Security and Privacy in the Internet of Things

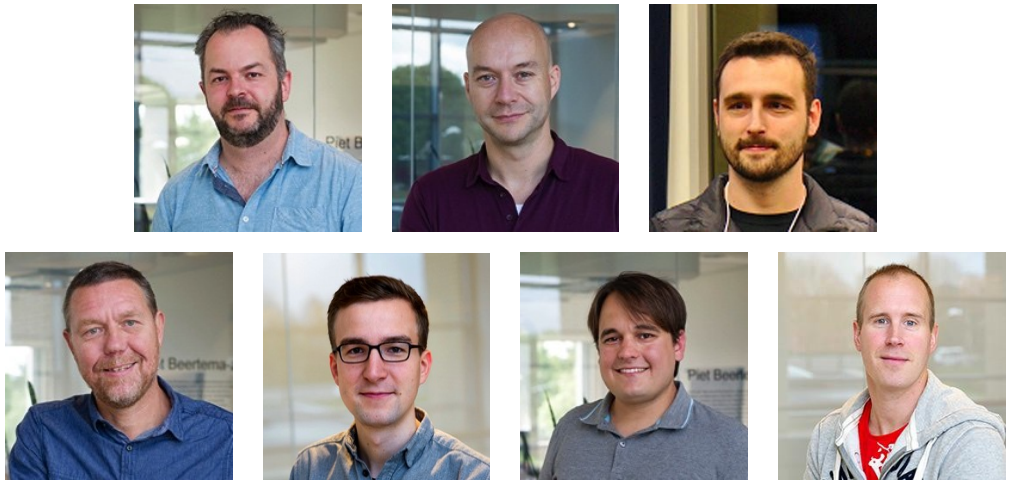
Jelte Jansen and Cristian Hesselman

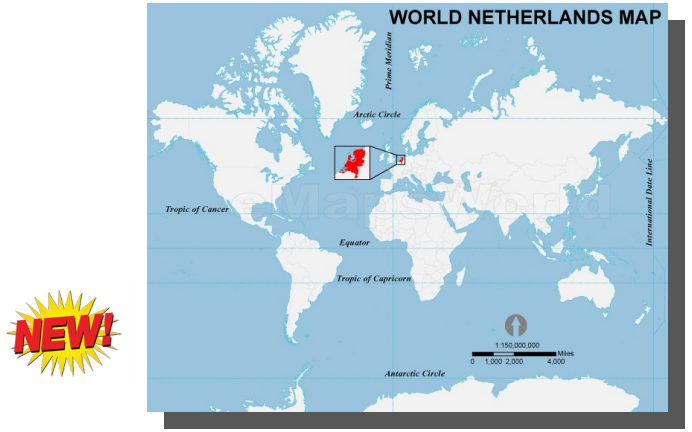
International ONE conference
2017-05-16

SIDN LABS

SIDN Labs

- Research team of the .nl registry operator, SIDN
- Goal: improve operational security, resilience, and privacy of the Internet infrastructure through measurement-based research and technology development
- Themes: DNS performance, privacy-aware network analytics, IoT security





.nl = the Netherlands
5.7M domain names
2.6M DNSSEC-signed
1.3B DNS queries/day

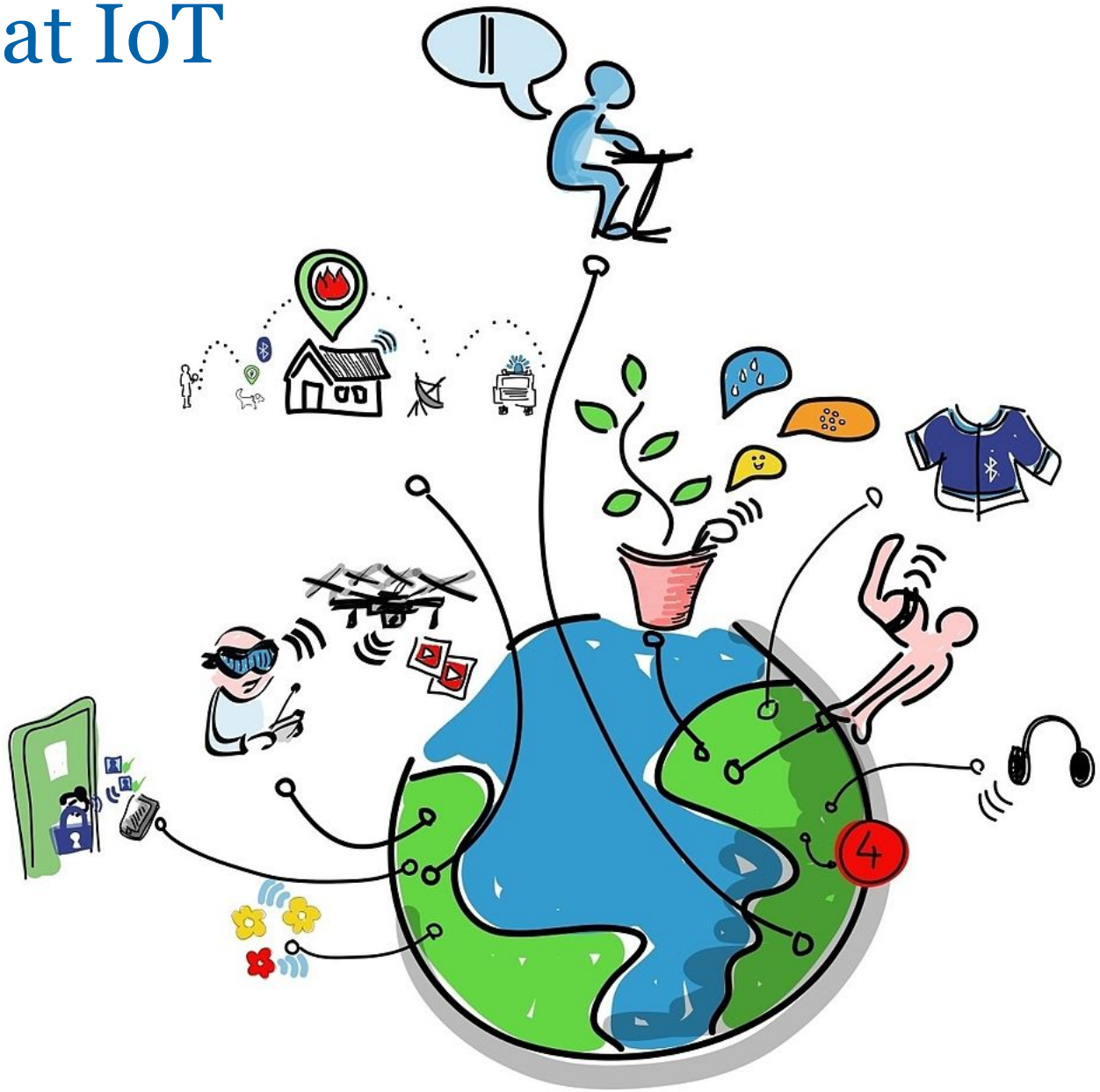
Security and Privacy in the Internet of Things

Jelte Jansen

International ONE conference
2017-05-16

SIDN LABS

So, about that IoT



What **is** the IoT?

- Wikipedia definition:

- “The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.”

What **is** the IoT?

- Global Standards Initiative definition:

- “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"[3] and for these purposes a "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks".”

What **is** the IoT?

- IEEE published a document: “Towards a definition of the IoT”
- Only 86 pages!

What **is** the IoT?

- A simpler definition:

- "Stuff that was not
- networked before"

What **is** the IoT?

- An even simpler definition:
- “One big mess”

What **is** the IoT?

- Many different **types** of things
  - Cameras
  - Lights
  - Sensors
  - Locks…
  - Cars……
  - Pacemakers……
- WiFi chips + IP stacks are cheap
- Also LoraWAN, ZigBee, local AP, ad-hoc networking, etc. etc. etc.

Some small issues

- Devices with security holes
- Devices are not updated
- Devices have no, or bad passwords
- Devices don’t encrypt data
- Devices leak sensitive data such as wifi passwords
- The list goes on and on

SIDN LABS

So, about that IoT

Home > Data Protection > Internet of Things

SLIDESHOW

The internet of insecure things: Thousands of internet-connected devices are a security disaster in the making

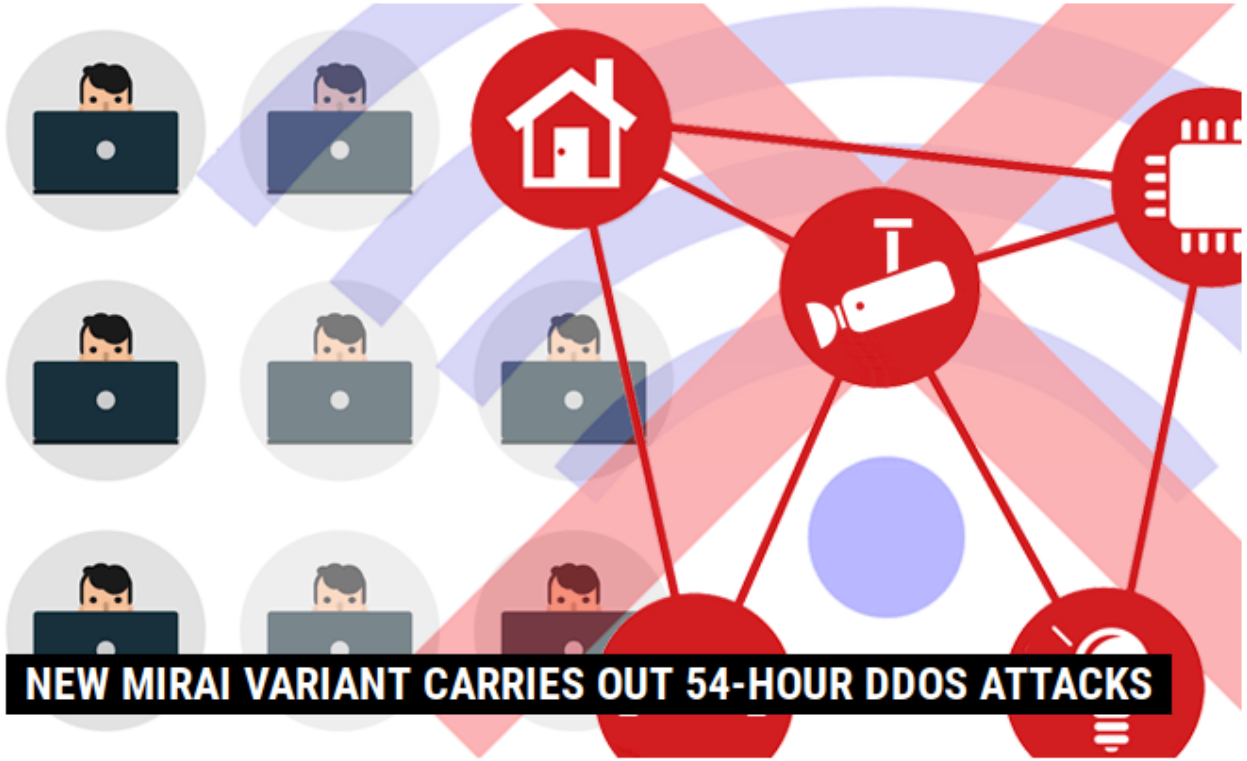
By Josh Fruhlinger, CSO | Oct 12, 2016 4:00 AM PT

So, about that IoT

threatpost

CATEGORIES | FEATURED | PODCASTS | VIDEOS

Welcome > Blog Home > Hacks > New Mirai Variant Carries Out 54-Hour DDoS Attacks



by Tom Spring

March 30, 2017 , 2:50 pm

SDN LABS

Why is that?

- Security is hard
- Security is expensive
- In some cases: security is not ‘userfriendly’
- Security is not a feature that sells devices
  - Time to market and price are
- Security is invisible

SIDN LABS

Just let the market fix it!

Computers will never be secure. To manage the risks, look to economics rather than technology

But will it?

"The market can't fix this because neither the buyer nor the seller cares.

The owners of the webcams and DVRs used in the denial-of-service attacks don't care. Their devices were cheap to buy, they still work, and they don't know any of the victims of the attacks.

The sellers of those devices don't care: They're now selling newer and better models, and the original buyers only cared about price and features.

There is no market solution, because the insecurity is what economists call an externality: It's an effect of the purchasing decision that affects other people. Think of it kind of like invisible pollution."

https://www.schneier.com/blog/archives/2017/02/security_and_th.html

SIDN LABS

Some users may care a bit

This guy's light bulb performed a DoS attack on his entire smart house

Kashmir Hill

3/03/15 9:41am · Filed to: REAL FUTURE

182

Some users may care a bit

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

BrickerBot, the permanent denial-of-service botnet, is back with a vengeance

New botnet squadrons wage fiercer, more intense attacks on unsecured IoT devices.

DAN GOODIN - 4/24/2017, 10:43 PM

Some users may care a bit

Hacker hijacks wireless...

www.computerworld.com/article/2878741/hacker-hijacks-wireless-foscam-l

Search

DON'T MISS: Excel 2016 cheat sheet · Do IT certifications matter? · Microsoft pulls plug on Win 10's debut version · Newsletters ·

COMPUTERWORLD FROM IDG

INSIDER Sign In | Register

Home > Security > Cybercrime & Hacking

SECURITY IS SEXY

By Darlene Storm, Computerworld | FEB 2, 2015 12:09 PM PT

About

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

NEWS ANALYSIS

Hacker hijacks wireless Foscam baby monitor, talks and freaks out nanny

This is the third time news has circulated about some jerk hijacking a wireless Foscam camera/baby monitor and made his virtual intrusion known by talking. Please change the default password!

MORE LIKE THIS

Hacker strikes again: Creep hijacks baby monitor to scream at infant and...

SDN LABS

And what about privacy?

- Privacy is hard
- Privacy is expensive
- In some cases: privacy is not ‘userfriendly’
- Privacy is not a feature that sells devices
  - At least, not as much as selling the private data
  - ‘you are the product’
- Privacy is invisible

SIDN LABS

So, what to do about this?

- 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?

SIDN LABS

So, what to do about this?

- 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"

SIDN LABS

So, what to do about this?

- No silver bullet
- We need to do it all
- But in this project we will focus on the last one:
  - Empower users

Users

- Some genuinely don’t care
- A lot actually do
- Problems:
  - Not aware
  - Not able to solve or fix

User questions

- How can I tell my device is hacked?
- Why doesn’t it just work?
- What devices are safe? How can I tell?

The SPIN project

- Security and Privacy for In-home Networks
- Research the user-empowerment part
  - Visualise network traffic (current prototype)
  - Block unwanted traffic (next prototype)
  - Scan devices (next project phase, with external researchers)
  - Sharing platform for device info (future?)

SIDN LABS

Motivation

- Protect internet infrastructure operators (such as SIDN) as well as
- other service providers

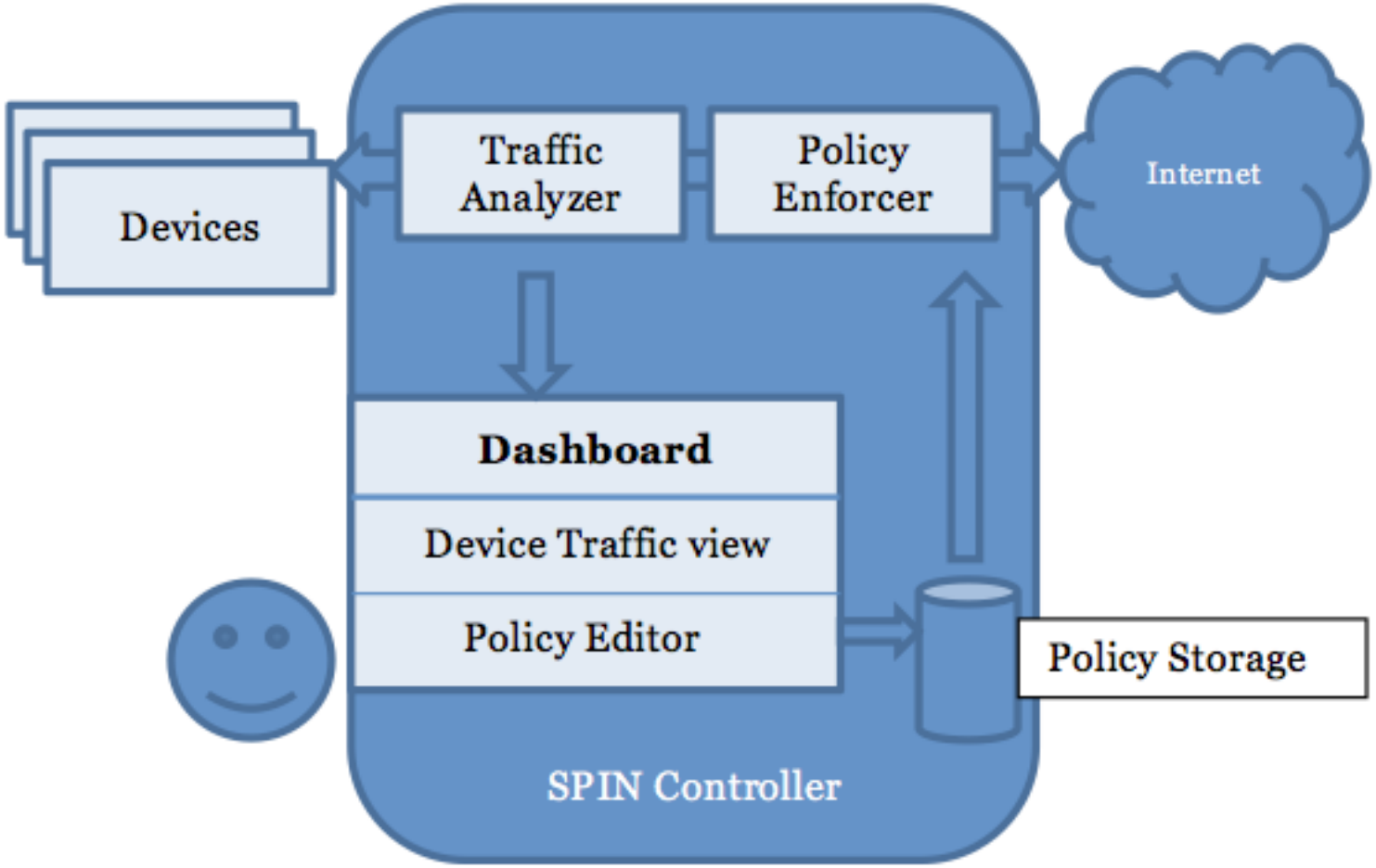
- Give users more control over their security and privacy in the IoT

- Preserve trust in the internet (fewer DDoS-es, less abuse)

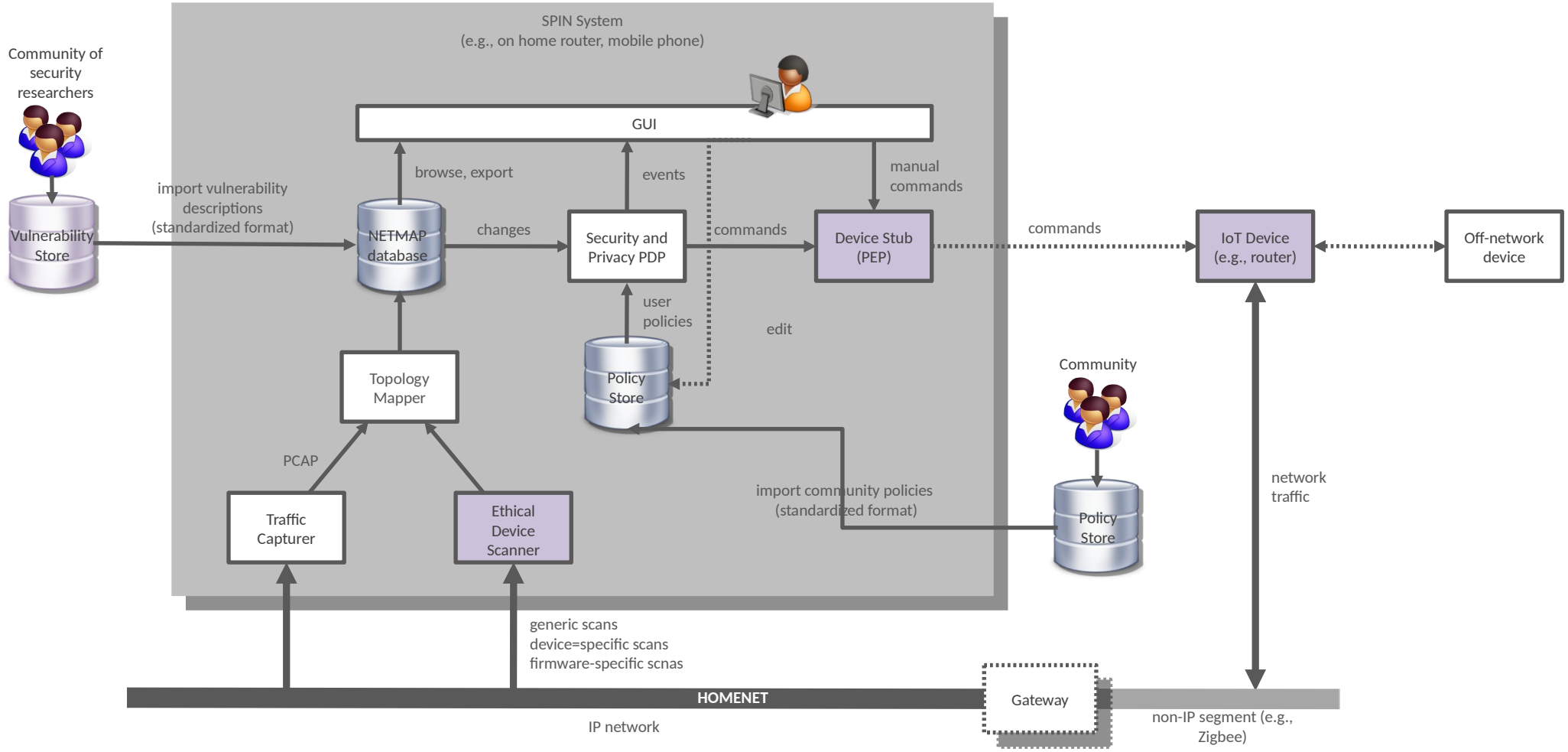
SIDN LABS

The SPIN concept

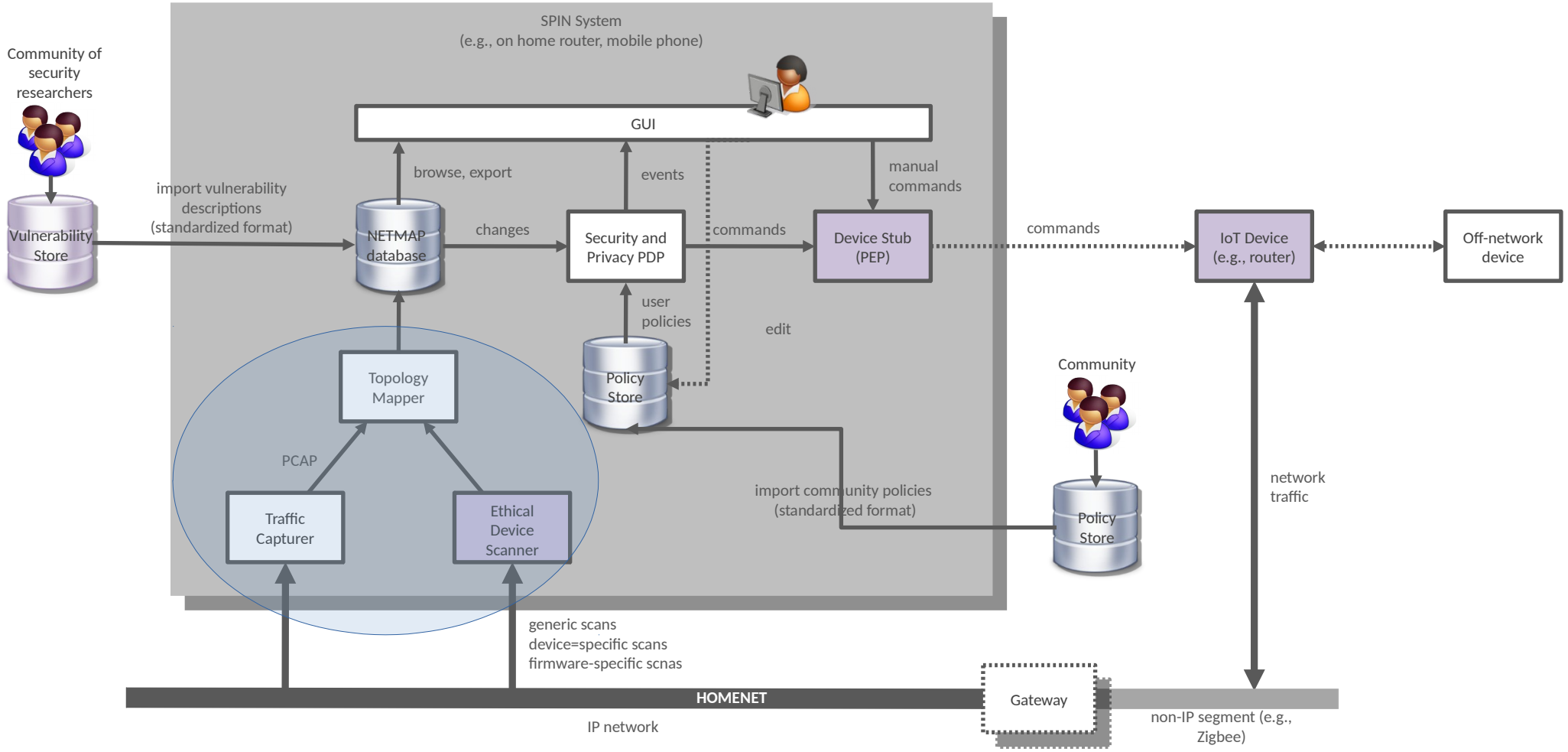
- SPIN controller
  - Visualises traffic
  - Controls traffic
- Processing done locally
  - User in control
  - But largely automated



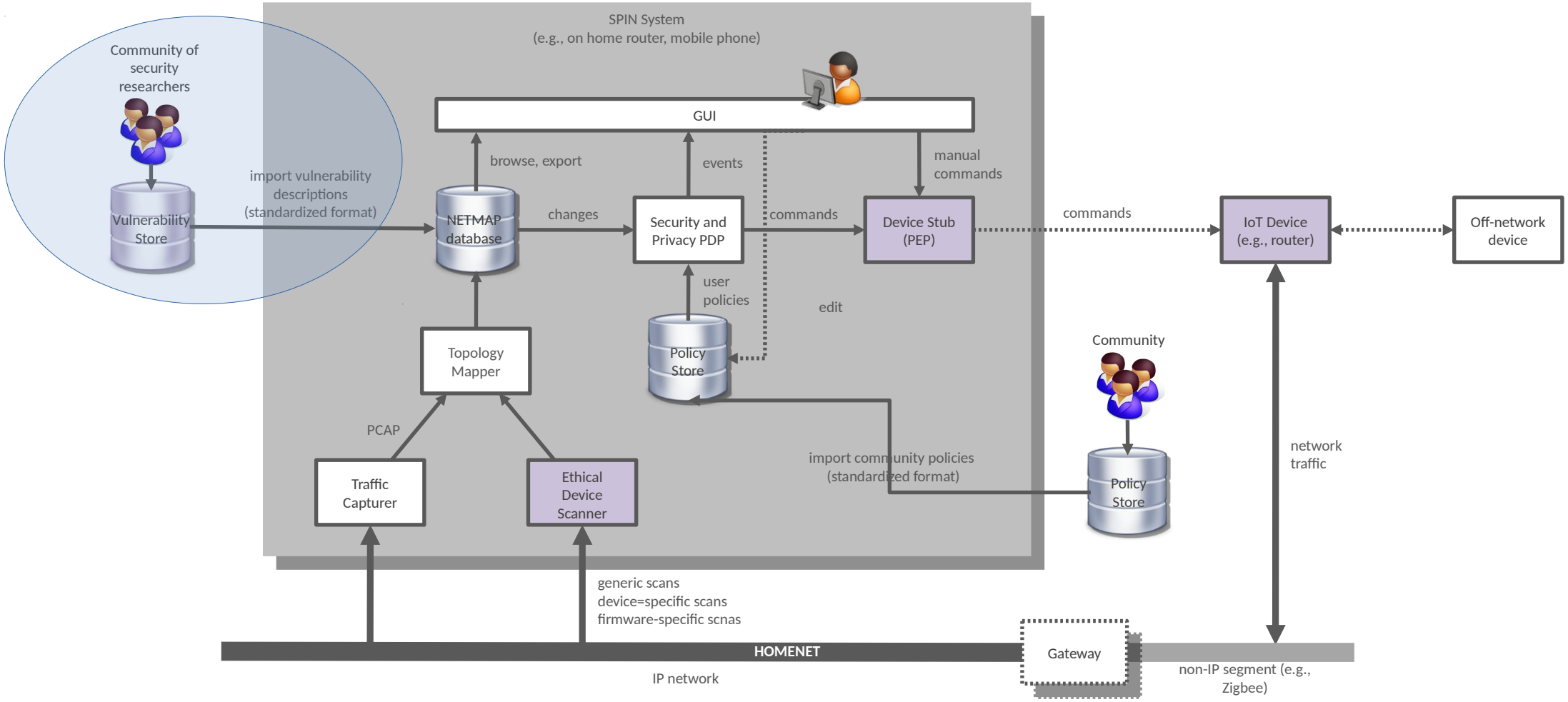
The SPIN architecture



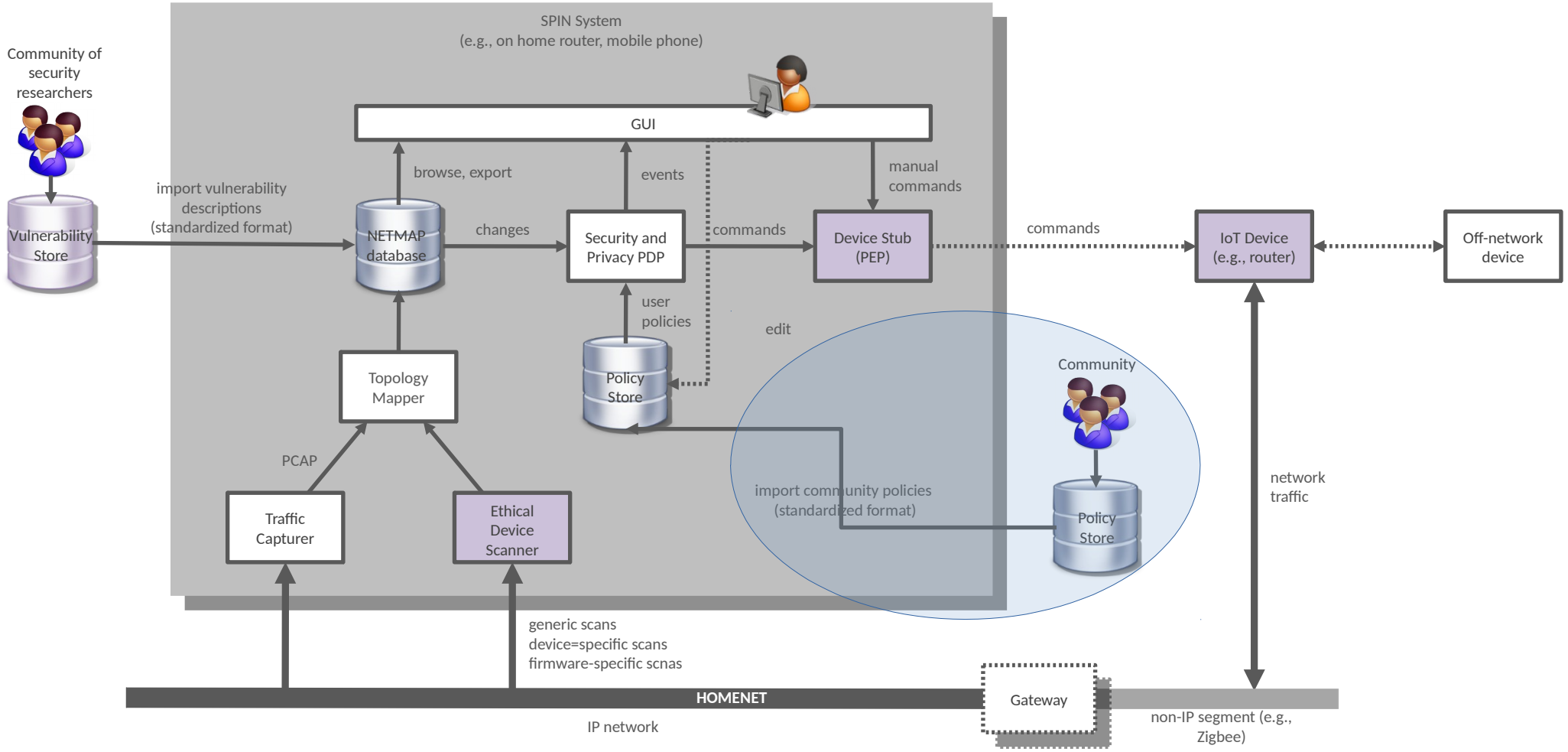
The SPIN architecture



The SPIN architecture

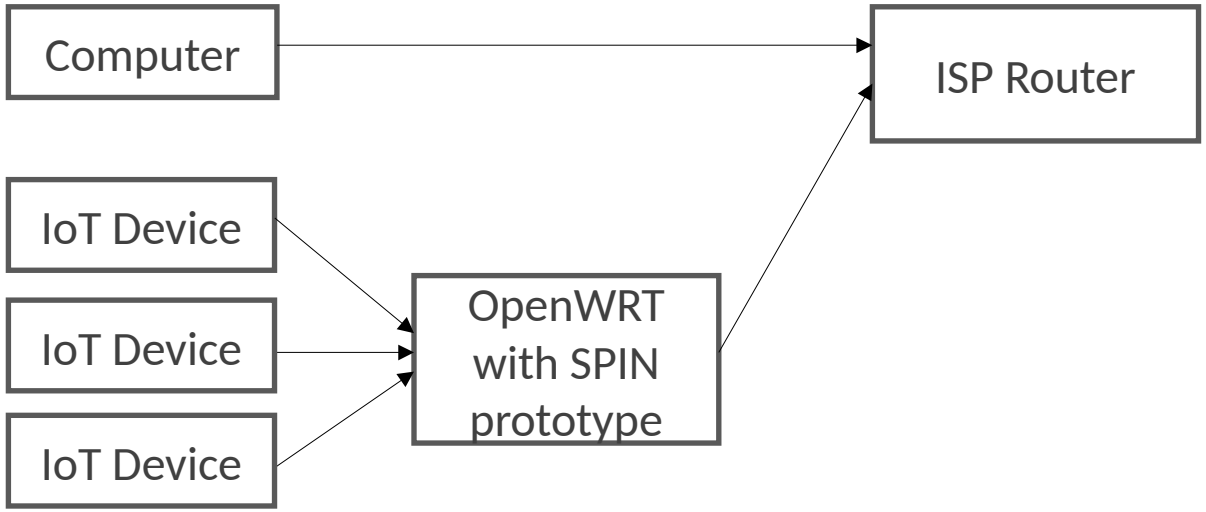


The SPIN architecture



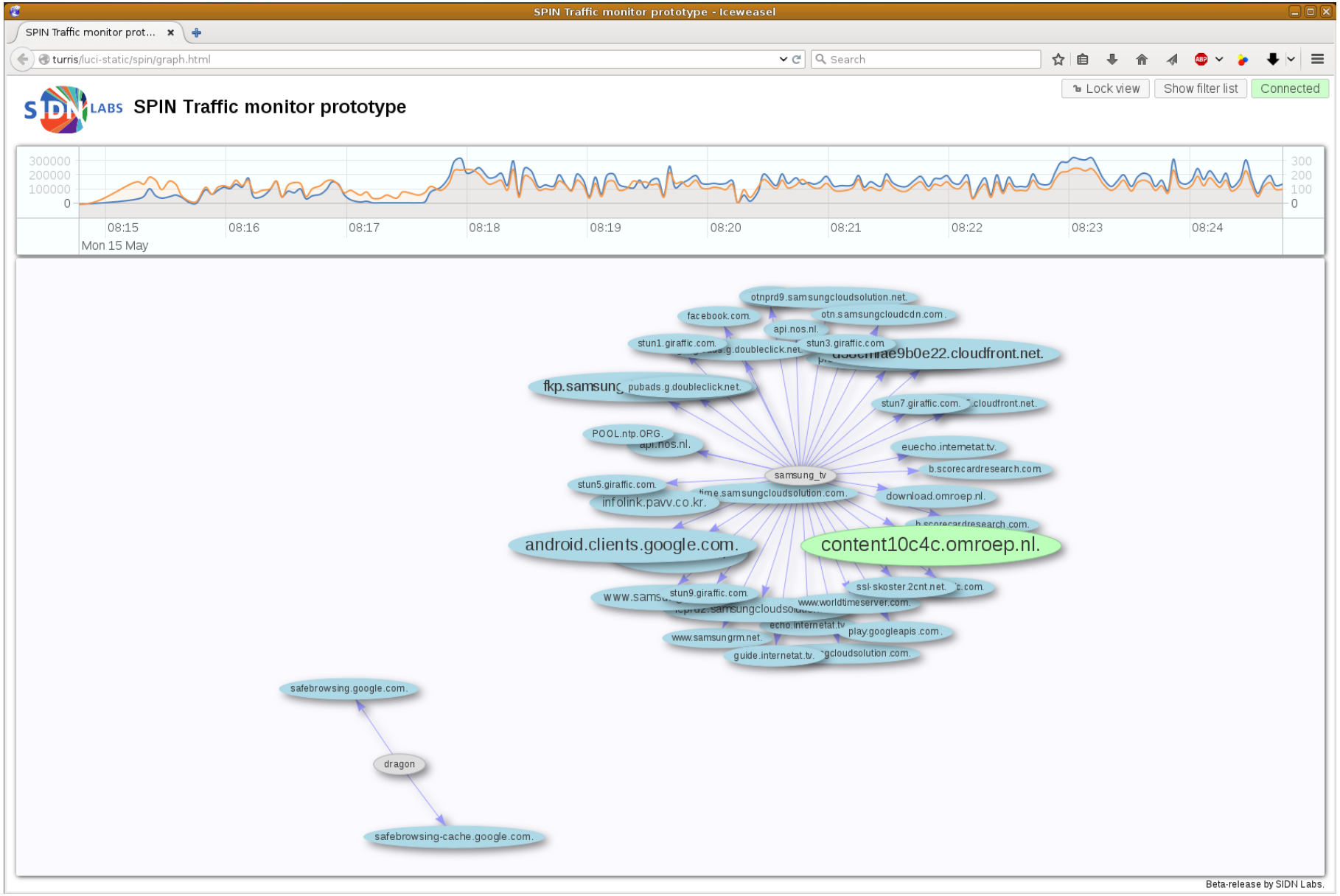
Prototype built on OpenWRT

- Currently bundled with our open source
  - ‘Valibox’ software
- Working on separate OpenWRT package feed



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.
stun3.giraffic.com
fkp.samsung
pubads.g.doubleclick.net.
stun7.giraffic.com.
POOL.ntp.ORG.
euecho.internetat.tv.
b.scorecardresearch.com
samsung_tv
stun5.giraffic.com.
infolink.pavv.co.kr.
download.omroep.nl.
android.clients.google.com.
content10c4c.omroep.nl.
ssl-skoster.2cnt.net.
stun9.giraffic.com.
www.worldtimeserver.com.
echo.internetat.tv
play.googleapis.com.
www.samsungrm.net.
guide.internetat.tv.
safebrowsing.google.com.
dragon
safebrowsing-cache.google.com.
Beta-release by SIDN Labs.

Demo video

Status

- Running prototype on our Valibox (OpenWRT) platform
  - ‘vertical slice’ of the concept
  - Visualise basic traffic with DNS names if known
  - Block traffic to/from devices or external points
- Incremental updates deployed as features are implemented
- Open source: https://github.com/SIDN/spin
- (GL-inet images at: https://valibox.sidnlabs.nl)

SIDN LABS

Deployment

- Get it into deployed devices?
- Maybe even standard home routers at ISPs?
- Free software, go get it ;)

SDN LABS

Future Research

- Set up 'IoT lab' with IoT devices
- Research visualisation/control
- (Collaborate on) a platform for sharing IoT device information?
  - Research into device scanning
  - Repositories for known bad devices/versions?
  - (would that be good or bad?)
  - Trusted traffic profiles?
  - "My TV should stream the news and Netflix, but do nothing else"
- Interested in collaboration? Come talk!

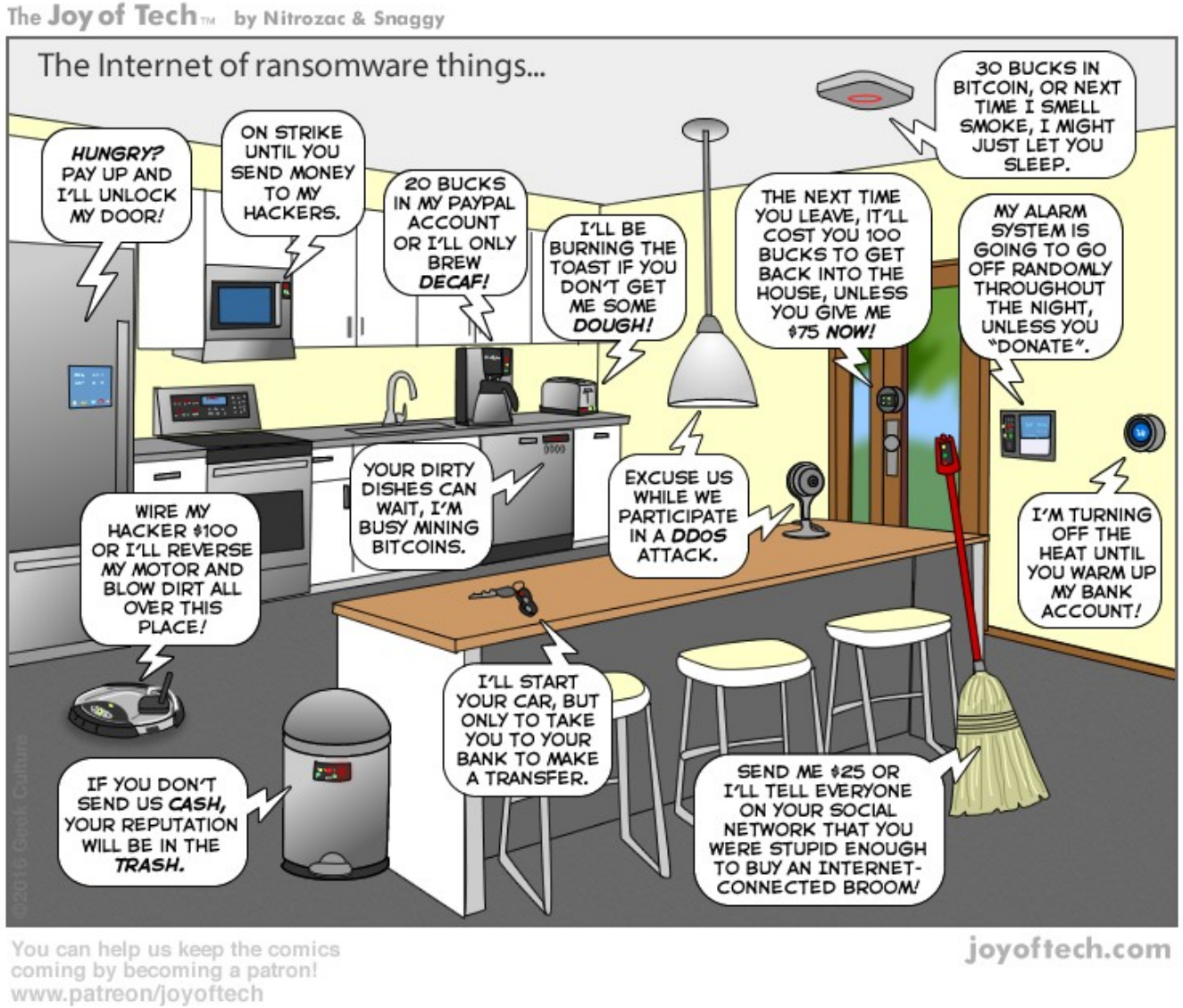
SIDN LABS

Potential SPIN Business Roles

- Quarantine support provider (similar to ISP abuse desk)
- Security and privacy intel provider using anonymized info from homenets (opt-in, of course)
- Privacy profile developers for IoT devices
- IoT security and privacy testing/certification facility
- “SPIN Consortium”: open public-private-user alliance to define protocols, data formats, APIs

SDN LABS

Questions/ideas/suggestions?



@twitjeb