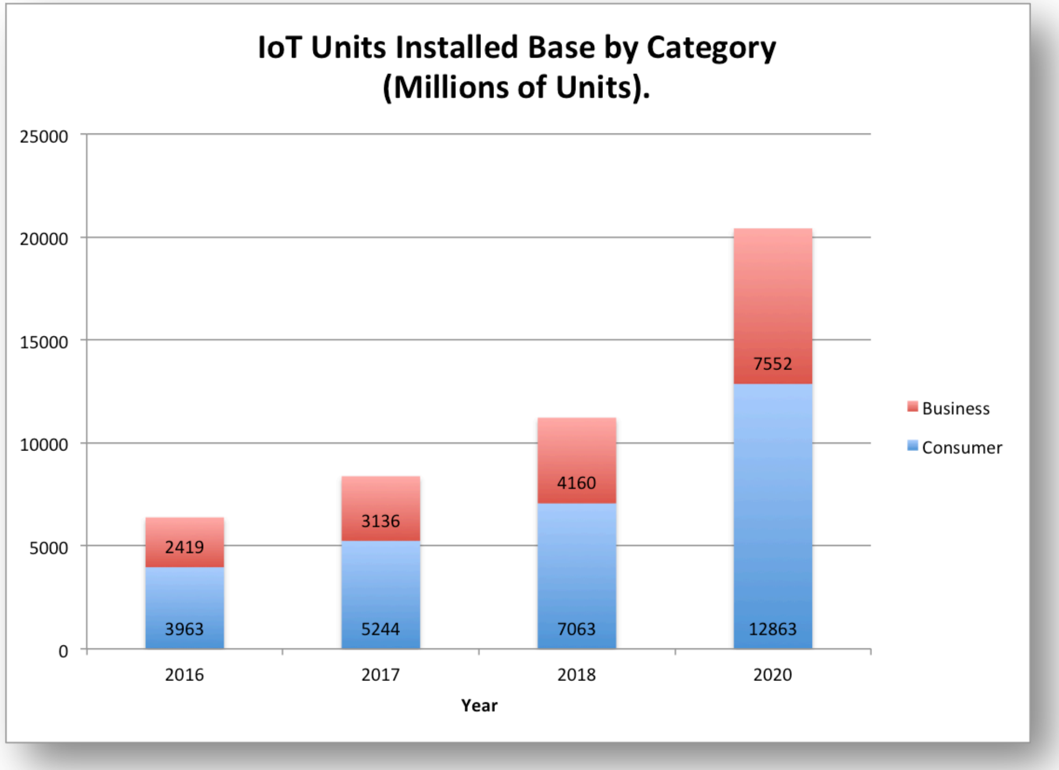
SPIN: Security and Privacy in the Internet of Things

Marco Davids

IETF 99
NMRG (IRTF)

What *is* the IoT?

- Quite a few definitions of IoT
  - I like the approach of RFC7452
- We may not agree on a definition…
- But we know there will be **plenty** of ‘IoT’!

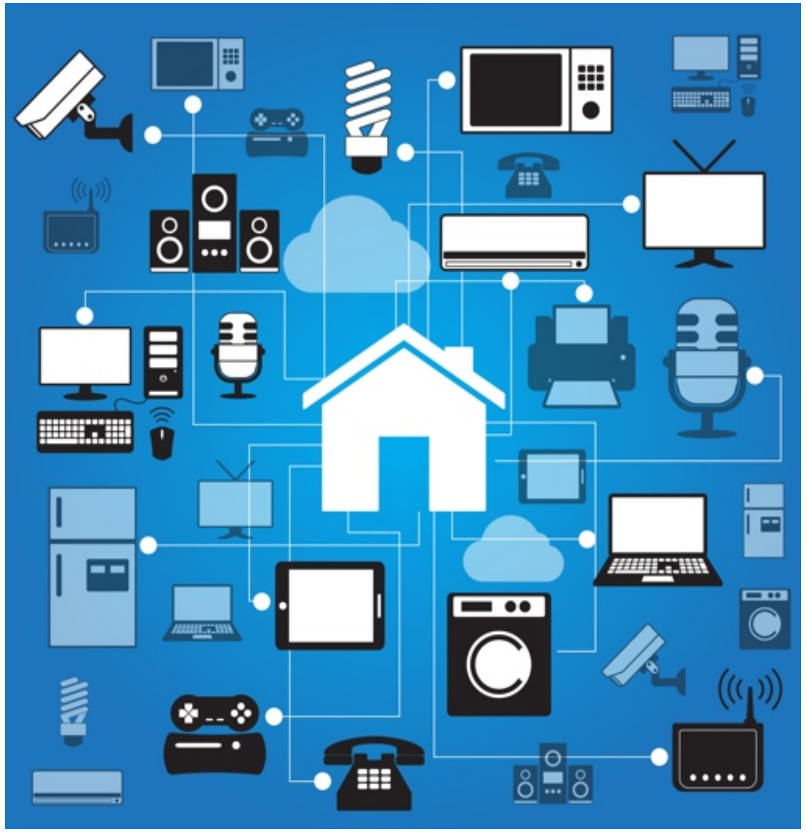


Source: Gartner

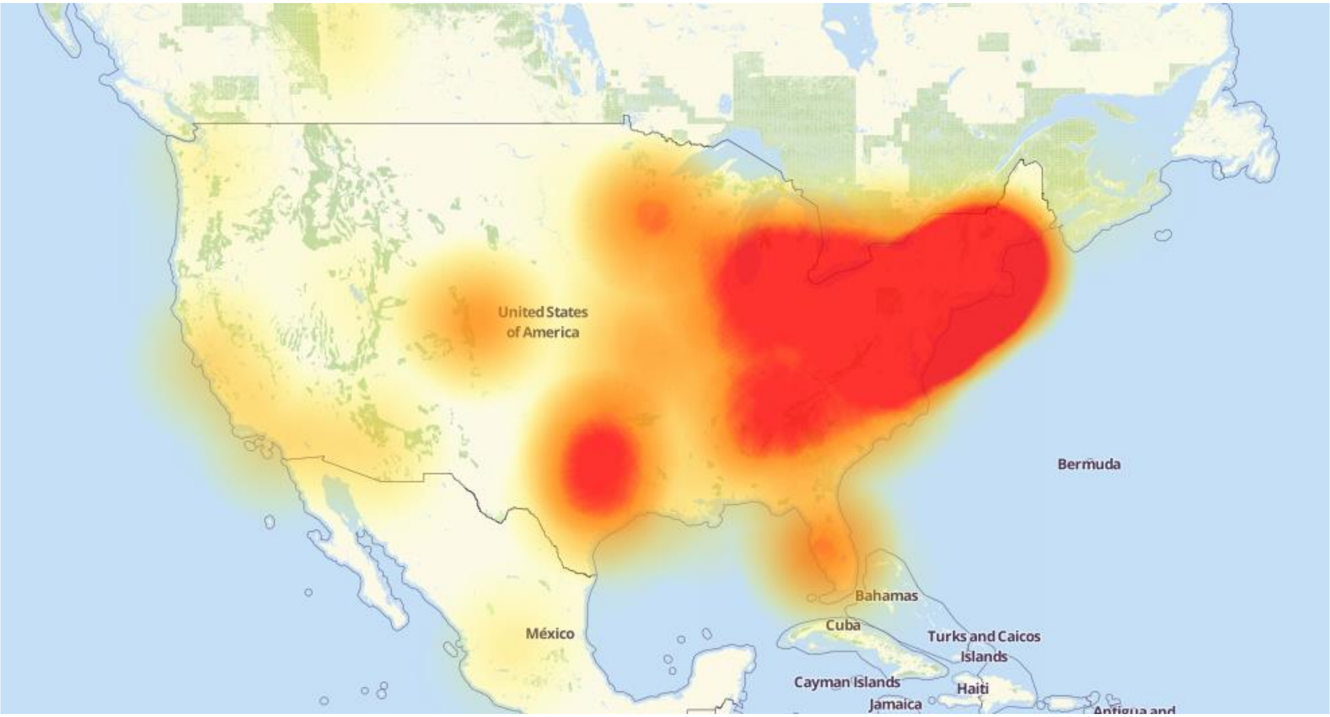
What *is* the IoT?

Actually it is (also):

- “One big mess”
- A security nightmare



The result…



https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

So, what to do about this?

- No silver bullet
- We need to do it **all**
- But in our project we focus on:

  -***Empower users***

The SPIN project

- ‘Security and Privacy for In-home Networks’

- Research the user-empowerment part:
  - Detect anomalies in the home network
  - Automatically block suspicious traffic to/from IoT devices
  - Inform the end user about the system’s findings and actions
  - Allow the user to configure security and privacy parameters

Motivation

- Protect infrastructure operators (such as SIDN)
- Give users more control over their in-home IoT
- Preserve trust in the internet

User centric approach

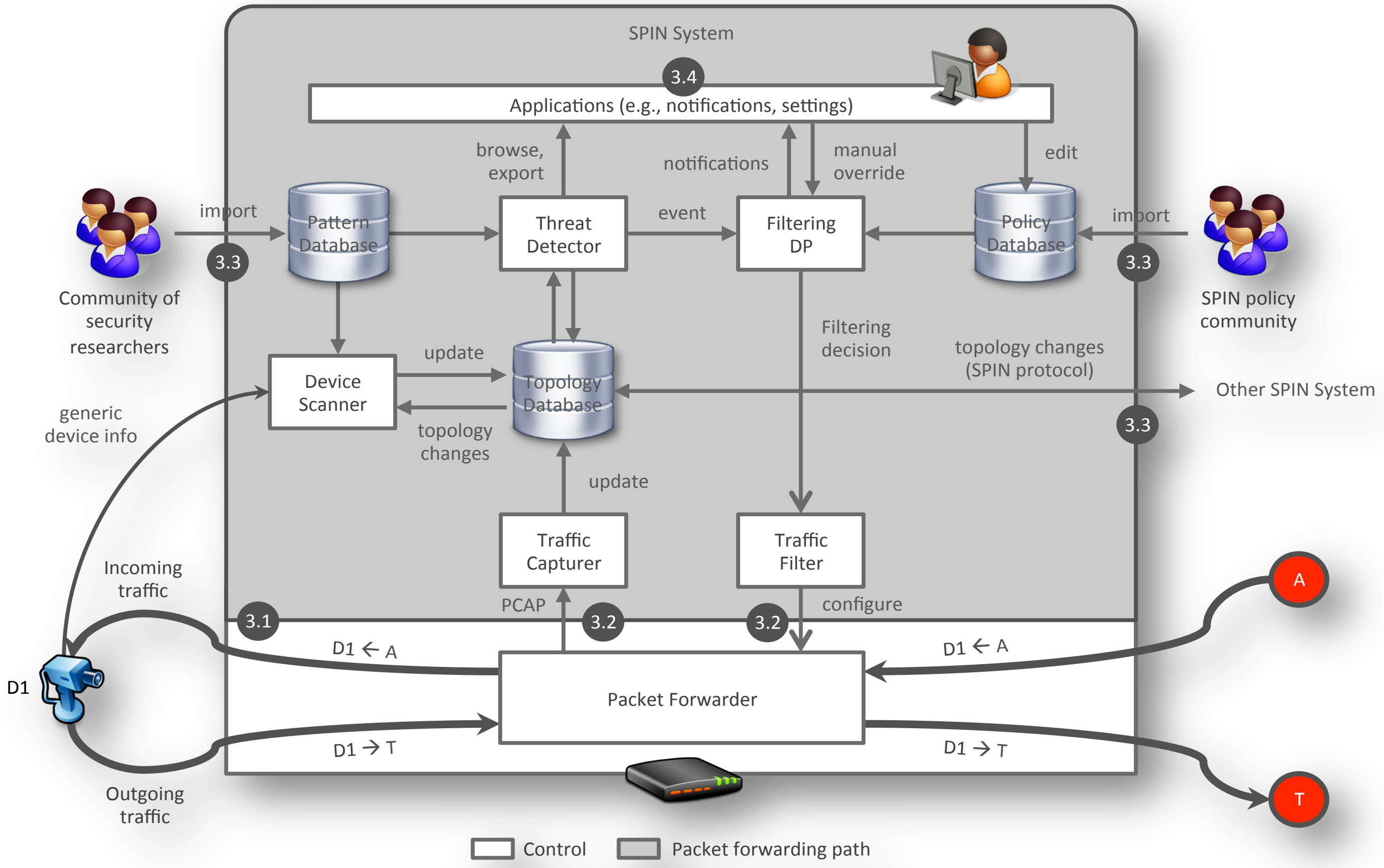
- Allow users to easily deploy it
- Protect users' privacy by keeping the intelligence within the home
- Allows users to configure the system with their security preferences

Also:

- Embrace collaborative 'security by design' security community

The SPIN concept

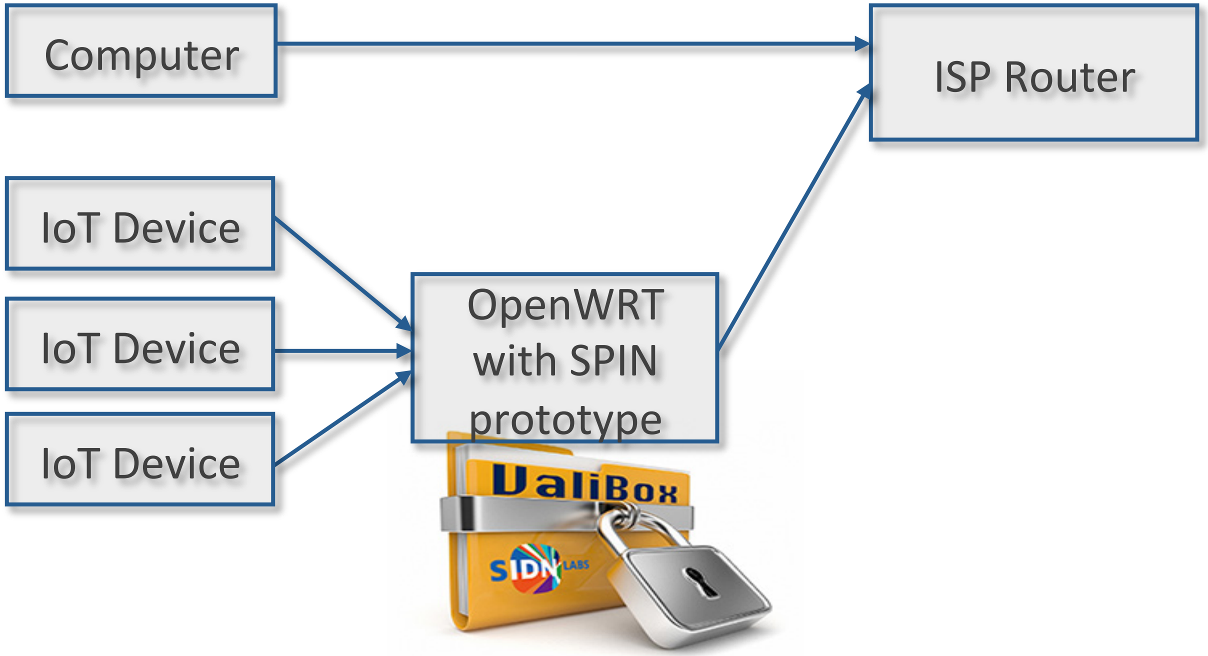
- SPIN controller
  - Visualize traffic
  - Monitor devices
  - Control traffic
- Processing is done locally
  - User in control
  - But largely automated



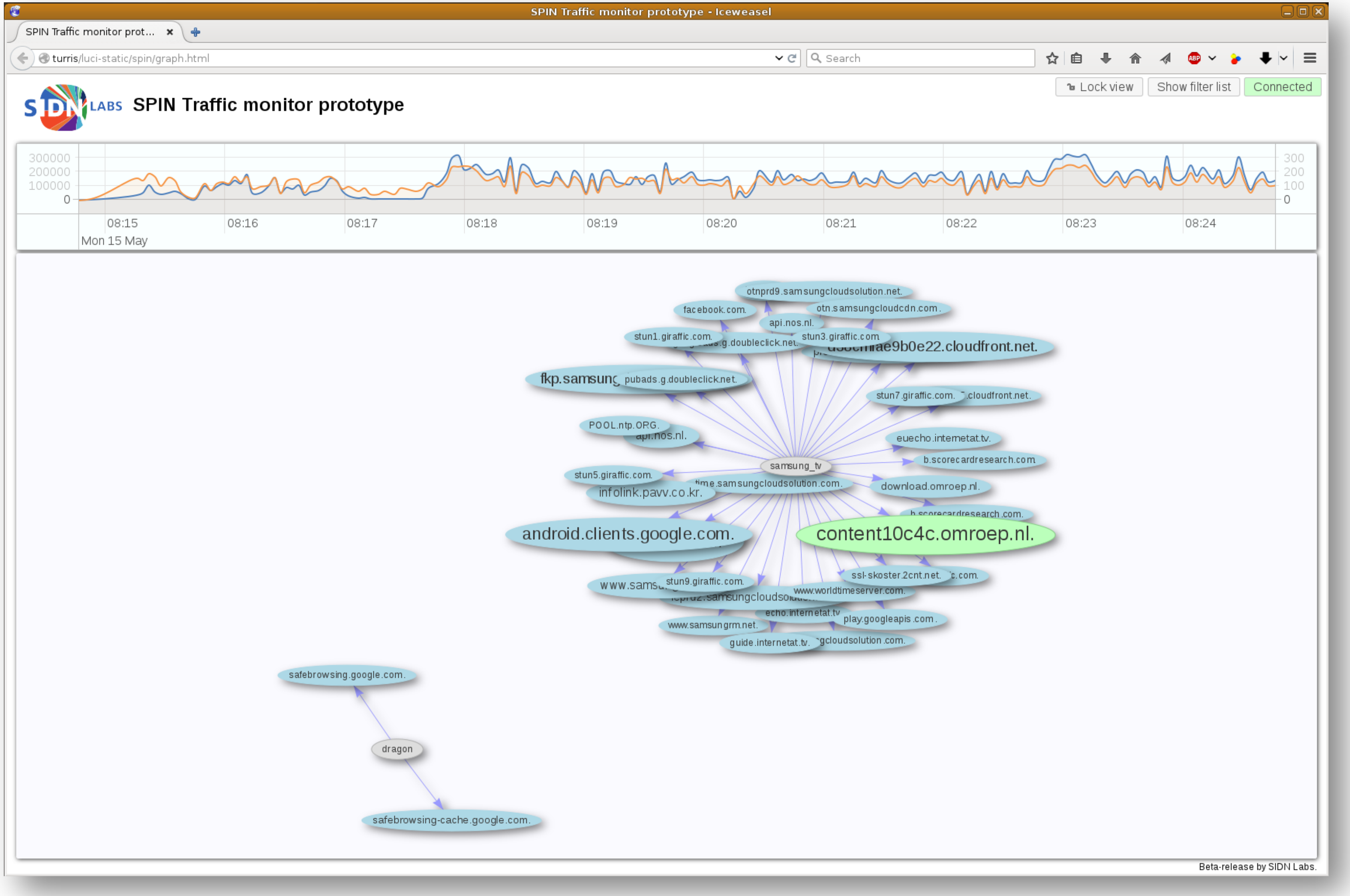
Prototype built on OpenWRT

- Currently bundled with our open source 'Valibox' software
- Working on a separate OpenWRT package feed
- Focus on IoT devices with 'predictable behavior'

prototype 2, GL-Inet hardware



Visualiser


SPIN Traffic monitor prototype - Iceweasel
SPIN Traffic monitor prot...
turris/luci-static/spin/graph.html
Search
Lock view
Show filter list
Connected
SIDN LABS
SPIN Traffic monitor prototype
300000
200000
100000
0
300
200
100
0
08:15
08:16
08:17
08:18
08:19
08:20
08:21
08:22
08:23
08:24
Mon 15 May
otnprd9.samsungcloudsolution.net.
facebook.com.
otn.samsungcloudcdn.com.
api.nos.nl.
stun1.giraffic.com.
g.doubleclick.net.
stun3.giraffic.com.
d38cmrae9b0e22.cloudfront.net.
fkp.samsung
pubads.g.doubleclick.net.
stun7.giraffic.com.
cloudfront.net.
POOL.ntp.ORG.
api.nos.nl.
euecho.internetat.tv.
samsung_tv
b.scorecardresearch.com.
stun5.giraffic.com.
time.samsungcloudsolution.com.
infolink.pavv.co.kr.
download.omroep.nl.
b.scorecardresearch.com.
android.clients.google.com.
content10c4c.omroep.nl.
ssl-skoster.2cnt.net.
c.com.
www.samsu
stun9.giraffic.com.
samsungcloudsolution
www.worldtimeserver.com.
echo.internetat.tv
play.googleapis.com.
www.samsungrm.net.
guide.internetat.tv.
gcloudsolution.com.
safebrowsing.google.com.
dragon
safebrowsing-cache.google.com.
Beta-release by SIDN Labs.

Current status

- Running prototype on our Valibox (OpenWRT) platform
  - Focus on privacy
  - ‘Vertical slice’ of the concept (modular deployment)
  - Visualize basic traffic (with DNS names, if known)
  - Block traffic to/from devices or external points
- Incremental updates deployed as features are implemented
- Software (free, go get it):
  - Open source: *https://github.com/SIDN/spin*
  - GL-inet images at: *https://valibox.sidnlabs.nl/*

Vision

- Get it into deployed devices
  - Bullguard Dojo seems similar, but is proprietary
  - So is the Bitdefender Box
  - NIC.CZ Turris router comes closer
- Become an open standard in/for home routers
  - We have it running on the Turris
- Work on interoperable ‘IoT security/privacy standards’
  - Protocols
  - Data formats
  - API’s

(T2TRG WG?)

Future Work

- Refinements
- Research question: how to protect the protector
- (Collaborate on) a platform for sharing IoT device information
  - In a uniform, standardized way
  - Repositories for known bad devices/versions
  - Trusted traffic profiles
    - “My TV should stream the news and Netflix, but do nothing else”
    - Perhaps something like **draft-ietf-opsawg-mud-08**?
- Interested in collaboration? Come talk!

Questions/ideas/suggestions?

Tech-paper about this on:

- https://www.sidnlabs.nl/a/weblog/spin-a-user-centric-security-extension-for-in-home-networks

Short URL:

http://tinyurl.com/SIDN-IoT

@marcodavids