Architectural Considerations for IoT Device Security in the Home

A guide for ISPs specifying CPE devices

The IoT BCOP „Taskforce“

Initiated by Jim after RIPE-79

- Sandoche Balakrichenan
- Jelte Jansen
- Eliot Lear
- Jim Reid
- Michael Richardson
- Phil Stanhope
- Peter Steinhäuser
- Jan Žorž

Motivation for the document

- Number of IoT devices is growing rapidly
- Majority of the devices has to be considered to be insecure
- Availability of many standards and technologies related to IoT devices‘ security
- But IoT devices‘ software implementations still lack appropriate security measures
- „While there is progress on IoT standards and regulatory activities, and the future will be better, it's not evenly distributed yet, and we will always need mitigation of legacy“

→ It‘s time to look at things differently

Change of Perspective

- Improving security of IoT devices themselves will take time
  - Needs dealing with a countless number of device makers
  - Regulators will need time to define and **enforce** rules
- Day by day more of those devices are added to networks
- Shifting the view from the IoT devices themselves to the CPE / Home Gateway
  - Gatekeeper to the internet
  - Can be used to prevent unwanted traffic north– and southbound
  - Can „organise“ the consumer‘s internal network

→ Let‘s focus on the Home Gateway / CPE instead

This is not a BCOP document...

- Home Gateway / CPE firmware rarely deals with IoT devices
- IoT device security is still no major issue for Carriers and ISPs

→ There are no current practices for Home Gateways / CPEs at all ...

- While the content of this document could become BCOP when adopted, currently it‘s a „Proposed CPE evolution for IoT security“

Document Scope

- Targeted to ISPs and CPE makers
- Focus on consumer home networks
- Home networks are considered a critical space when it comes to IoT security
- Home customers are security unaware
- ISPs and Carriers (should) have a strong interest in securing their customer's networks
  - Reduces support effort due to hacked devices
  - Avoid network limitations due to malicious traffic

  → Keep their customers **happy (!)**

Approach

- **Practice oriented** – take what‘s already there
- The document does not deal with
  - Upcoming standards
  - Emerging technologies
- The document delivers
  - methodologies to handle parts of an IoT device's lifecycle
  - Principles device manufacturers should follow to ensure customer safety and privacy
  - References to suitable technologies and standards

Document Structure

- Securely introducing the device to the network
  - Use of Device Provisioning Protocol
- Providing appropriate access to the device
  - Use of fingerprinting and Manufacturer Usage Descriptions
- Monitoring device behaviour and limiting its access
  - Responsibilities of the CPE and others
- User Interactions
  - What an approval flow might look like and who has responsibility to do what
- Putting it all together
  - ISP provided secure devices
  - Customer provided second Home Router device (stacked devices)
  - Some principles on **device safety** and **privacy**

It's just the beginning...

- Providing the initial version of the document is just a first step
- The authors hope for
  - Feedback from the community
  - Discussions with Carriers and ISPs
- Next steps would/could be
  - Improving the document and adding emerging standards and technologies
  - Providing a reference configuration for OpenWrt
    (needs some work on providing packages, i.e. for DPP)

Discussion

- Questions / Remarks?