Bootstrapping Key Infrastructures

draft-pritikin-anima-bootstrapping-keyinfra-01.txt

92\textsuperscript{th} IETF, 24 Mar 2015
Max Pritikin
Michael Behringer
Steinthor Bjarnason
Outline

1. Introduction
2. Architectural Overview
3. Operational Overview
4. Functional Overview
5. Protocol Details
6. Reduced security operational modes
7. Security Considerations
8. Acknowledgements
9. References

Describe “optimal” approach

Describe “sub-optimal” (but pragmatic) alternatives
Secure Enrolment Process

New device

Proxy

Registrar

MASA Service

“my unique device identifier” (802.1AR / SUDI)

“my domain certificate”

“new device with ID x”

Accept?

Accept?

new device ID x; domain y

Authorization token

Audit log for device

Join?

Domain parameters

Authorization token

Domain enrolment

Domain certificate

Domain parameters

Authorization token

Domain enrolment

Domain certificate

All decisions are in the domain!!
Features

• New device has only link local connectivity
  – Can only attack first hop

• New device can be cryptographically authenticated

• New device can authenticate network
  – Join only the authorized network

• Applicability: Potentially anywhere, network devices, sensors, etc.
Possible Security Zones

Field devices, e.g., factory floor

New device

“my unique device identifier”
(802.1AR / SUDI)

“my domain certificate”

Join?

Domain parameters

Authorization token

Domain enrolment

Domain certificate

Proxy

“new device with ID x”

Accept?

MASA Service

Internet

“new device ID x; domain y”

Accept?

Audit log for device

Authorization token

Domain parameters

Domain enrolment

Domain certificate

Registrar

Domain parameters

Authorization token

Join?

Domain enrolment

Domain certificate
Applicability: Homenet (a possible scenario)

New device

Proxy

Registrar

MASA Service

“challenge”

“my domain certificate”

“new device with challenge x”

Accept?

Homenet owner verifies “string”

Accept?

Join?

Domain enrolment

Domain certificate

Domain enrolment

Domain certificate

Domain parameters

Response

Domain parameters

Response

new device ID x; domain y

Authorization token

Audit log for device

Homenet owner

Verifies “string”
Discussion

• Approach relies on a link local proxy device
  – Need another approach when such a proxy not available
    Ex: draft-ietf-netconf-zerotouch

• Still needed:
  – Protocol Discussions
  – Cover the case where vendor MASA no longer available
    • Solution: Trust anchors from various MASAs
  – Description on how symmetric schemes are supported

• Applicability drafts for target architectures:
  – Homenet (draft-behringer-homenet-trust-bootstrap)
  – 6tisch
  – Others…
Relationship with draft-ietf-netconf-zerotouch: Today

Starting point: Device has IDevID

Case 1: link local response
Bootstrap using draft-pritikin-anima-bootstrapping-keyinfra

Case 2: DHCP response / DNS
Bootstrap using draft-ietf-netconf-zerotouch

Device receives domain certificate
Use to secure subsequent operations
- Download configuration
- Download image, licence, etc
- Secure management channels
Relationship with draft-ietf-netconf-zerotouch: Possible joint approach

Starting point: Device has IDevID

Case 1: link local response
  - Bootstrap using draft-pritikin-anima-bootstrapping-keyinfra

Case 2: DHCP response / DNS
  - Bootstrap using draft-ietf-netconf-zerotouch

Device receives domain certificate
Use to secure subsequent operations

- Download configuration
- Download image, licence, etc
- Secure management channels

Bootstrap Security
Operate Network