SUIT WG at IETF 113

1) Logistics

- Agenda Bashing
- Minute Taker: Mike Jenkins, Russ Housley, Dave Thaler

2) Hackathon Summary

Hannes Tschofenig has been working on the firmware encryption, which is on the agenda later. Fewer people at hackathon, about 100 or so.

3) SUIT Manifest Format

Presentation: Brendan Moran
slides
draft-ietf-suit-manifest

Desire to introduce mandatory-to-implement (MTI) PQC algorithms into documents. Firmware authors should be responsible for determining which algoritms. Comparison of HSS-LMS (known secure, already a standard) to ECDSA indicates that there are likely to be problems for boot loaders. Falcon-512 has better performance, but is not a standard, and it may not become a standard. Crypto algorithm agility is desirable and doable for updatable clients, but not stage-0 boot loaders.

- David Brown: "mandatory" is less relevant than "what fits, what works" with hardware. Implementations will use configuration options to select away from MTI due to hardware limitations. Is it for both verifying and signing?
- Emmanuel Baccelli: clarified the result of the report that Brendan Moran was quoting specs from. Essentially, there is work on reducing code size, but nothing to report yet. Sizes reported were both signing and verification side. Russ pointed out that verify-only should be significantly smaller, so we really need that number to evaluate applicability to bootloaders.
- Hannes Tschofenig: wondered if it is possible to defer crypto choice into a profile document to avoid blocking the manifest spec? This would allow the selection of PQC algorithms by NIST to be taken into account.

A discussion regarding the feasibility of using large PQC signatures due to the comparison to large firmware payloads. Sometimes the firmware update is large, but other time is is a small patch. Do not want the PQC signature to be bigger that the whole firmware payload. Also, the recipient only needs the code to validate a signature, and the sizes reported on the slides include the key generation and signing code as well.

David Waltermire: Potential way forward is to create a document that discusses only algorithms, with indications of which are being moved to and which away.

- Hannes: may be too early to pick a PQC MTI. We can make ECDSA as MTI, and then in the future move to PQC once we have more data.

- Brendan: suggests that MTI should be defined for everything except the boot loader. The boot loader is too difficult to have a one-size-fits-all, long lived MTI algorithm.

4) SUIT Trust domains

Presentation: Brendan Moran
slides
draft-ietf-suit-trust-domains

Need to move quickly on this draft because of TEEP dependencies; however, Brendan is unaware of running code. Please report if you have done implementation. Request for review of document, especially the use of CWT.

- Brendan: will make sure there are examples in the next version of the draft.

5) SUIT Update Management

Presentation: Brendan Moran
slides
draft-ietf-suit-update-management

Currently specifies CoSWID, but CoRIM is probably better. The CoRIM document has not even been accepted by the RATS WG yet, so we should not wait for it. Request for review of document, and make sure that your use case is covered.

6) Firmware Encryption with SUIT Manifests

Presentation: Hannes Tschofenig
slides
draft-ietf-suit-firmware-encryption

HPKE is published (RFC 9180). This Internet-Draft depends on the COSE HPKE document (draft-ietf-cose-hpke). Will keep this document in sync with the COSE HPKE document as it goes through ths COSE WG. An open source reference implementations exists (see slide). This document includes examples that are relevant to SUIT Manifest.

The COSE additional information structures ensure that the sender and the recipient have the same context for the keying material, including the optional identification of the parties. In the SUIT context, the digital signature provides the authentication of the sender, but this may be a concern in other uses of the COSE HPKE document.

7) Secure Reporting of Update Status

Presentation: Brendan Moran
slides
draft-ietf-suit-report

Suit-parameters and component identifiers were added as property claims, which enables attestation of properties.

8) SUIT-related Claims

Presentation: Brendan Moran
slides
draft-birkholz-rats-suit-claims

SUIT reporting (that contain SUIT-related claims) is built on the fly to reduce burden on constrained devices. EAT draft-ietf-rats-eat has similar data but different structure. The SUIT report is evidence but not a claim; SUIT report could be converted to EAT claim for attestation.

- Brendan: Proposed solution is for the SUIT report to become a single EAT claim. This is consistent with using it as evidence, and this moves the translation burden from the constrained device to the (probably not constrained) verifier.
- Dave Thaler: There are four possible ways to use SUIT reports:
    1. (AS): Use SUIT report AS an evidence format instead of eat
    2. (IN): Use SUIT report encapsulated IN an eat (what is on Brendan's slide)
    3. (TO): Use SUIT report to translate claims TO an eat (e.g., what Brendan mentioned might do to translate info to attestation result fields)
    4. (WITH): Use SUIT report separate from (i.e., WITH) attestation, e.g., send in a message to a relying party where the message has both evidence and the suit report in separate parts of the message
- Dave Thaler: Today in TEEP there is no requirement that a TEEP Agent must generate SUIT reports at boot time, only at Update time. Should there be? Requiring #1 or #2 would introduce such a requirement.
- Dave Thaler: Should we add SUIT reports to the QueryResponse message in TEEP to allow #4?
- Chairs: We are out of time. Please continue this discussion on the mailing list.

--- out of time ---

9) Strong Assertions of IoT Network Access Requirements

slides
draft-ietf-suit-mud

GOAL: Recently adopted; discuss open issues

Postponed

10) Any Other Business (if time permits)

None