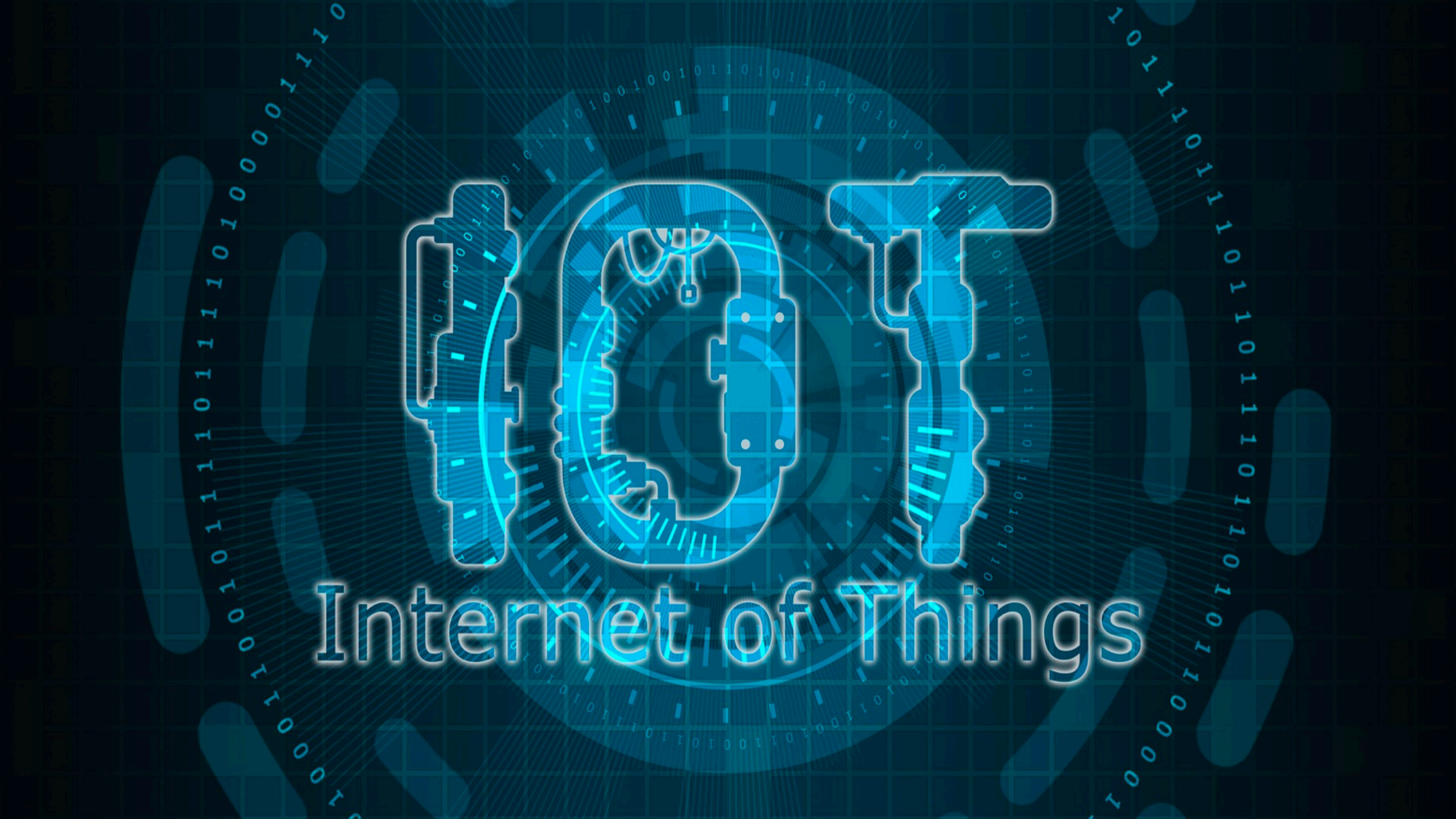
Security (and privacy) versus IoT

Elmer Lastdrager

SIDN Labs

KÉRASTASE

m


IOT
Internet of Things

YOU GET CONNECTED!
AND YOU GET CONNECTED!
EVERYTHING GETS CONNECTED!
imgflip.com

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?

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 useful 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, port numbers & 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

Additional standardization (or not)

Broadband Forum

UPnP / CPE Firewall

- When UPnP is enabled on a CPE (~75%), all traffic measures can be overruled by 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.

SIDN focus:

- Aiming to implement the security and privacy standardization initiatives.

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

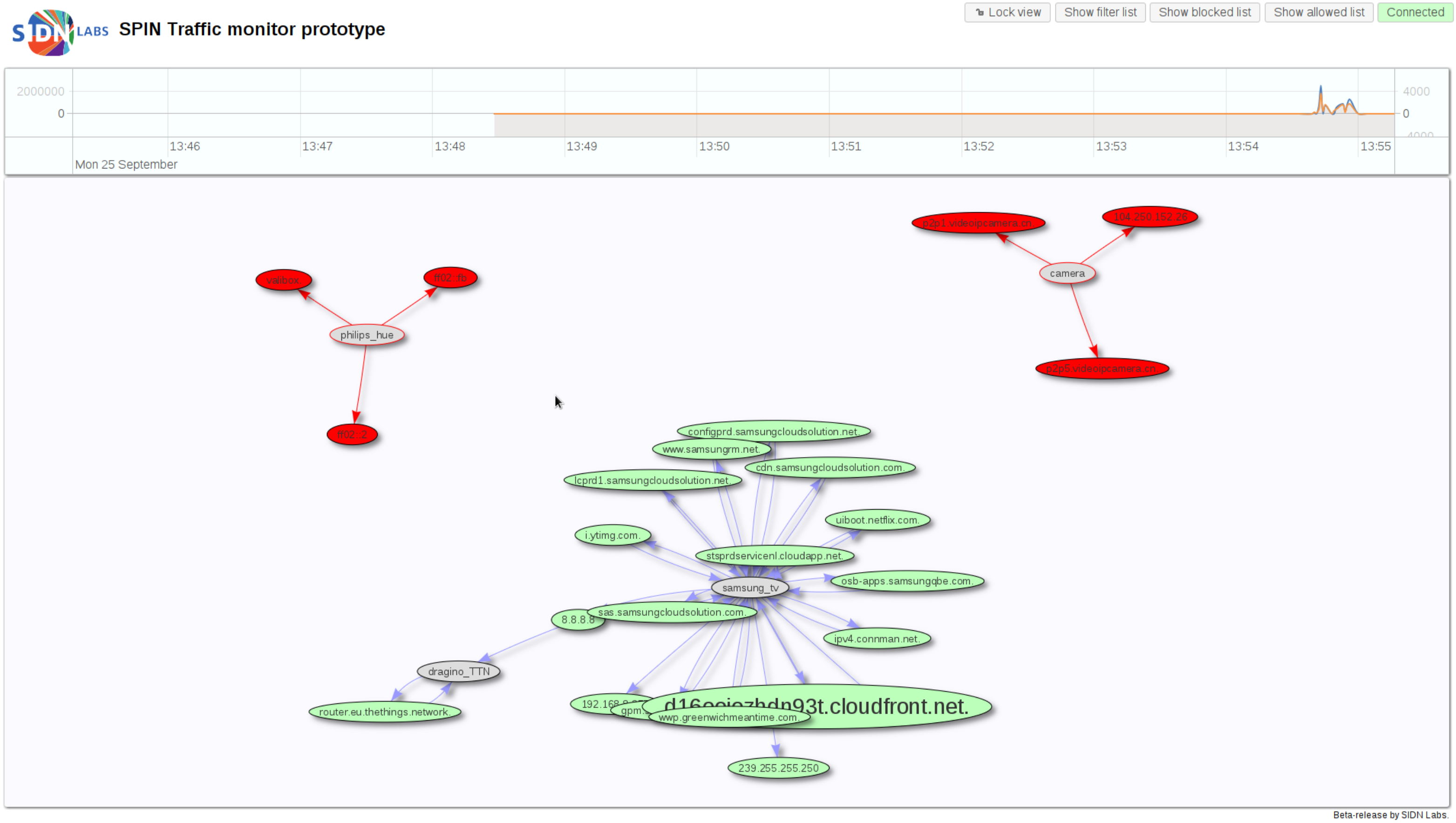
- Security and Privacy for In-home Networks

- 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



Why running security functions on router

- Previous SPIN setups required a separate device
- Moving SPIN and related services into the CPE reduces home network complexity (*from our point of view*)
- 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 security functions: *who buys a separate security device?*

Discussion points

- Feasible to run Anomaly Detection on CPE?
- Any interest into implementing security standards (MUD, DOTS, …)?
- Privacy versus manageability (involvement ISP?)

Follow us

.nl SIDN.nl

@SIDN

in SIDN

Thank you for your attention!

https://valibox.sidnlabs.nl
https://github.com/SIDN/spin

elmer.lastdrager@sidn.nl