Software Updates for Internet of Things (SUIT) WG

IETF 111

Friday, 2021-07-31 at 19:00 UTC

Chairs:

Dave Thaler

David Waltermire

Russ Housley

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

• By participating in the IETF, you agree to follow IETF processes and policies.

• If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.

• As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.

• Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

• As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:
•BCP 9 (Internet Standards Process)
•BCP 25 (Working Group processes)
•BCP 25 (Anti-Harassment Procedures)
•BCP 54 (Code of Conduct)
•BCP 78 (Copyright)
•BCP 79 (Patents, Participation)
•https://www.ietf.org/privacy-policy/ (Privacy Policy)

Administrative Tasks

Bluesheets will happen automatically by joining MeetEcho

We need volunteers:

- Two note takers
- One jabber room watcher

Jabber: xmpp:suit@jabber.ietf.org?join

MeetEcho: https://www.meetecho.com/ietf111/suit

Etherpad: https://codimd.ietf.org/notes-ietf-111-suit#

Agenda (1 of 2)

1) Logistics

2) Hackathon

- Share things that were learned

3) SUIT Manifest Format

- draft-ietf-suit-manifest
- Discuss open issues; get ready for WG Last Call

4) Firmware Encryption with SUIT Manifests

- draft-ietf-suit-firmware-encryption
- Recently adopted; discuss open issues

Agenda (2 of 2)

5) Secure Reporting of Update Status

- draft-ietf-suit-report
- Recently adopted; discuss open issues

6) Strong Assertions of IoT Network Access Requirements

- draft-moran-suit-mud
- Discuss open issues; get ready for WG call for adoption (to be done in parallel with the IESG recharter)

7) Any Other Business (if time permits)

Milestones Status

Date	Milestone
Mar 2020	**Submit an initial manifest serialization format to the IESG for publication as a Proposed Standard.**
Done	Submit architecture to the IESG for publication as Informational.
Done	Submit manifest information model to the IESG for publication as Informational.
Done	Calendar item: Second interoperability event at IETF 102.
Done	Adopt initial manifest serialization format(s) as WG item(s).
Done	Calendar item: First interoperability event at IETF 101.
Done	Adopt a manifest information model as a WG item.
Done	Adopt "Architecture" document as WG item.

Draft Text for Recharter (1 of 7)

Review of the draft text for recharter is underway on the mail list...
Comments are also welcome now.

Vulnerabilities in Internet of Things (IoT) devices have raised the need for a secure firmware update mechanism that is also suitable for constrained devices. Security experts, researchers, and regulators recommend that all IoT devices be equipped with such a mechanism. While there are many proprietary firmware update mechanisms in use today, there is no modern interoperable approach allowing secure updates to firmware in IoT devices. In June 2016, the Internet Architecture Board organized a workshop on 'Internet of Things (IoT) Software Update (IOTSU)', and RFC 8240 documents various requirements and challenges that are specific to IoT devices.

Draft Text for Recharter (2 of 7)

A firmware update solution consists of several components, including:

* A mechanism to transport firmware images to compatible devices.
* A manifest that provides meta-data about the firmware image (such as a firmware package identifier, the hardware the package needs to run, and dependencies on other firmware packages), as well as cryptographic information for protecting the firmware image in an end-to-end fashion.
* The firmware image itself.

Draft Text for Recharter (3 of 7)

The SUIT WG is defining a firmware update solution (taking into account past learnings from RFC 4108 and other proprietary firmware update solutions) that are usable on Class 1 (as defined in RFC 7228) devices, i.e., devices with ~10 KiB RAM and ~100 KiB flash. The solution may apply to more capable devices as well. The SUIT WG is not defining any new transport or discovery mechanisms, but may describe how to use existing mechanisms within the architecture.

The SUIT WG has already completed work on two documents:

* An IoT firmware update architecture that includes a description of the involved entities, security threats, and assumptions.
* An information model for the SUIT manifest.

Draft Text for Recharter (4 of 7)

Now that the information model is complete, the SUIT WG has selected the CBOR serialization format and the associated COSE cryptographic mechanisms to encode the SUIT manifest. The SUIT WG may consider a small number of additional formats in the future; however, to reduce the complexity of a firmware management solution, a very small number of formats is preferred to enable SUIT maifest integration and interoperability with other IoT technologies and ecosystems. To support a wide range of deployment scenarios, the formats are expected to be expressive enough to allow the use of different firmware sources and permission models.

Draft Text for Recharter (5 of 7)

The SUIT WG does not aim to create a standard for a generic application software update mechanism, but instead the SUIT WG is focusing on firmware development practices in the embedded industry. Software update solutions that target updating software other than the firmware binaries (e.g., applications) are also out of scope.

To support the SUIT manifest format, the SUIT WG is also defining formats and protocols that enable a SUIT Status Tracker to determine if a particular manifest could be successfully deployed to a device and determine if an operation was successful.

Draft Text for Recharter (6 of 7)

In addition, the SUIT WG will specify claims related to the SUIT Status Tracker that can be used to provide evidence in support of the architecture defined by the RATS WG.

The SUIT WG will continue to work with silicon vendors and OEMs that develop IoT operating systems to produce implementations based on SUIT WG specifications. In particular, the SUIT WG plans to continue to Participate in IETF Hackathons.

Draft Text for Recharter (7 of 7)

The SUIT WG document deliverables are:

* A SUIT manifest format specification using CBOR.
* A firmware encryption specification for use with SUIT manifests.
* A secure method for an IoT device to report on firmware update status.
* A set of claims for attesting to firmware update status.
* A SUIT manifest extension to include a MUD file as defined in RFC 8520.