arm Research

Secure Firmware Updates for IoT devices using IETF SUIT

Brendan Moran

2019-11-26

All Software Contains Bugs

Some bugs

- Have substantial customer impact
- Introduce security vulnerabilities

Vulnerabilities in air-gapped/ non-IoT networks

- Physical security adds defence in depth
- Limited impact of vulnerabilities

Vulnerabilities in IoT networks

- Broad exposure
- High impact
- Require a response

Response to bugs in IoT devices

1. Ignore and hope for the best?

2. Onsite service?

3. Recall/ Refurbish?

4. Decommission/ Replace?

Each of these options is expensive in reputation, money, or both.

5. Fixing Bugs Remotely

IoT devices have network connectivity

- Use that to patch devices

Many jurisdictions are considering requiring patching capability

- NCSC's IoT code of practice, item 3) Keep software updated

Patching is the single most important security repair tool

- Remote patching makes it viable to fix bugs in IoT devices

Remote patching is simple

Remote firmware update risks

Reliability

- Power interruption
- Network interruption
- Firmware mismatch
- Network mismatch
- Stability
- Processing errors

Security

- Explicitly allowing remote code execution
- Otherwise unauthorized updates
- Rollback
- IP disclosure

Other sectors do this

Auto updates on PCs is the norm

Auto updates on handsets is the norm

Everything we do in security is based on this:

- Vulnerability disclosure
- Developing patches

Auto updates in IoT ~~is the norm~~

The IoT faces different challenges

Auto updates on PCs

Are done by each application

- Some use platform services, but this is recent

Auto updates on handsets

Are handled by:

- The handset vendor for OS updates
- The platform vendor for app updates

Why is automatic updating not the norm?

Commercial complexity

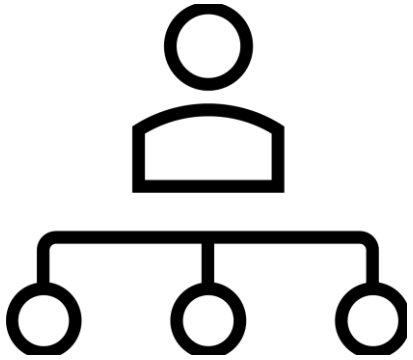
- Insufficient incentives
  - Economic
  - Reputation
  - Legal/regulatory
- High risk
- User intervention unavailable

Technical complexity

- Heterogeneous devices
- Devices constrained in
  - Bandwidth
  - Energy
  - Storage
  - Processing power
- No platform to provide update machinery

Surely this is a solved problem?

Existing deployments of constrained, networked devices



Fleet Management Systems

Networked Sensors

IoT Platforms

Firmware Update Solutions

Existing Firmware Update Solutions

- Signed Binary
  - Just the firmware and a signature
- Binary with secure boot metadata
  - The firmware, boot metadata and signature
- PKCS#7 for Firmware (RFC4108)
  - Rich metadata in PKCS#7 container
- The Update Framework
  - Extensive metadata, many signatures
  - Uptane

Adoption of existing standards

- Little adoption information available
- Major IoT platforms offer firmware updates
  - Each platform appears to use a different update mechanism and format
  - Many IoT platforms appear to directly use binaries with secure boot metadata

Status Quo: A fractured market

Current approaches to firmware updates:

"No one else should deploy firmware to our devices so we don't need a standard"

"The server creates the metadata that each device needs, so every device can have an update tailored to it"

"Use single-vendor installations if you want updates"

"OTA Update is too hard, so we require manual intervention"

"We need something no standard provides"

Is the Status Quo a problem?

Probably, but it depends on the business model

It might not matter for you only if

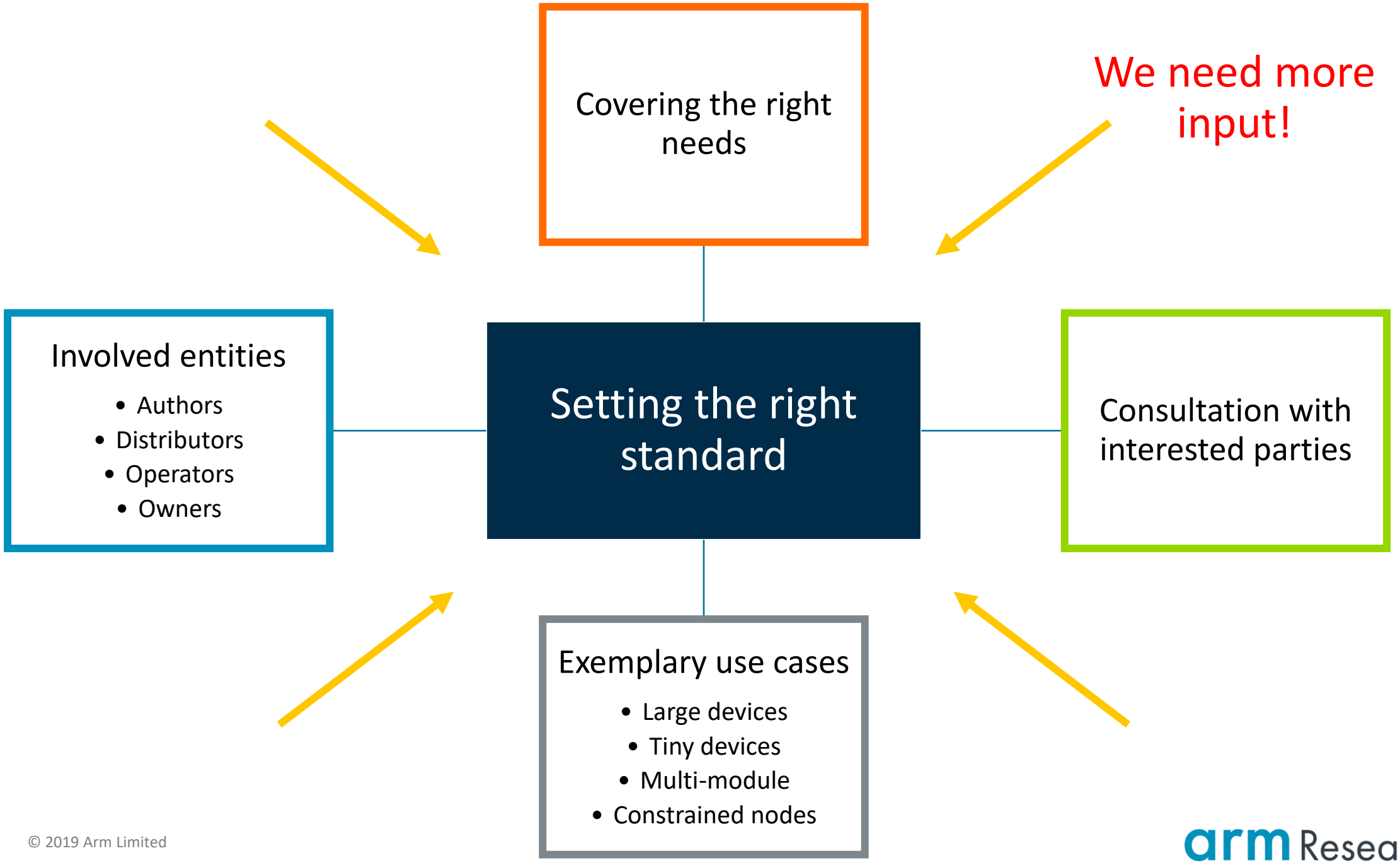
- Your products do not interoperate with other vendors' products **and**
- You have a direct relationship with the end user **and**
- You have the expertise to deploy and secure an update solution either
  - In-house
  - From a platform vendor

It **is** a problem for you if

- Your products interoperate with other vendors' products **or**
- There are intermediaries between you and the end user **or**
- You do not have the expertise to deploy and secure an update solution

Changing the Status Quo

- The Internet Engineering Task Force (IETF) has chartered a working group:
  - Software Update for the Internet of Things (SUIT)
- SUIT's charter includes:
  - Providing a standard for updating constrained IoT devices
  - Describing the overall structure & requirements of firmware update systems, including
    - Involved entities
    - Security threats
    - Assumptions
  - Specifying one or more manifest formats
- SUIT is backed by interested parties including Arm and Arm's partners
- Lower risks, greater incentives for updates



arm Research

What will SUIT provide?

- The standard will define common threat & security models
  - Helps developers to consider security challenges in IoT update
  - Arm's Platform Security Architecture (PSA)
    - Defines similar and compatible threat & security models
    - Recommends SUIT for firmware updates
    - Shares common approach to security of firmware update for IoT
    - See https://www.psacertified.org/ for more details

- The standard will define a common metadata format
  - Lower risk
  - Reference implementations for testing and validation
  - Faster time to market through libraries
  - Better security through increased scrutiny
  - Consistent tools for intermediaries
  - More interoperability between devices and management systems
  - Easier coordination of updates to interoperating systems

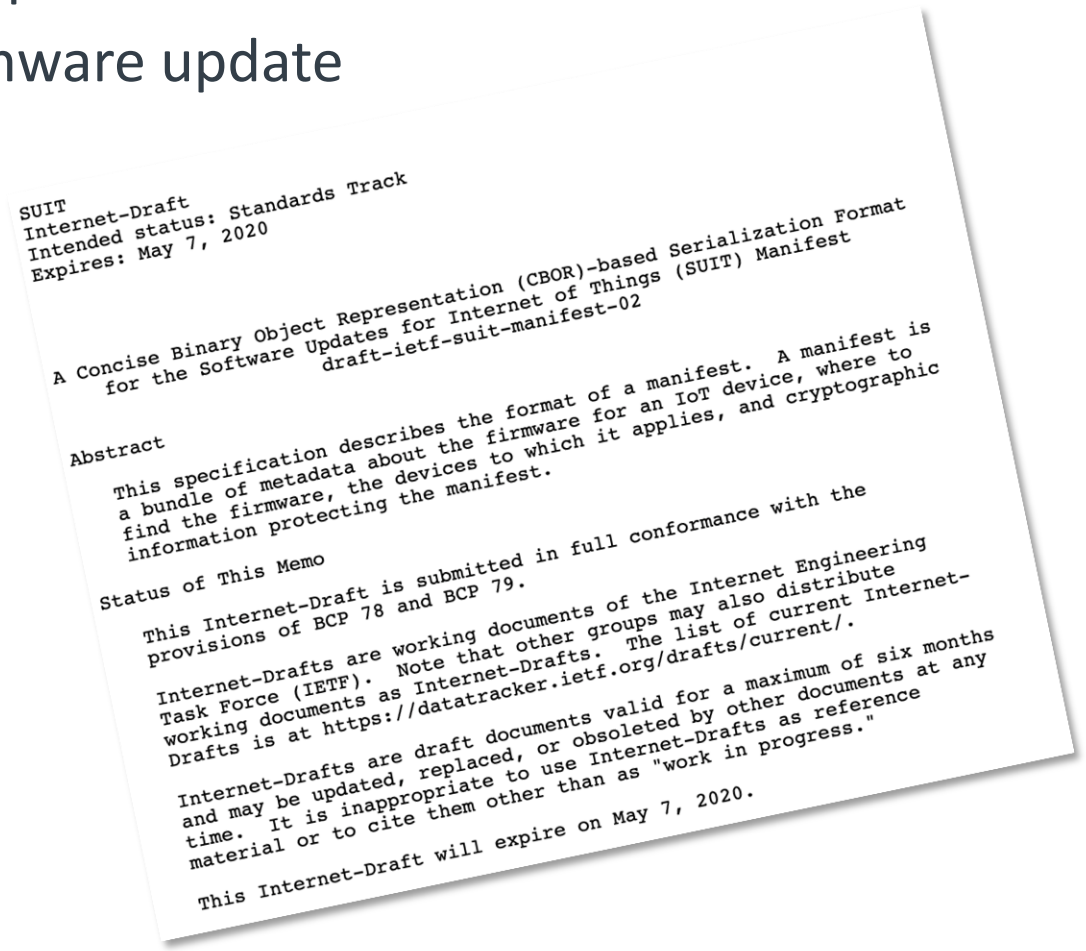
The SUIT manifest

- Software Update metadata
- Encoded in CBOR
- Secured using COSE
- Broadcast and multicast friendly
- Targets very small devices, also good for very large devices
- Unique approach
  - Enables many use cases by encoding a compact, simple, extensible update language
  - Text metadata are authenticated, but removable

IETF SUIT Today

Current documents

- Architecture definition – Approaching completion
  - High level definitions, requirements for IoT firmware update
- Information Model – Approaching completion
  - Threats, User stories, Requirements
- Manifest – Stable, completion expected in 2020
  - Serialization of Information Model
  - Designed for low complexity parsing



SUIT
Internet-Draft
Intended status: Standards Track
Expires: May 7, 2020

A Concise Binary Object Representation (CBOR)-based Serialization Format
for the Software Updates for Internet of Things (SUIT) Manifest
draft-ietf-suit-manifest-02

Abstract

This specification describes the format of a manifest. A manifest is a bundle of metadata about the firmware for an IoT device, where to find the firmware, the devices to which it applies, and cryptographic information protecting the manifest.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 7, 2020.

arm Research

Get Involved!

- Do you have a use-case in mind?
  - Let us know!
- Are you building IoT devices or services?
  - SUIT needs your input!
- Do you want to collaborate?
  - Review the drafts
  - Join the mailing list
  - Join us at our hackathon in February
  - Attend the next IETF meeting in March
  - https://datatracker.ietf.org/group/suit/about/

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
תודה