Henk: There are a small amount of universal claims. Sorting this out is the core issue.

DaveT: Some of the claims in Henk's document are already obsoleted by the most recent update to the EAT Internet-Draft.

DaveW: This might be the discussion of the interim.

DaveT: I hope that the non-SUIT specific aspects will be sorted out long before the virtual interim.

DaveW: Is there any chance that we can resolve the discussion about where the discussion should happen? For example, at the 2nd RATS meeting this week.

DaveT: I don't think this is on the agenda.

Henk: There is a question about timing.

DaveW: Some form of coordination is necessary here. I think Roman's suggestion is good to have a milestone added into the charter.

Roman: I will add this milestone and send it to the IESG for approval.

3) Hackathon Summary

GOAL: Share things that were learned

Hannes Tschofenig: Some attendence. Slides are available
here.
Hacking events happened on multiple fronts.

Lesson learned: it more difficult to do hackathons in the current virtual state given how much that is going on. Hoping to switch to face-to-face or we need to manage the work more closely.

The hackathon tutorial recordings and slides are available
here.

Hannes: Please drop me (or Emmanuel Baccelli) an email if you have questions regarding the software or tools.

4) SUIT Manifest Format

draft-ietf-suit-manifest

GOAL: Discuss open issues; get ready for WG Last Call

Slides 3 and 4: Brendan talks about the document split, which was agreed at the last IETF meeting.

Slide 5: Brendan discusses how integrated payloads are now handled using tstr keys based on decisions from IETF 111.

Slide 6: URIs are handled using URI references now.

Brendan leads a discussion of mandatory-to-implement (MTI) algorithms:

Russ: A lot of agility comes from the COSE constructs.

Brendan: This works really well in the non-constrained environment. In the constrained environment for some of the components that cannot be updated. Here we have to be careful.

Russ: I agree. That is a constraint outside the protocol. I am not sure what we put into the protocol to address this.

DaveT: There are a couple of things regarding the MTI question. MTI for whom? There is the author, consumer, and maybe there is an intermediary. In some cases the MTI requirements refers to both sides but sometimes we can have two algorithms MTI on one side and only one algo on the other side. The question to the group is whether the different roles should have different MTI requirements? Which way do we want to go?

Brendan: I think the author has a list of the MTI algorithms and the recipient has one.

David Brown: Picking something as MTI will lead to lots of implementations and deployments that are not compliant. In Mcuboot, the algorithms are a compile-time requirement.

DaveW: Summarizing the discussion so far... We want to set the target for interoperability. We seem to be heading towards non-interoperable, or non-compliant implementations, or both.

Michael: We should make HSS/LMS the MTI.

Akia Tsukamoto: The MTI algorithms for SUIT will automatically be MTI for TEEP. I would prefer SUIT/TEEP/EAT not to specify contradicatory algorithms.

Brendan: We had a discussion about capability reporting. Does the MTI discussion become irrelevant if we specify a capability reporting?

DaveT: When specifying a system for your binary, then you need to consider the algorithms supported by the target for that binary.

Brendan: Do we have to tie the signature to the device or do we have to create pairs of authors/consumers?

DaveT: It depends whether the intermediaries perform some actions on the manifest?

DavidB: The device being updated, may not be network connected. An intermediary may need to take the manifest and perform actions and then relay it. I am not sure I see the value of MTI.

DaveW: Summarizing the discussion so far... I think there are multiple parties that are working together. The signature algorithms will effectively need to be sorted out by the involved party and that's why we do not need an MTI.

DaveT: If you have middle entities, then you need to specify a MTI. I propose: "end points implement either ECDSA or HSS/LMS and intermediares need to implement both."

Michael: You captured what I was agreeing with. The author knows what is available to the device. The operator has to pick something the device supports. I would say ECDSA is a SHOULD.

DaveW: Based on the last poll we had a single algorithm for MTI: HSS/LMS.

Russ: This makes sense to me.

Russ: We need to confirm it on the list. HSS/LMS mandatory, and ECDSA is a SHOULD.

5) Firmware Encryption with SUIT Manifests

draft-ietf-suit-firmware-encryption

GOAL: Recently adopted; discuss open issues.

The earlier document was split into two documents. The first one defines a COSE HPKE mechanism, which will be handled by the COSE WG. This document was revised to use that COSE HPKE mechanism.

6) SUIT Trust Domains

draft-moran-suit-trust-domains-00

draft-moran-suit-update-management-00

Running very short on time. Brendan decided to talk about the SUIT Trust Domains document (instead of the SUIT Update Management document) because it has relevance for TEEP. The content of this document was extracted from the SUIT manifest.

DaveT: Asking whether there is option to adopt the documents since the content was extracted from the previous WG document.

Akira: Running code for the dependency concept will be coming.

Russ asked Brendan to post the two documents as WG items.

--- out of time --

7) Secure Reporting of Update Status

draft-ietf-suit-report

GOAL: Recently adopted; discuss open issues

Postponed

8) Strong Assertions of IoT Network Access Requirements

draft-moran-suit-mud

GOAL: Discuss open issues; get ready for WG call for adoption (to be done in parallel with the IESG recharter)

Postponed

9) Any Other Business (if time permits)

None