Spinning CPEs

Collaborative work on CPE IoT protection

Peter Steinhäuser – Embedd
Jelte Jansen – SIDN Labs

RIPE 78 - May 23, 2019

So, about that IoT

Ways to add some ‘s’ to IoT

- Better practices for manufacturers?
- Better (free) standard software libraries?
- International policy, regulation, and certification?
- Generate market demand for secure products?
- Quarantine bad actors at ISP level?
- Educate users?
- Empower users?

Ways to add some ‘s’ to IoT

- Better practices for manufacturers?
- Better (free) standard software libraries?
- International policy, regulation, and certification?
- Generate market demand for secure products?
- Quarantine bad actors at ISP level?
- Educate users?
- Empower users?

“Yes”

Ongoing work around IoT (security) in IETF

Manufacturer Usage Description (MUD) Specification – RFC8520

- Limit the Internet destinations of Things in networks.
- Thing tells the location (URL) of it's communication profile
- Communication profile is enforced (MUD file)
- Enforcement of communication profile is also usefull for other applications
- https://datatracker.ietf.org/doc/rfc8520/

Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Call Home - Drafts

- With the DOTS initiative, information on DDoS attacks is shared and analysed
- A major part of the DDoS sources are IoT devices.
- With the DOTS .. Call Home initiative, IoT devices can selectively be quarantined
  - Based on 5-tuple (IP addresses, portnumbers & time stamp)
  - Service providers can use this feature without knowledge about the Thing (Privacy!)
- https://datatracker.ietf.org/doc/draft-reddy-dots-home-network/

Formal standardization in ISO/IEC and CEN/CENELEC

- Formal standardization is country – region – worldwide organized; CEN & CENELEC European, ISO & IEC worldwide
- CEN/CLC/JTC 13 aims at Cybersecurity and Data Protection including IoT
- WG 6: Security of products including related services and environments
- In the Netherlands there is an initiative to focus om IoT Security & Privacy standardisation
- A similar initiative might be happening in your country

- Formal standardization often takes place in alignment with regulators.
- There are already government initiatives to improve IoT security:
  - Code of Practice for consumer IoT Security (UK)
  - Baseline Security Recommendations for IoT (EU ENISA)
  - Radio Equipment Directive (RED)
  - (there are ~12 European directives / recommendations / regulations that could improve IoT security)
- Could end up in certifications

Ways to add some ‘s’ to IoT

- Better practices for manufacturers?
- Better (free) standard software libraries?
- International policy, regulation, and certification?
- Generate market demand for secure products?
- Quarantine bad actors at ISP level?
- Educate users?
- **Empower users: SPIN**

IoT at SIDN / SPIN goals

- Protect home networks from rogue/insecure IoT devices

- Protect the Internet from home networks

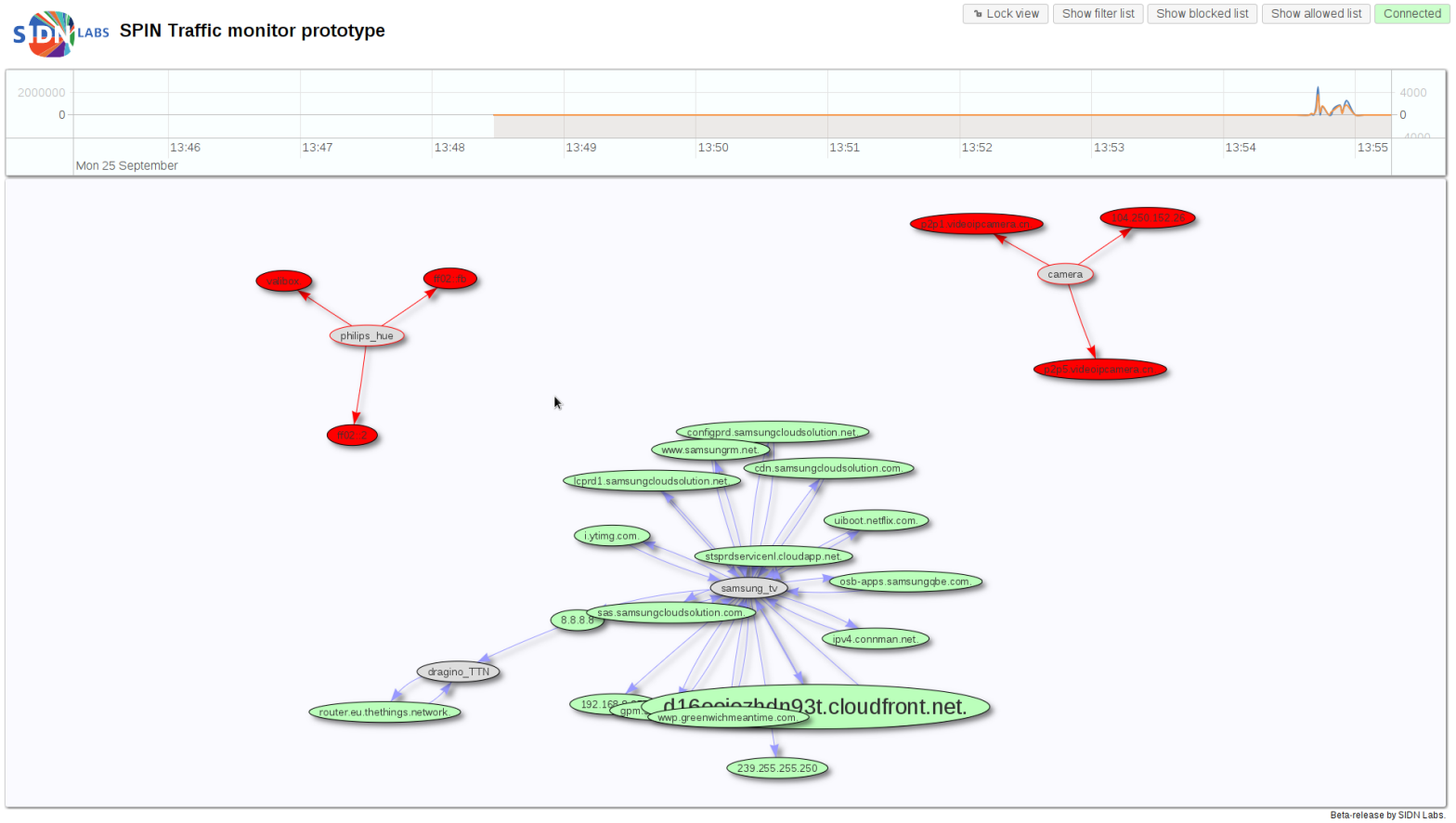
The SPIN project at SIDN Labs

- Security and Privacy for In-home Networks
- Research into ways of SPIN functionality:
  - Empower home users
  - Protect home network
  - Protect from home networks
- Software prototype(s)
  - Traffic monitor
  - Traffic analysis (local!)
  - Traffic control

Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based on source or destination

- In latest release:
  - Select device and download (live) pcap for selected device



Core components, changes after talks with CPE people

Since last presentation here, lots of talks and collaboration

Other changes after talking to random people (tm)

- Valibox release images now available for other systems
  - Raspberry Pi v3
  - VirtualBox
- Adding prototype ‘spin-off’ tools in releases
  - Pcap-reader
  - Peak-detection
  - Fancier custom interface
  - Pre-dots-signal-home (‘incident reporter’) PoC
- Some of this in current release, some will be in next

Core components, changes after talks with CPE people

- Use standard kernel modules for traffic capture
  - (custom kernel module too scary)
- Add UCI (and soon luci) configuration
  - (easier integration with configuration tools)
- Add RPC with optional UBUS support
  - (easier integration with control tools)
- Better packaging
  - (easier deployment)
- Some of this in current release, some will be in next

Why CPE?

- Previous SPIN setups required a separate device
- Moving SPIN and related services into the CPE reduces home network complexity
- Putting SPIN to the home network's "border" simplifies
  - Automatic actions like firewalling malicious devices
  - Reporting unusual activities to the ISP to initiate further analysis/actions
- Could significantly improve the coverage and adoption of SPIN

Why OpenWRT?

- Quasi-standard SDK for open source CPE firmware development
- Wide hardware support (QCA / BRCM / MTK / Marvell…)
- Gaining more and more industry support, even adopted by some chipset makers (i.e. QCA QSDK)
- Simple integration as an opkg; information here:
  - https://github.com/SIDN/spin/blob/master/doc/install_package.md
  - Hassle-free install work in progress

embeD SIDN LABS

Related initiatives

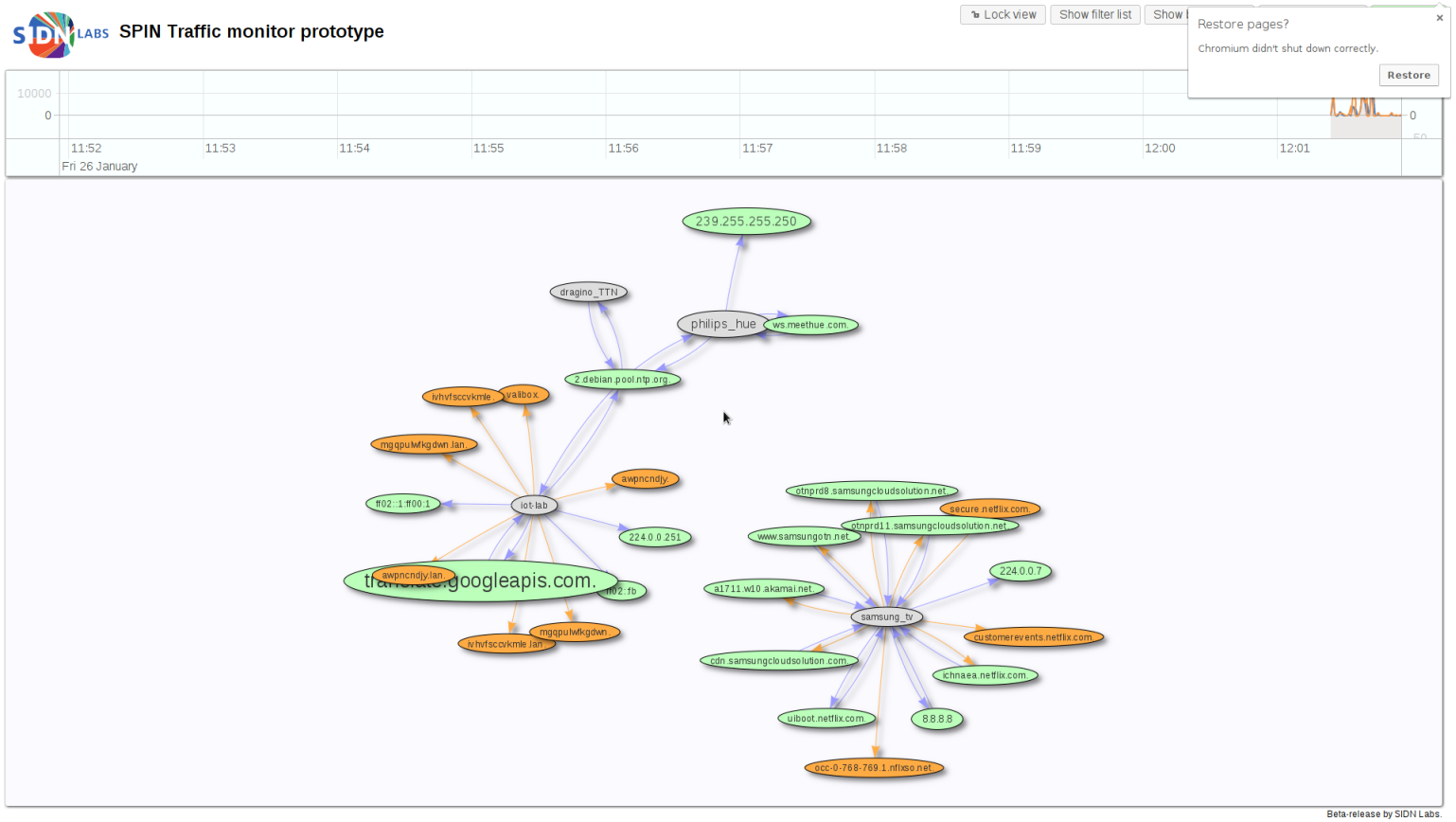
Broadband Forum Collaboration

- CPE management standards are set in the Broadband Forum
- Best known for TR-069 (to be replaced by USP), which is behind the over 1 Billion broadband connections.
- IoT and security are hot topics; next meeting will have a Security BoF.

“Fixing” UPnP on CPE’s

- When UPnP is enabled on a CPE (~75%), all traffic measures can be overruled be devices on the local network.
  - Source: https://blog.trendmicro.com/trendlabs-security-intelligence/upnp-enabled-connected-devices-in-home-unpatched-known-vulnerabilities/
- No improvement / standardization effort is identified to address this issue.

Demo


SPIN Traffic monitor prototype
Lock view
Show filter list
Restore pages?
Chromium didn't shut down correctly.
Restore
10000
0
11:52
11:53
11:54
11:55
11:56
11:57
11:58
11:59
12:00
12:01
Fri 26 January
239.255.255.250
dragino_TTN
philips_hue
ws.meethue.com
2.debian.pool.ntp.org
ivhvfsccvkmle
vaillbox
mgqpulwfkgdwn.lan
awpncndjy
ff02::1:ff00:1
iot-lab
224.0.0.251
awpncndjy.lan
translate.googleapis.com.
ff02::fb
mgqpulwfkgdwn
ivhvfsccvkmle.lan
otnprd8.samsungcloudsolution.net
secure.netflix.com
otnprd11.samsungcloudsolution.net
www.samsungotn.net
224.0.0.7
a1711.w10.akamai.net
samsung_tv
customerevents.netflix.com
cdn.samsungcloudsolution.com
ichnaea.netflix.com
uiboot.netflix.com
8.8.8.8
occ-0-768-769.1.nflxso.net
Beta-release by SIDN Labs.

Discussion/questions/cheers/tomatoes

Go try it out!

(and send us feedback)

((or any other suggestions))

Jelte Jansen

jelte.jansen@sidn.nl

https://sidnlabs.nl

Peter Steinhäuser

ps@embedd.com

https://embedd.com