Bootstrapping Trust in a Homenet

draft-behringer-homenet-trust-bootstrap-01.txt

88th IETF, 7 Nov 2013

Michael Behringer

Max Pritikin

Steinthor Bjarnason

Overview

Problem Statement:

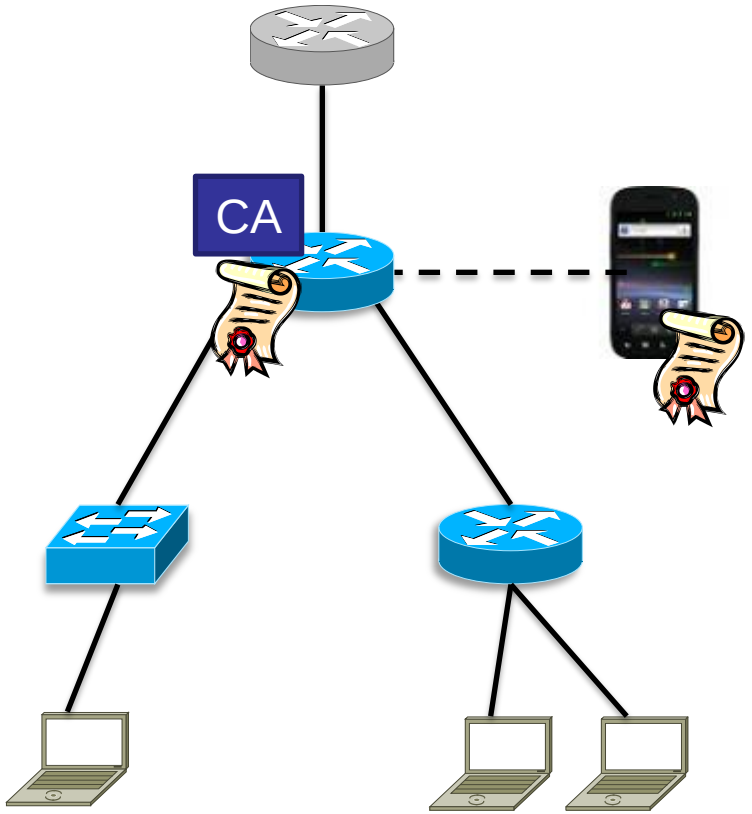
- **Find boundaries**
- **Establish trust to permit self-configuration**
  - **Devices need to know whether they are part of the homenet**

Change from -00:

- **Explained the approach in much more detail**

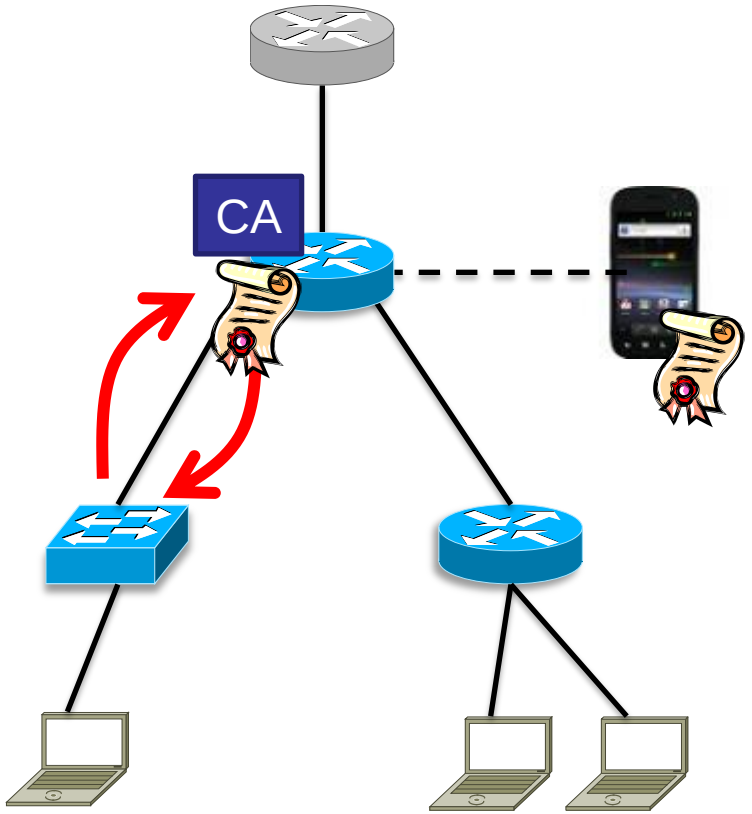
Approach:
1) Defining a Trust Anchor

- **Pair smart phone with a homenet device**
  - **As today**
- **Tell homenet device: "You're the trust anchor"**
  - **This enables a CA/RA function**
  - **Assign domain cert to smart phone**
  - **(Alternative: auto-select to be a trust anchor)**



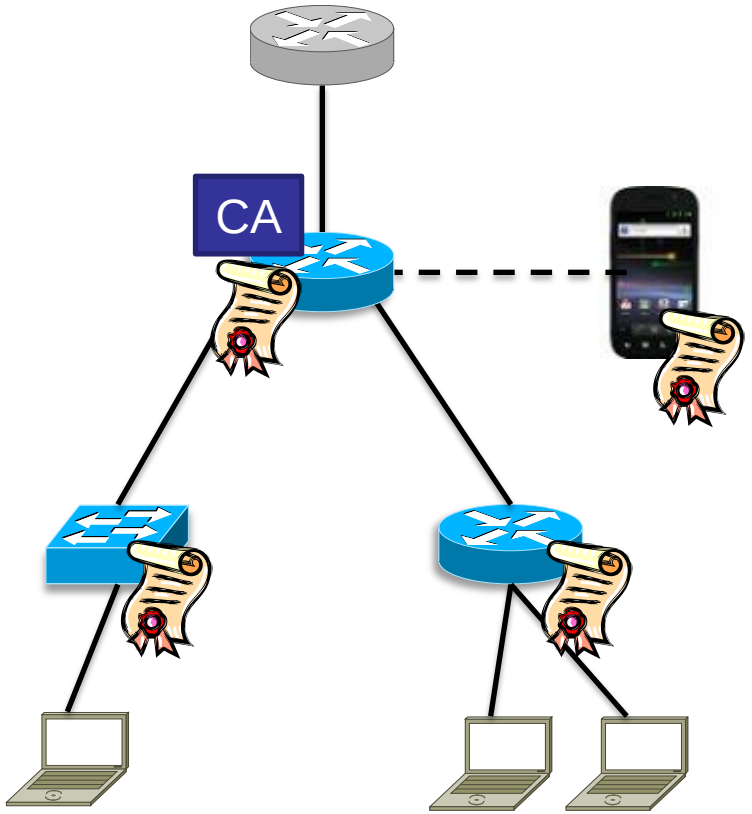
Approach:
2) Neighbor Discovery

- **A homenet device sends discovery messages on all links**
  - **If it has a domain cert: Send this**
  - **If it doesn't, send a device ID**



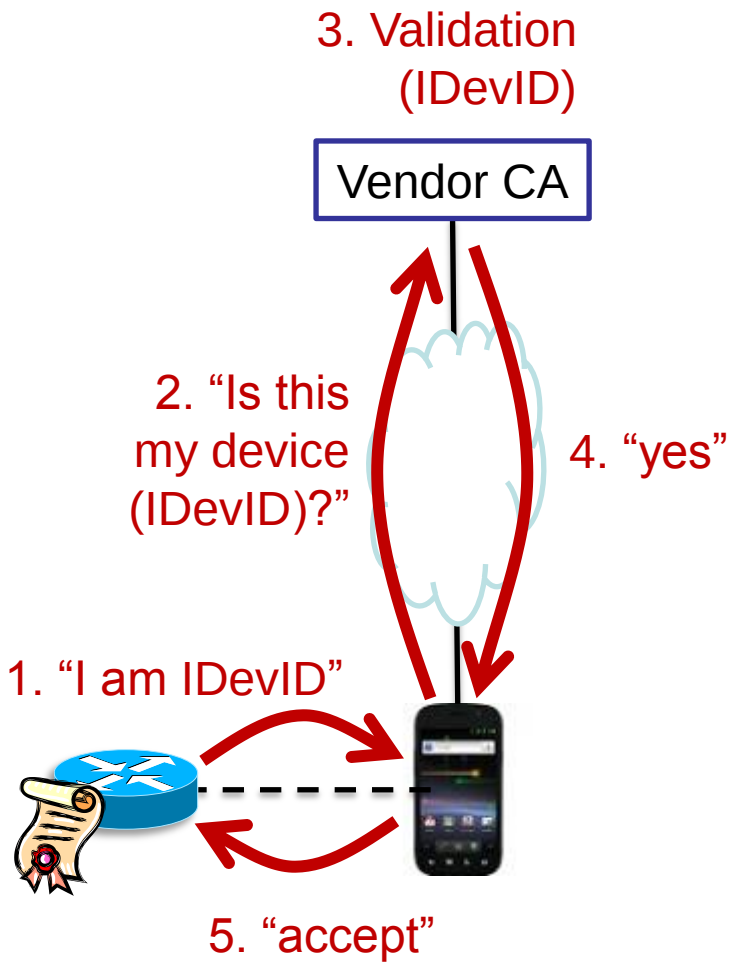
Approach:
3) Domain Join

- Device with domain cert invites device without domain cert
- Can validate on smart phone (optional)
- If new device accepted, it can enrol for a domain cert
- Result: All homenet devices have a domain cert



Approach:
3a) Validation using Vendor Cert

- **Devices may have 802.1ar IDevID (vendor cert)**
- **Use vendor cloud service to validate IDevID**
- **Accept device into domain if correct**
  - **Can exclude fake devices**



Result

- **User experience:**
  - **Plug in a device**
  - **“Ack” it on a user interface**
  - **done**
- **Benefits:**
  - **Boundary detection:**
    - **Peer doesn’t respond to my messages, or**
    - **Peer is in a different domain**
  - **Trust for self-configuration:**
    - **Routing**
    - **Addressing**
    - **…**