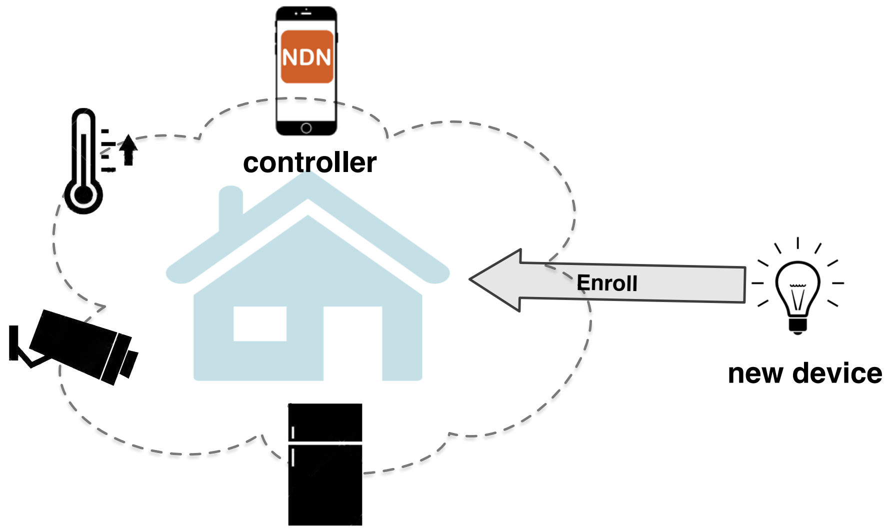
IoT Bootstrapping

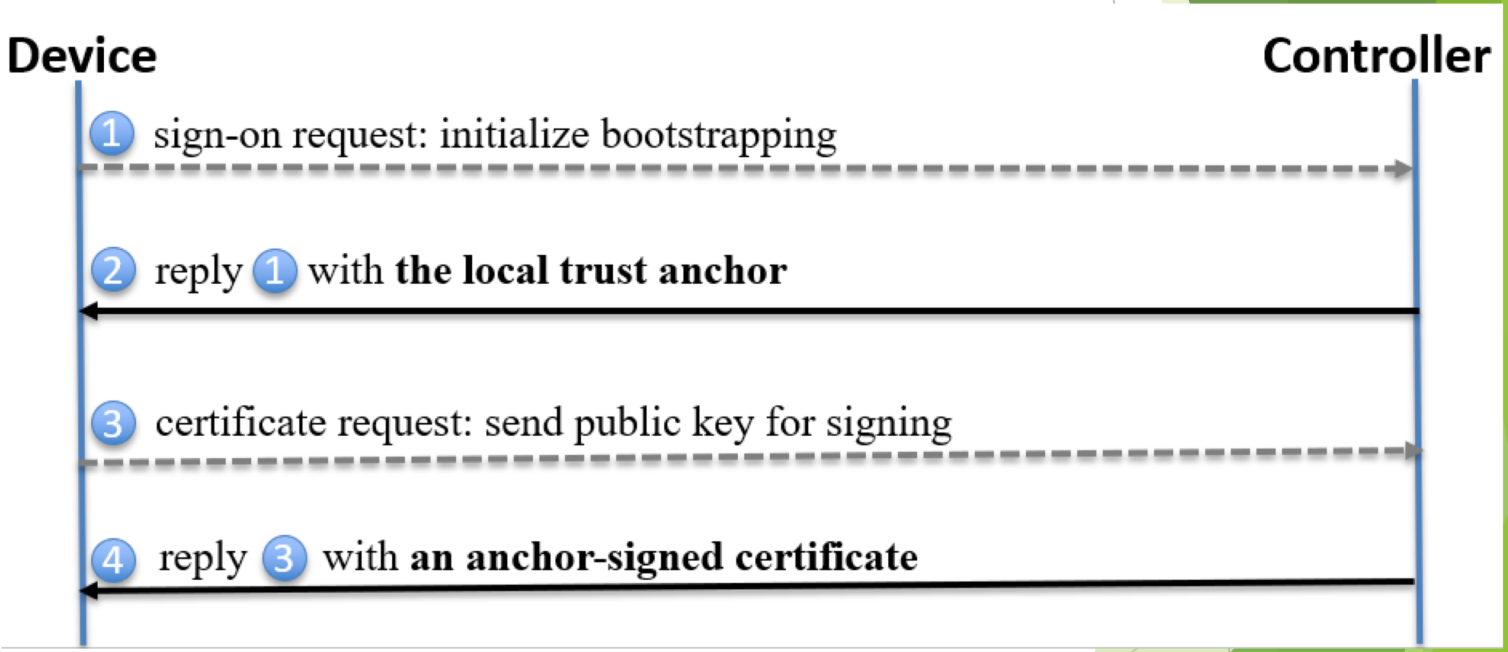
1) NEED

- Allow IoT devices to be trusted by a home network, for home IoT setups



Approach

- Assume that there is physical connectivity between controller and device (wifi, Bluetooth)
- Controller gets device's bootstrapping key (public key) by QR code scanning
- After that, exchange two interests and two data to set up trust between the controller and the device

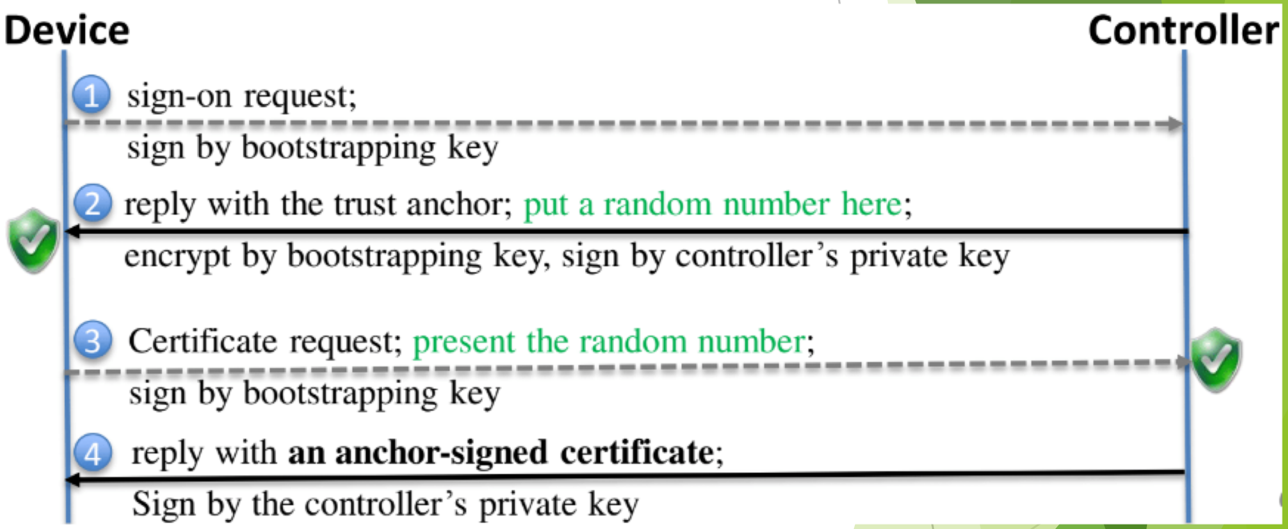


Threat Model

- Fake controller: the attacker obtained the bootstrapping info pretends to be the controller to cheat the device
- Fake device: the attacker obtained the bootstrapping info pretends to be the device to cheat the controller. Once the fake device obtains a anchor-signed certificate, it can further cheat other devices in the system
- Man in the middle attack: the attacker intercepts the message, alters it and then send to the intended receiver
- Replay attack: the attacker sniffs and stores exchanges between device and controller, then replays to both/either side later

Threat Countermeasures

- Sign Interests 1 and 3 by the bootstrapping key; then the controller can authenticate the device and thus perceive any fake device
- Put a random number in Data 2, then the presence of this number in Interest 3 enables the controller to detect and stop replay of Interest 3.
- In Data 2, encrypt its content by the bootstrapping key. decryption of the first random number indicates that the controller knows the bootstrapping key; we design to let the device trust the first controller who talks to it and knows the bootstrapping key.
- Sign the Data 2 and 3 by the controller's private key to enable the device authenticate the controller and perceive any alteration.



Benefit

- Allow consumers to easily bootstrap security for their home IoT devices; just scan QR code of the device with the controller
- Allow bootstrapping to be done without connection to the cloud, a remote server

Achieved

- Have Android app that acts as controller; scans a device’s QR code to bootstrap it; then exchange interests and data to get secure communication
- Have Raspberry Pi and laptop acting as IoT devices; can scan the Raspberry Pi’s QR code and do the bootstrapping, then send a signed interest to it to turn a light on

Link

- https://github.com/6th-ndn-hackathon/iot-bootstrapping

Demo

- Live demo