Survey of Security Bootstrapping

draft-he-6lo-analysis-iot-sbootstrapping

Ana(Danping) He ana.hedanping@huawei.com

Behcet Sarikaya Sarikaya@ieee.org

What is Proposed So Far?

- **[I-D.pritikin-anima-bootstrapping-keyinfra]** EAP-EST, EAP-TLS, 802.1X, EAP-IKEv2 for 802.1 AR certificate
- **[I-D.kwatsen-netconf-zerotouch]** Same authentication methods can be used for X.509 certificate
- **[I-D.struik-6tisch-security-considerations]** Undefined joining protocol for certificate
- **ZigBee IP stack based Smart Energy** EAP-TLS, PANA for certificate
- **[I-D.sarikaya-6lo-bootstrapping-solution]** EAP-TLS for Raw public key
- **[I-D.he-iot-security-bootstrapping]** EAP, PANA for various credential material
- **[I-D.kumar-6lo-selective-bootstrap]** DTLS for various credential material, order selected by Commissioning Tool (CT)

What is the credential issue?

- **Certificate:**

  high security, mutual authentication, PKI infrastructure, (de)centralized architecture, high computation and communication cost, should avoid complex trust dependency and circular dependency

- **Raw public key/self signed certificate:**

  high security, no authentication, decentralized architecture, high computation and communication cost

- **Pre-shared key:**

  high security, mutual authentication, decentralized architecture, low computation and communication cost

- **Product installed code(?) Thread Group:**

  high security, one-way authentication, centralized architecture, low computation and communication cost

Considering different networks

Such as IoT…

Things / different types of devices

- Thing categories with different Transmission technologies (e.g. Bluetooth LE, Ethernet, WiFi,…) and mix of Things with different capabilities
  - Personal devices
  - Sensors, Actuators
  - Computing devices
  - Relaying devices

Architecture

- Architectural aspects of Things without human interaction (personal awareness)
- Optimal architecture considering Things capabilities

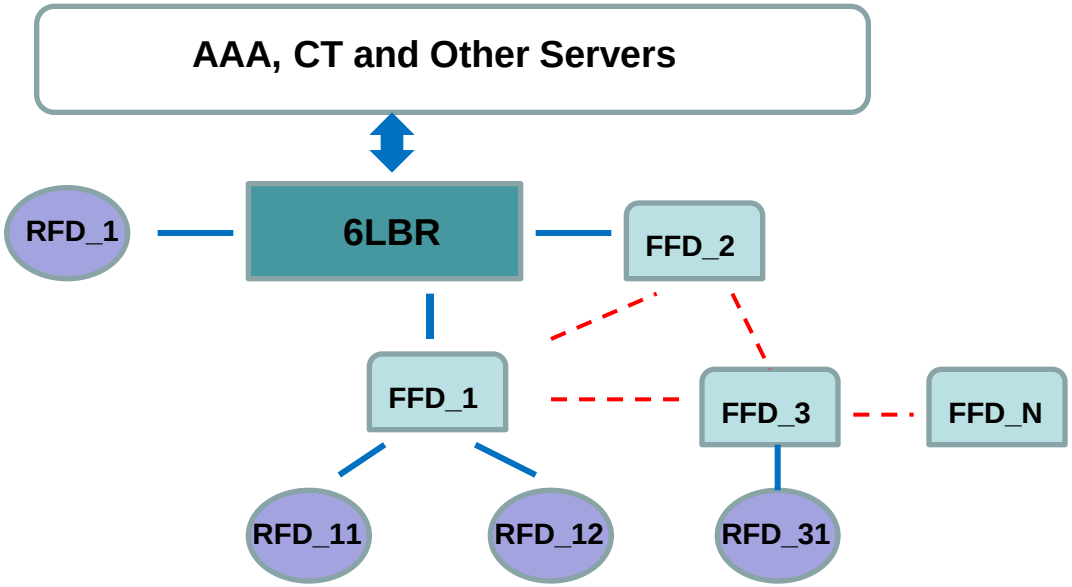
Network

- Automation of Things discovery and integration into the system
- T←→ T, T → T(relay, processing) → T
- Things network configuration with different topologies (e.g. Mesh, Star, Ring, line…)
- # of devices per Things domain/ perThings administrator

Application Layer (distributed, interaction)

- Communication relationships (e.g. Automation chains, federations) between Things
- Scheduled interactions Vs. Event driven Vs. Human interaction
- Different Services (e.g. Monitoring, Control, Configuration management, etc.)

What is the Problem?



IEEE 802.15.4
Low rate, Low power
Different types of devices
Mix topologies: star, mesh, cluster-tree

Users are not experts
Devices without sufficient input interface
Scale can be large

Protocols e.g. 6LoWPAN ND, IPv6 over 802.15.4, RPL, AODV, DSR, DTLS, CoAP can be selected for different applications

Security self-bootstrapping is fundamental to Self-Organizing IoT

A new device joining the network securely
The bootstrapping of all other information can be conducted securely

How should a good design be like?

- Able to clearly define security dependency and trust domains
  - Clear Security dependency
  - Mutual authentication
  - Agreement on security association
- Cross-layer design
  - Security bootstrapping in collaboration with other layers is likely to produce a comprehensive solution.
- Reduce human interaction to the minimum
- Able to resist attacks
- Low computation cost and communication overhead

Detailed comparison of [I-D.pritikin-anima-bootstrapping-keyinfra] and [I-D.kwatsen-netconf-zerotouch]

Referenced Solution	Credential	Initial Req. of HW	Component	Domain	Ownership
[I-D.pritikin-anima-bootstrapping-keyinfra]	802.1 AR MASA Auth. Token Domain Certificate	802.1AR, TA of Factory, private key	Proxy, Registrar, DHCP, Orchestrator, Factory CA, MASA Service, Domain CA	Y	N
[I-D.kwatsen-netconf-zerotouch]	IDevID x.509 Cert. of bootstrap server Owner certificates Owner voucher	802.1AR, Cert. of bootstrap server TA of Owner certificates TA of Owner voucher List of BS Private key	DHCP, Bootstrap server, NMS, Vendor	N	Y

Applying both methods to IoT network

[I-D.pritikin-anima-bootstrapping-keyinfra]

- Proxy , router are also constrained things, DOS should be prevented at the first hop.
- Ownership is important for IoT and should be considered.
- Registrar's 802.1AR can't be used to validate the ownership. Validate the owner's manipulation is more important.
- DHCP service are realized/relayed by constrained things:
  - DoS attack in relay mode for relay element.
  - Cost of DHCP service at constrained things should be estimated.
  - Reflect attack of forged DHCP configuration
- Domain certificate increases the burden of constrain device.
- Relay of cert. based authen. message is cost.

[I-D.kwatsen-netconf-zerotouch]

- Many pre-configured credential material stored on device.
- The trust relationship is more complicate and should be succinct for IoT scenario.
- The same DHCP service security issues occur
- Ownership is preferred for IoT, but it should be fetched/modified online rather than pre-installed on the device. A cloud or database should be built at the vendor/manufacturer side.
- Relay of many cert. based authen. message costs higher than **[I-D.pritikin-anima-bootstrapping-keyinfra]**

Improve both works for security bootstrapping of heterogeneous autonomic network

- PKI technology may be sound, but implementing it correctly can be very difficult.
- One framework that supports different credential material?
- One framework that supports different network topologies?
- One framework that also considers constrained devices and constrained communications?
- Different levels of ownership should be considered, owners are able to upgrade devices. Owners might change their password/token at the vendor side. Owner can be changed.

Thank you!

Any Comments?

Ana(Danping) He ana.hedanping@huawei.com

Behcet Sarikaya Sarikaya@ieee.org

Appendix

C1: Able to clearly define security dependency and trust domains

Referenced solution	Clear Security dependency	Mutual authentication	Agreement on security association
[I-D.pritikin-anima-bootstrapping-keyinfra]	Y	Y	Y
[I-D.sarikaya-6lo-bootstrapping-solution]	N	N	Y
[I-D.struik-6tisch-security-considerations]	Y	Y	Y
[I-D.kwatsen-netconf-zerotouch]	TBD, different certificates and trust relationship	Y	Y
[I-D.he-iot-security-bootstrapping]	Y	Y	Y
[I-D.kumar-6lo-selective-bootstrap]	Y	N	Y
ZigBee IP stack based Smart Energy	Y	Y	Y

C2 &C4: Cross layer design and Reduce human interaction to the minimum

Referenced solution	Cross layer design	Reduce human interaction to the minimum
[I-D.pritikin-anima-bootstrapping-keyinfra]	N	Y, but certificate management is expensive
[I-D.sarikaya-6lo-bootstrapping-solution]	Y	Y
[I-D.struik-6tisch-security-considerations]	N	Y, but certificate management is expensive
[I-D.kwatsen-netconf-zerotouch]	N	Y, but certificate management is expensive
[I-D.he-iot-security-bootstrapping]	Y	Y
[I-D.kumar-6lo-selective-bootstrap]	Y, but unsecure routing is used to relay the bootstrapping messages	N, requires CT and Commissioner's decision on the bootstrapping order.
ZigBee IP stack based Smart Energy	N/A	N/A

C3: Able to resist attacks

Referenced solution	Able to resist attacks STRIDE
[I-D.pritikin-anima-bootstrapping-keyinfra]	S(DHCP), D (exhausting the RE's resource)
[I-D.sarikaya-6lo-bootstrapping-solution]	S, T, R, D
[I-D.struik-6tisch-security-considerations]	Y
[I-D.kwatsen-netconf-zerotouch]	S, D
[I-D.he-iot-security-bootstrapping]	Y
[I-D.kumar-6lo-selective-bootstrap]	S, T, R, I, D
ZigBee IP stack based Smart Energy	S, T, D