HR Review: Firmware Updates for IoT Devices

An assessment of human rights considerations in:

draft-ietf-suit-architecture-01

draft-moran-suit-manifest-02

draft-ietf-suit-information-model-01

Gurshabad Grover

gurshabad@cis-india.org

Sandeep Kumar

sandeepkjha18@gmail.com

Some Terms (caveat: simplified)

Firmware Image: binary that is the firmware of a device

Manifest: meta-data of firmware image

Author: Entity creating the firmware image and manifest

Device operator: responsible for administering the device

Overview of SUIT Drafts

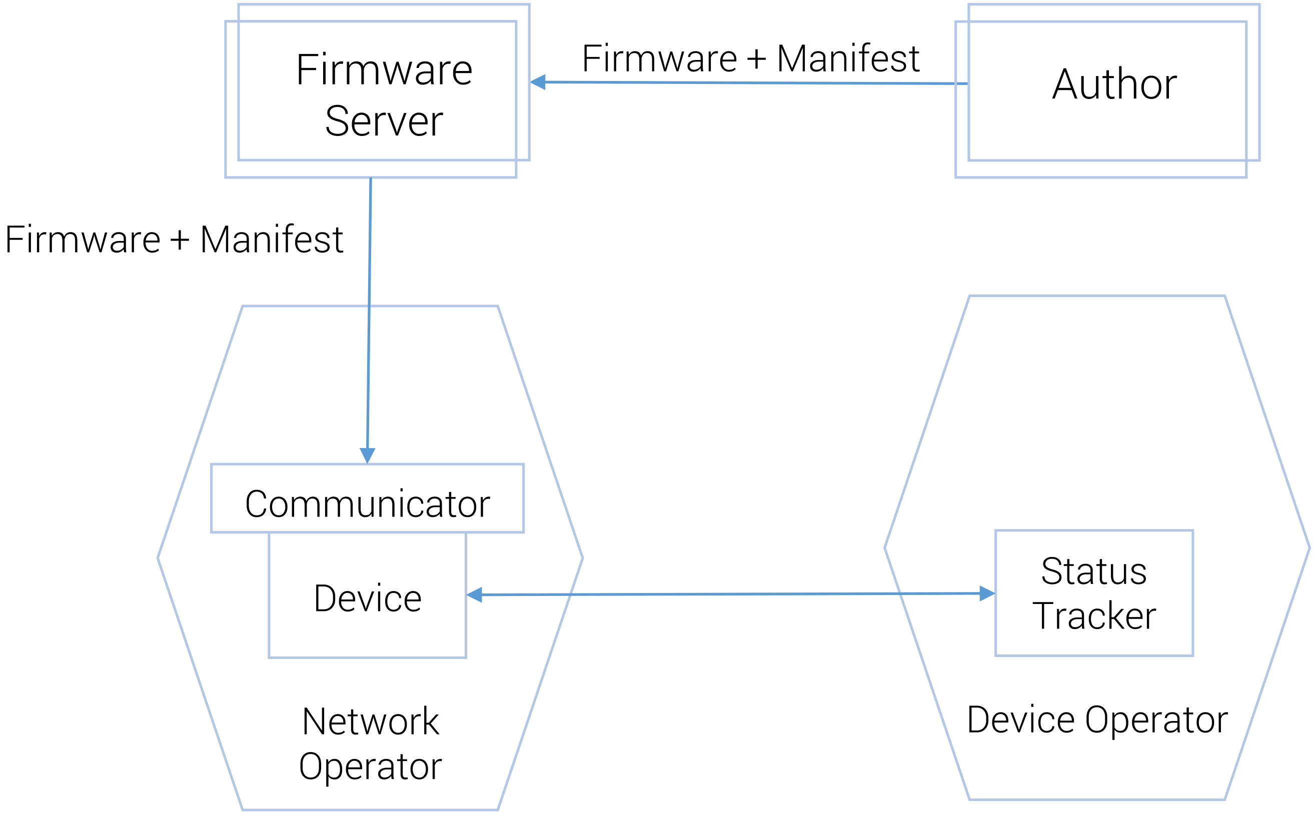
draft-ietf-suit-architecture-01

‘A Firmware Update Architecture for Internet of Things Devices’

- Architecture for firmware update mechanism
- Various requirements for the architecture

[SUIT-ARCH]

[SUIT-ARCH]



Re-drawing of Figure 1 in [SUIT-ARCH]

draft-ietf-suit-information-model-01

‘Firmware Updates for Internet of Things Devices - An Information Model for Manifests’

- Use cases and security threats
- Usability and security requirements of the architecture
- Information fields in the manifest

[SUIT-IM]

draft-moran-suit-manifest-02

‘A CBOR-based Manifest Serialisation Format’

- Describes the serialisation format of the manifest

[SUIT-MF]

Human Rights Considerations

Human Rights Considerations (RFC 8280)

RFC 8280, 19 categories of considerations:

- Connectivity
- Privacy
- Content Agnosticism
- Security
- Internationalisation
- Censorship Resistance
- Open Standards
- Heterogeneity Support
- Anonymity
- Pseudonymity
- Accessibility
- Localization
- Decentralization
- Reliability
- Confidentiality
- Integrity
- Authenticity
- Adaptability
- Outcome Transparency

Human Rights Considerations (RFC 8280)

Out of scope

- Connectivity (S 6.2.1)
- Content Agnosticism (S 6.2.3)
- Censorship Resistance (S 6.2.6)
- Anonymity (S 6.2.9)
- Pseudonymity (S 6.2.10)
- Accessibility (S 6.2.11)
- Decentralization (S 6.2.13)

Human Rights Considerations (RFC 8280)

We found no concerns related to:

- Heterogeneity Support (S 6.2.8)
- Integrity (S 6.2.16)
- Authenticity (S 6.2.17)
- Adaptability (S 6.2.18)

Human Rights Considerations (RFC 8280)

We found concerns related to:

- Privacy (S 6.2.2) & Security (S 6.2.4) & Confidentiality (S 6.2.15)
- Internationalisation (S 6.2.5) & Localisation (S 6.2.12)
- Open Standards (S 6.2.7)
- Reliability (S 6.2.14)
- Outcome Transparency (S 6.2.19)

Concerns & Recommendations

Privacy & Security: Encryption of firmware

Context

- Vendor ID and Class ID (device information) as strings in the firmware
- Drafts ambiguous about requirement level

Privacy & Security: Encryption of firmware

Context

- Vendor ID and Class ID (device information) as strings in the firmware
- Drafts ambiguous about requirement level

Concern

- Loss of privacy for operator
- Attackers can mount targeted attacks

Privacy & Security: Encryption of firmware

Context

- Vendor ID and Class ID (device information) as strings in the firmware
- Drafts ambiguous about requirement level

Concern

- Loss of privacy for operator
- Attackers can mount targeted attacks

Recommendation

- RECOMMEND encryption of firmware image

Privacy & Security: Encryption of manifest

Context

- Vendor ID and Class ID (device information) in cleartext in the manifest
- Drafts currently don’t talk about encryption of manifest

Privacy & Security: Encryption of manifest

Context

- Vendor ID and Class ID (device information) in cleartext in the manifest
- Drafts currently don’t talk about encryption of manifest

Concern

- Loss of privacy for operator
- Attackers can mount targeted attacks

Privacy & Security: Encryption of manifest

Context

- Vendor ID and Class ID (device information) in cleartext in the manifest
- Drafts currently don’t talk about encryption of manifest

Concern

- Loss of privacy for operator
- Attackers can mount targeted attacks

Recommendation

- RECOMMEND encryption of manifest

Internationalisation & Localisation

Context

- “Does your protocol have text strings that have to be understood or entered by humans?” [RFC8280]
- Manifest will have “severable text” meant for humans [MF-MAIL]

Concern

- No mention of internationalization

Recommendation

- CBOR supports UTF-8; make i18n ability explicit

Open Standards

Context

- “Is your protocol fully documented in such a way that it could be easily implemented, improved, built upon, and/or further developed?” [RFC8280]

Concern

- Use of ‘extensions’ field in the manifest not defined

Reliability: Announce Degradation

Context

- “Do you have a documented way to announce degradation?” [RFC8280]

Reliability: Announce Degradation

Context

- “Do you have a documented way to announce degradation?” [RFC8280]

Concern

- No mechanism about announcing failure to operator

Reliability: Announce Degradation

Context

- “Do you have a documented way to announce degradation?” [RFC8280]

Concern

- No mechanism about announcing failure to operator

Recommendation

- Maybe the status tracker could server the function?

Reliability: Recovery Mechanism

Context

- “Do you have measures in place for recovery or partial healing from failure?” [RFC8280]
- Recovery mechanism is optional [SUIT-ARCH]

Reliability: Recovery Mechanism

Context

- “Do you have measures in place for recovery or partial healing from failure?” [RFC8280]
- Recovery mechanism is optional [SUIT-ARCH]

Concern

- For resource-constrained devices, recovery mechanisms are essential (especially because outcome of the process is not always apparent)

Reliability: Recovery Mechanism

Context

- “Do you have measures in place for recovery or partial healing from failure?” [RFC8280]
- Recovery mechanism is optional [SUIT-ARCH]

Concern

- For resource-constrained devices, recovery mechanisms are essential (especially because outcome of the process is not always apparent)

Recommendation

- Recommend/mandate recovery mechanism

Outcome Transparency: Update Result?

Context

- Whether an update has been successful/unsuccessful should be conveyed to the device operator

Concern

- No mechanism mentioned

Recommendation

- Elaborate on status tracker (if it can serve this function)

Additional suggestion: Operator control

Context

- Operator’s authorization is not necessary to initiate the update (left as a policy decision)

Concern

- Device operators’ control over device functioning is diminished

Recommendation

- Recommend operator authority to accept/reject updates

Learnings and Updates

Overview of recommendations

Encryption of firmware image	Discussed, will probably be incorporated
Encryption of manifest	Discussed, could be incorporated
Internationalisation & Localisation	Not discussed yet
Announce degradation	Not discussed yet
Recovery Mechanism	Not discussed yet
Update result?	Not discussed yet
Operator Control	Suggestion retracted after discussion

References and Acknowledgements

[RFC8280] ten Oever, N., Cath, C., “Research into Human Rights Protocol Considerations”, RFC 8280, October 2017, <https://www.rfc-editor.org/info/rfc8280>

[SUIT-ARCH] Moran, B., Meriac, M., Tschofenig, H., “A Firmware Update Architecture for Internet of Things Devices”, draft-ietf-suit-architecture-01, July 2018, <https://datatracker.ietf.org/doc/draft-ietf-suit-architecture/>

[SUIT-MF] Moran, B., Meriac, M., Tschofenig, H., “A CBOR-based Manifest Serialisation Format”, draft-moran-suit-manifest-02, July 2018, <https://datatracker.ietf.org/doc/draft-moran-suit-manifest/>

[SUIT-IM] Moran, B., Tschofenig, H., Birkholz, H., Jimenez, J., “Firmware Updates for Internet of Things Devices - An Information Model for Manifests”, draft-ietf-suit-information-model-01, July 2018, <https://datatracker.ietf.org/doc/draft-ietf-suit-information-model/>

[MF-MAIL] Moran, B., “[Suit] [suit]: draft-moran-suit-manifest-02”, IETF Mail Archive, July 2018, https://mailarchive.ietf.org/arch/msg/suit/rc1gkzf2jhICwcXHSq5JggdGiHo

Thanks to Amelia Andersdotter, Mallory Knodel, Niels ten Over, and Sunil Abraham for their inputs.

Thank you.

Gursabad Grover

gurshabad@cis-india.org