A Secure and Automatic Firmware Update Architecture for IoT Devices

draft-zhu-suit-automatic-fu-arch-00

Julian ZHU, Huawei
March 2018

Background

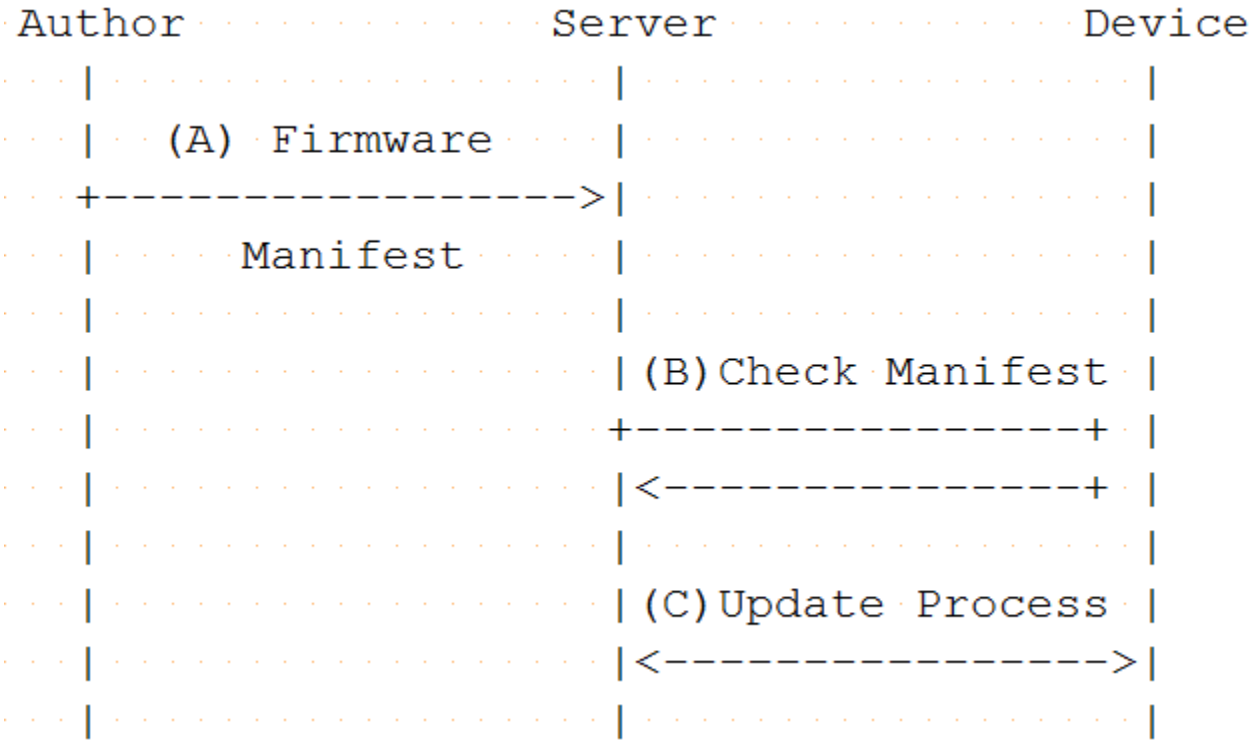
- The SUIT WG is focus on defining a secure and interoperable firmware update solution for IoT devices.
- Security is the key feature of this solution, existing drafts focus more on the Cryptography and Integrity aspects.
- This draft is more on the Availability aspect.

Issues

- 2016 Dyn Cyberattack. The root reason is the devices are not updated in time so that hacked with default username/password by brute-force attack.
- Existing FU mechanisms(e.g. OMA DM\LwM2m) are more on the device side, using “Idle” status as trigger. But any IoT devices do not have “Idle” status. E.g. smart meters, ECUs.

Architecture

- Using automatic update to protect availability:
  - Update in time with least human intervention.
  - Different devices have different update urgency levels.
  - Different firmware images have different update urgency levels.



3 Modes

1. Client-Initiated Update
   - The client itself pulls the latest firmware info from server periodically.
   - For more capable devices.
2. Server-Initiated Update
   - The server pushes the latest firmware info to device once the server gets the image from author.
   - For constrained devices.
3. Negotiated Update
   - Server notifies the firmware image info and client decides the update timing.
   - Mature in the Mobile and Desktop environment.

Thank you !

Comments / Questions ?