

Security and Privacy in the Internet of Things

Jelte Jansen | SIDN Connect

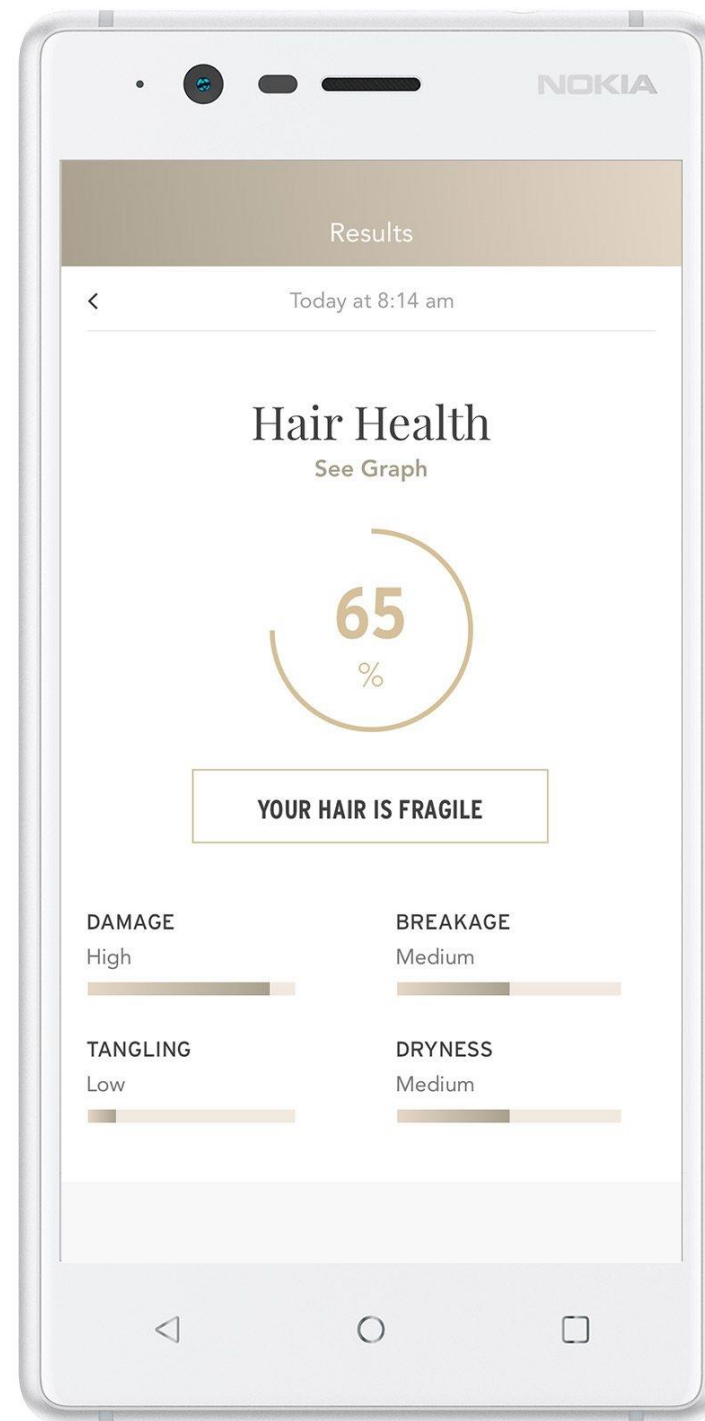
30 november 2017



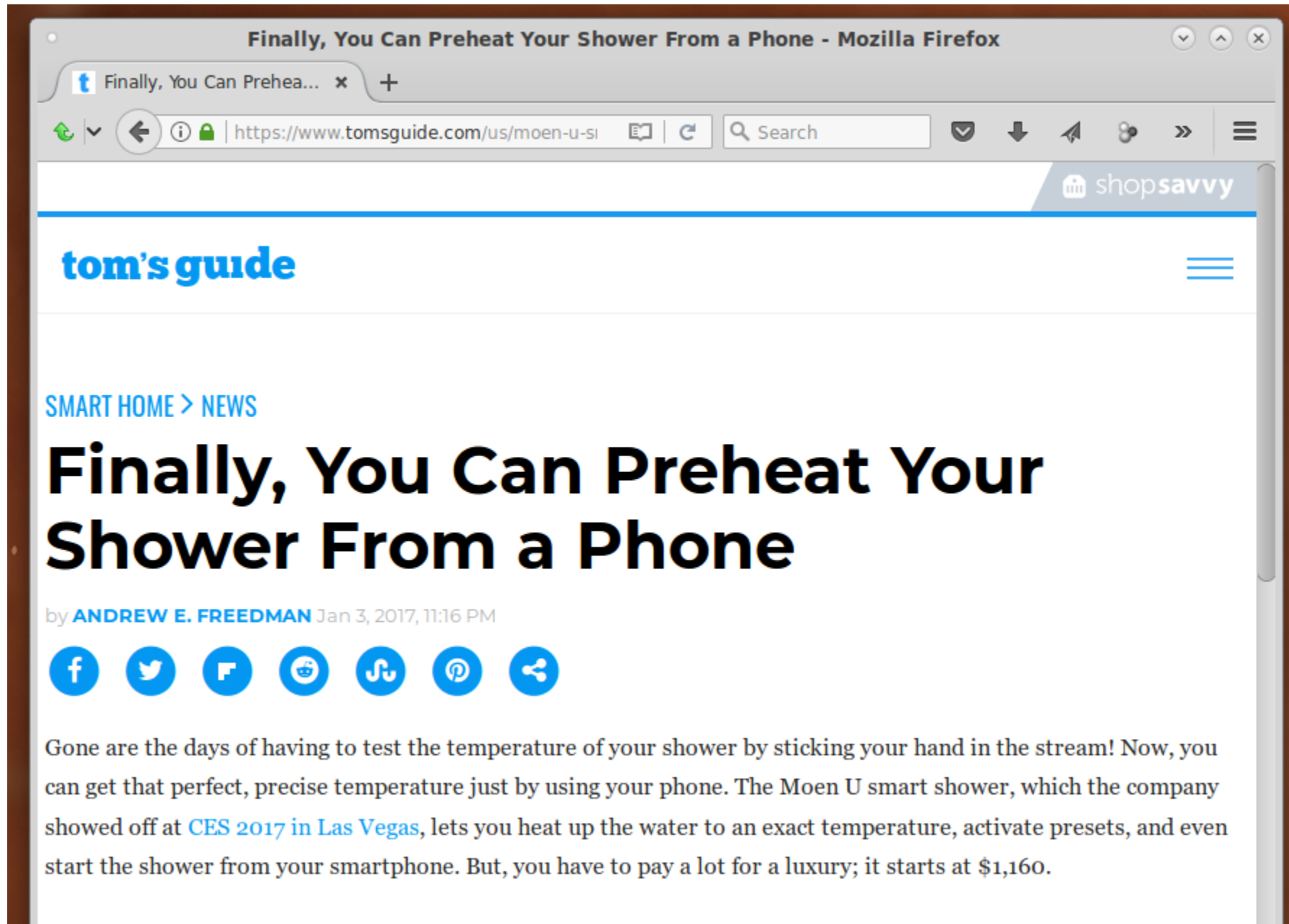
Smart Devices

“A smart device is an electronic device, [snip], that can operate to some extent interactively and autonomously.”

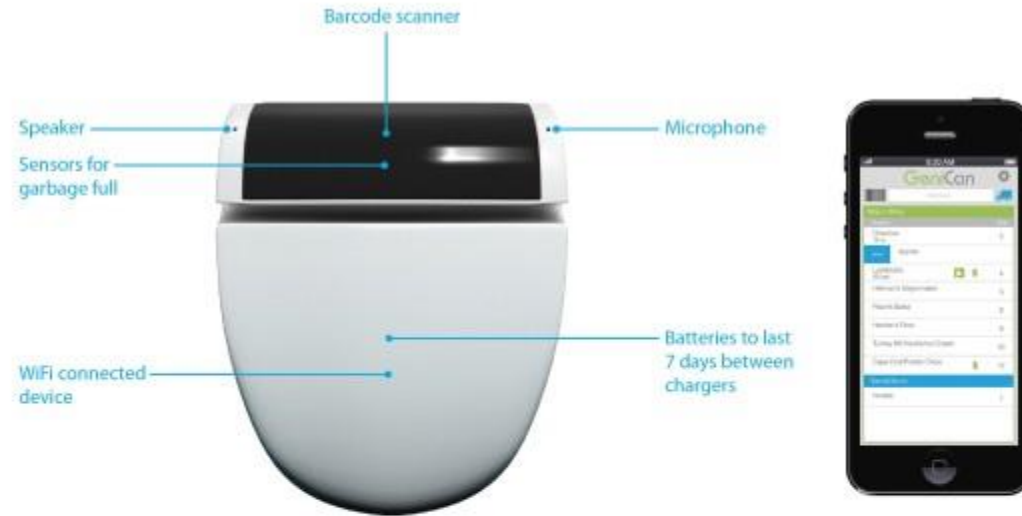
Source: Wikipedia











This is GeniCan.





Measures:

- * How long it took to eat your meal.
- * The amount of "fork servings" taken per minute.
- * Intervals between "fork servings".

This information is then uploaded via USB or Bluetooth to your Online Dashboard

Como Huggies TweetPee funciona

Design ergonômico

O design busca o conforto e segurança do bebê. Fácil de instalar e retirar para utilizar na próxima fralda.



O sensor da fralda monitora a umidade e envia um sinal quando o bebê faz xixi.



Todos que têm a permissão para acompanhar a atividade do bebê são notificados.



Através do APP mães e pais conseguem comprar fraldas sem sair de casa.



Pelo histórico de troca de fraldas do bebê, você acompanha a quantidade usada por dia.







With “Waistline Trend Analysis”!





What does i.Con do with its data? Can I use it anonymously?

Absolutely! All data will be kept anonymous but users will have the option to share their recent data with friends, or, indeed the world. You will be able to anonymously access stats that you can compare with i.Con users worldwide.

These Flip Flops Are 'Smart' for the Dumbest Possible Reason



Christina Warren

3/28/17 5:58pm • Filed to: WHO NEEDS THIS? ▾



28.3K



17



2



Image: Hari Mari





Bring the flavor

SMALT dispenses salt with
a shake/pinch of your
smartphone screen



Bring the flavor

SMALT dispenses salt with a shake/pinch of your smartphone screen or simply turning the dial manually.



SMALT with voice

Connect SMALT with Amazon Echo and simply say "Alexa, dispense half a teaspoon of salt".

8.4 Billion

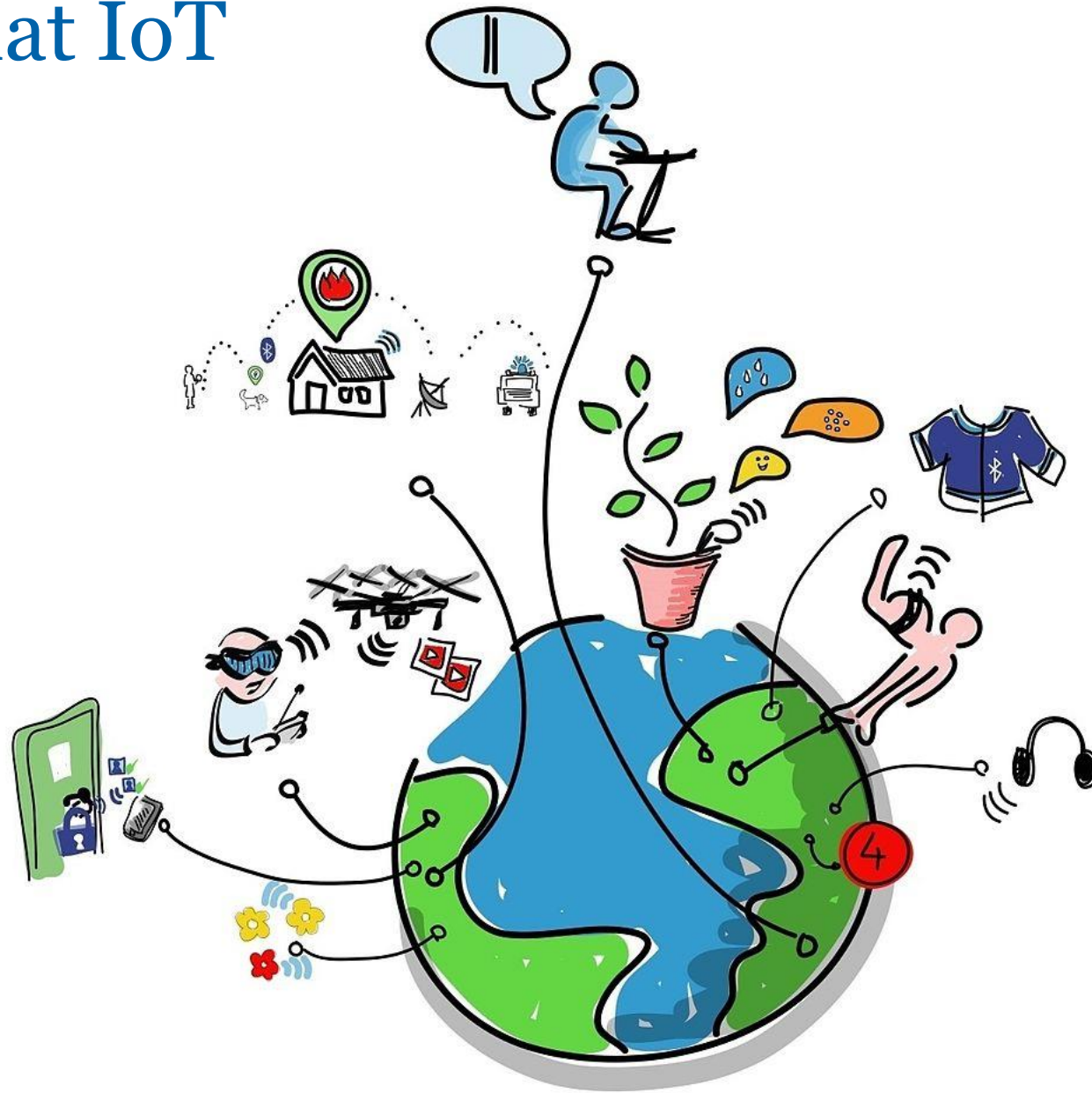
Devices connected to the Internet in 2017

Source: Gartner (January 2017)

20 Billion
in 2020



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 did not use to be networked”

What **is** the IoT?

An even simpler definition:

“One big mess”



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



The "S" in IoT
stands for
SECURITY



Attributed to @tkadlec



The S in IoT

- 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

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

The effects of lack of security

threat **post** CATEGORIES FEATURED PODCASTS VIDEOS

Twitter Facebook Google+ LinkedIn YouTube RSS

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



NEW MIRAI VARIANT CARRIES OUT 54-HOUR DDOS ATTACKS

by **Tom Spring** March 30, 2017 , 2:50 pm

The 2016 Dyn attack



1.2 Tbps

From 'only' 100.000 devices

The 2016 Dyn attack

Affected services [\[edit \]](#)

Services affected by the attack included:

- Airbnb^[11]
- Amazon.com^[8]
- Ancestry.com^{[12][13]}
- *The A.V. Club*^[14]
- BBC^[13]
- *The Boston Globe*^[11]
- Box^[15]
- *Business Insider*^[13]
- CNN^[13]
- Comcast^[16]
- CrunchBase^[13]
- DirecTV^[13]
- *The Elder Scrolls Online*^{[13][17]}
- Electronic Arts^[16]
- Etsy^{[11][18]}
- FiveThirtyEight^[13]
- Fox News^[19]
- *The Guardian*^[19]
- GitHub^{[11][16]}
- Grubhub^[20]
- HBO^[13]
- Heroku^[21]
- HostGator^[13]
- iHeartRadio^{[12][22]}
- Imgur^[23]
- Indiegogo^[12]
- Mashable^[24]
- National Hockey League^[13]
- Netflix^{[13][19]}
- *The New York Times*^{[11][16]}
- Overstock.com^[13]
- PayPal^[18]
- Pinterest^{[16][18]}
- Pixlr^[13]
- PlayStation Network^[16]
- Qualtrics^[12]
- Quora^[13]
- Reddit^{[12][16][18]}
- Roblox^[25]
- Ruby Lane^[13]
- *RuneScape*^[12]
- SaneBox^[21]
- Seamless^[23]
- *Second Life*^[26]
- Shopify^[11]
- Slack^[23]
- SoundCloud^{[11][18]}
- Squarespace^[13]
- Spotify^{[12][16][18]}
- Starbucks^{[12][22]}
- Storify^[15]
- Swedish Civil Contingencies Agency^[27]
- Swedish Government^[27]
- Tumblr^{[12][16]}
- Twilio^{[12][13]}
- Twitter^{[11][12][16][18]}
- Verizon Communications^[16]
- Visa^[28]
- Vox Media^[29]
- Walgreens^[13]
- *The Wall Street Journal*^[19]
- Wikia^[12]
- *Wired*^[15]
- Wix.com^[30]
- WWE Network^[31]
- Xbox Live^[32]
- Yammer^[23]
- Yelp^[13]
- Zillow^[13]

Some ways to protect against DDoS

- Overprovision
- Hide behind 'protection service'
- Install big packet scrubbers
- Work closely with networking peers to blackhole attack data

But what about **preventing** DDoS?

- “Let market fix it”



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

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](#) [SIGN IN](#)


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



DN LABS

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...

What should we do?

- Better practices for manufacturers?
- Free **secure** software stacks?
- International policy, regulation, certification?
- Clear up accountability issues?
- Generate market demand for secure products?
- Quarantine bad actors (e.g. at ISP)?
- Educate users?
- Empower users?

“Yes”

We need to do it all

Focus on one today:

Protect home networks

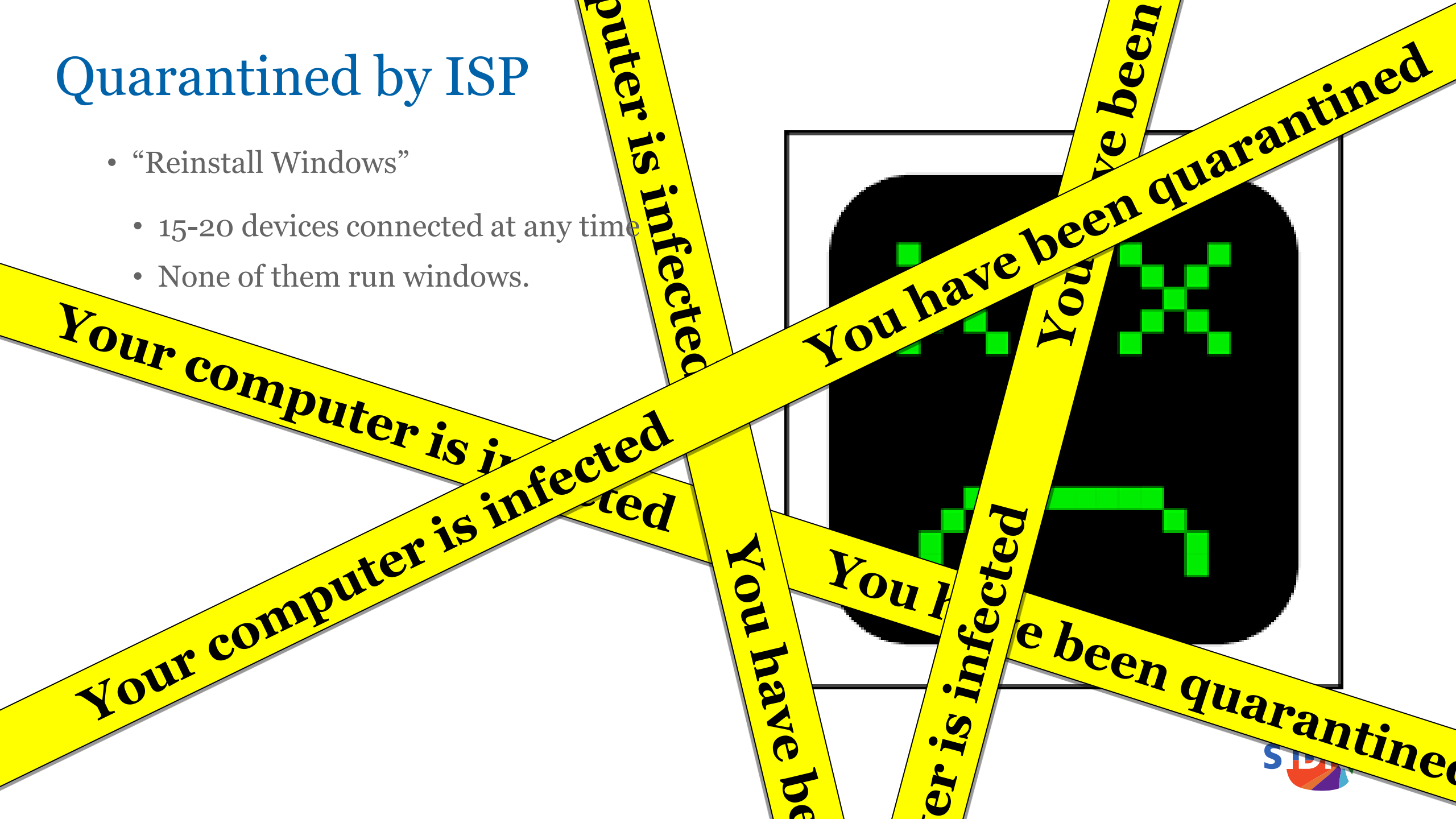
How to protect home networks?

- Home networks notoriously insecure
- Many different devices and device types
- There will always be bad devices and computers



Quarantined by ISP

- “Reinstall Windows”
- 15-20 devices connected at any time
- None of them run windows.



How to protect home networks?

- Lowest common denominator: IP
- So, firewall?
- We need something better

```
jelte@dragon: /home/jelte
wired = "em1"
wifi = "athn0"
table <martians> { 0.0.0.0/8 10.0.0.0/8 127.0.0.0/8 169.254.0.0/16 \
                  172.16.0.0/12 192.0.0.0/24 192.0.2.0/24 224.0.0.0/3 \
                  192.168.0.0/16 198.18.0.0/15 198.51.100.0/24 \
                  203.0.113.0/24 }

set block-policy drop
set loginterface egress
set skip on lo0
match in all scrub (no-df random-id max-mss 1440)
match out on egress inet from !(egress:network) to any nat-to (egress:0)
antispoof quick for { egress $wired $wifi }
block in quick on egress from <martians> to any
block return out quick on egress from any to <martians>
block all
pass out quick inet
pass in on { $wired $wifi } inet
pass in on egress inet proto tcp from any to (egress) port { 80 443 } rdr-to 192.168.1.2

~
~
~
~
~

1,1 All
```


The Dream

A surreal landscape with a girl in a blue dress looking at a whale carrying a castle. The scene is set against a backdrop of a sunset sky with soft orange and pink hues. In the foreground, a girl with long blonde hair, wearing a blue dress with white trim, stands on a grassy hill, looking up at a large, grey whale. The whale is floating in the sky, and on its back sits a large, ornate castle with multiple towers and spires. The whale's tail is visible, and it appears to be swimming through the clouds. The overall atmosphere is dreamlike and fantastical.

Open home security platform: open source, open standards

Automatic operation: guards and automatically blocks devices

Privacy friendly: runs locally, does not process application-level data

User-centric: automatic, but allow for 'power-use'

Enables new business models: network-level system w/ well-defined APIs

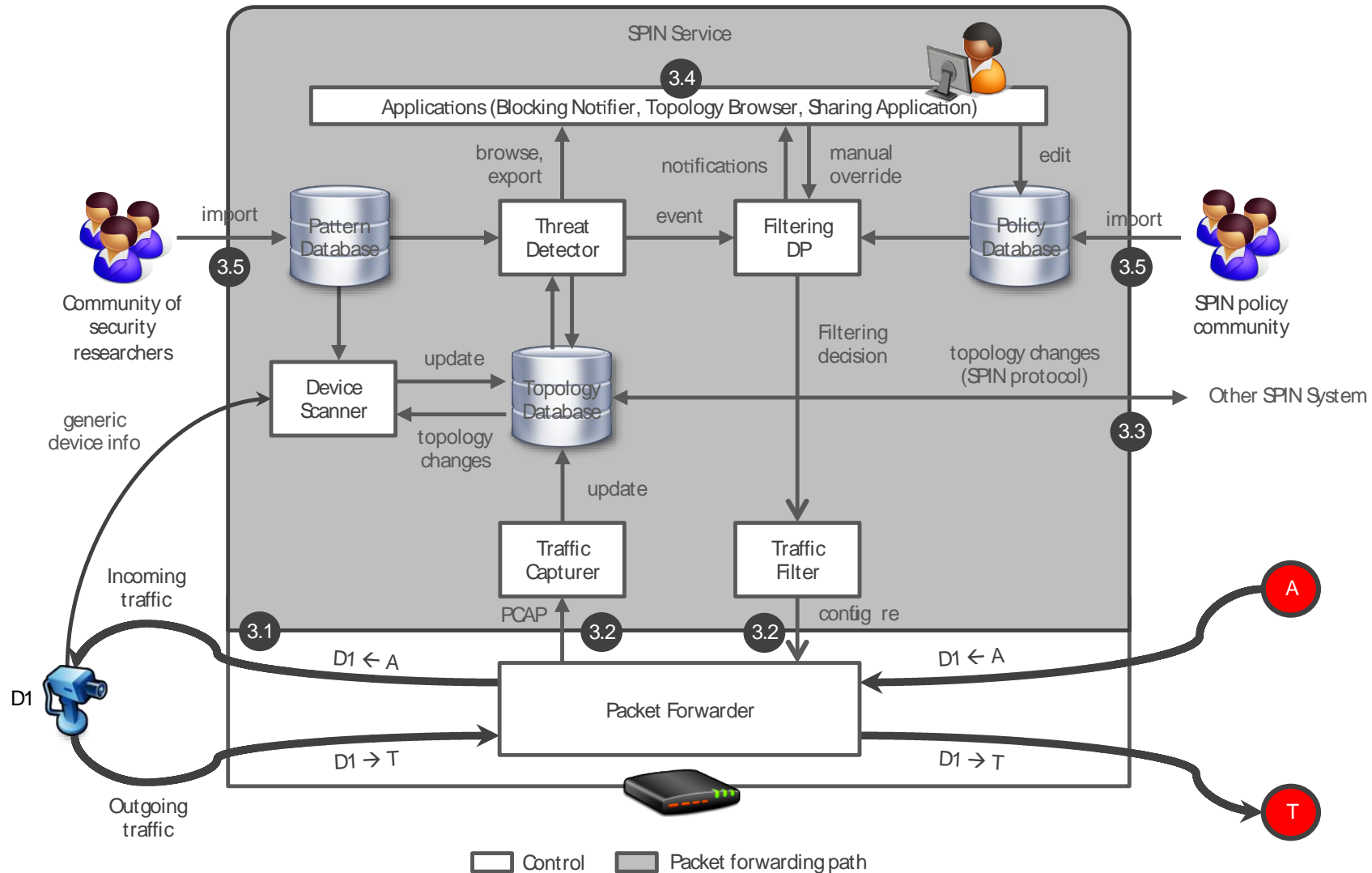
The SPIN project at SIDN Labs

- Security and Privacy for In-home Networks
- Research and prototype SPIN functions:
 - Visualise network traffic
 - Automatically block unwanted traffic/infected devices
 - Allow 'good' traffic
 - Scan devices
 - Sharing platform for device info

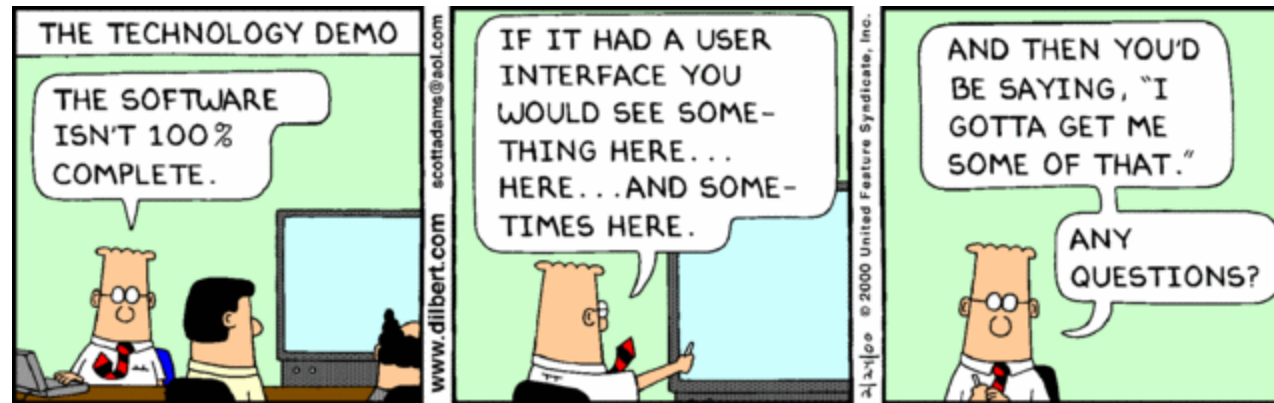
The SPIN project at SIDN Labs

- Open source in-home router/AP software that
 - Helps protecting DNS operators (like SIDN!) and other service providers from IoT-powered DDoS attacks
 - Helps end-users control their security and privacy in the IoT
 - All processing done locally, no VPN, no enforced cloud

High-level view

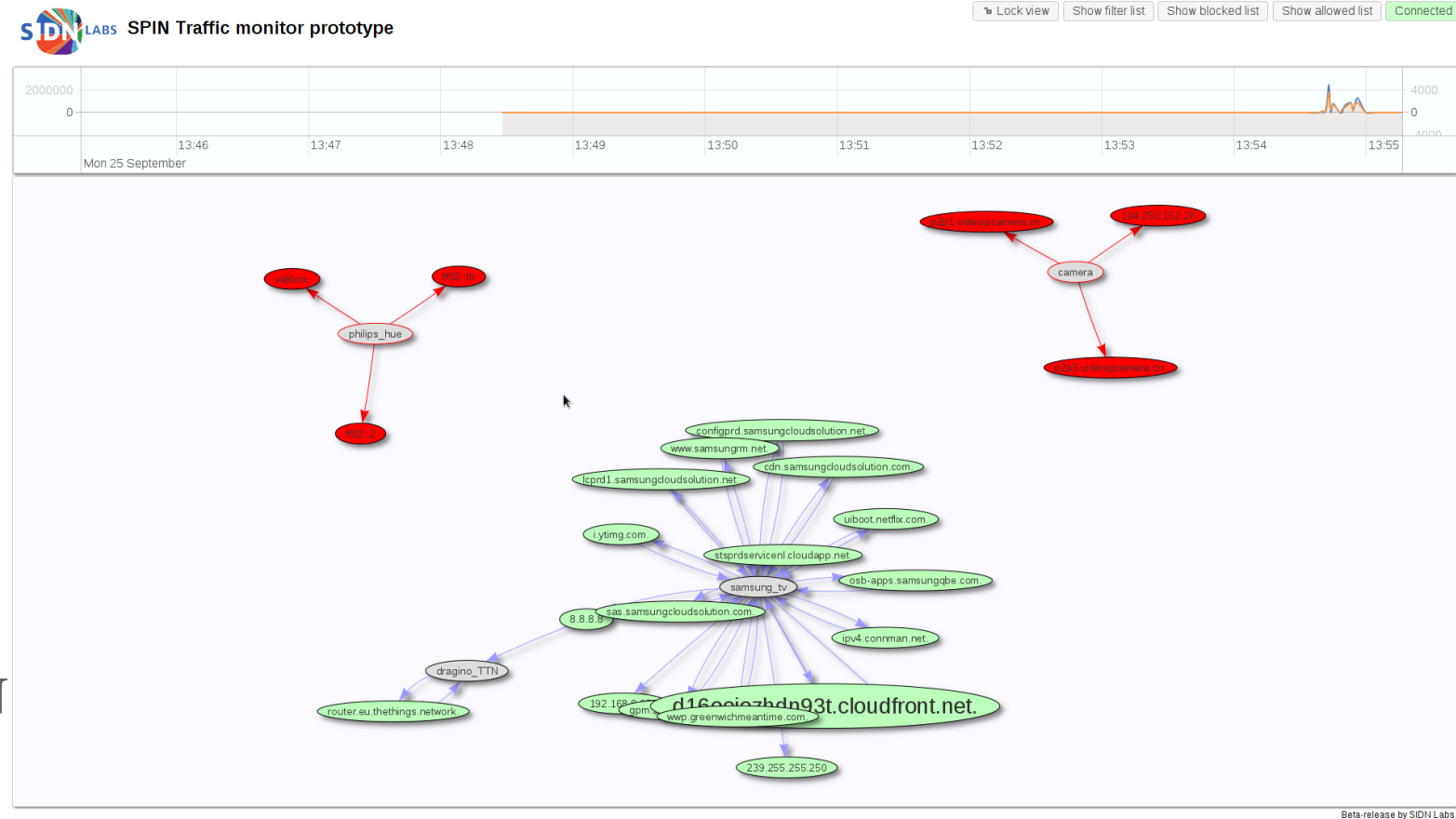


Demo!



Status

- Running prototype
 - ‘Vertical slice’ of the concept
 - Visualises basic traffic
 - Blocks specified traffic
- Open source:
<https://github.com/SIDN/SPIN>
- Full (GL-Inet) images at
<https://valibox.sidnlabs.nl>



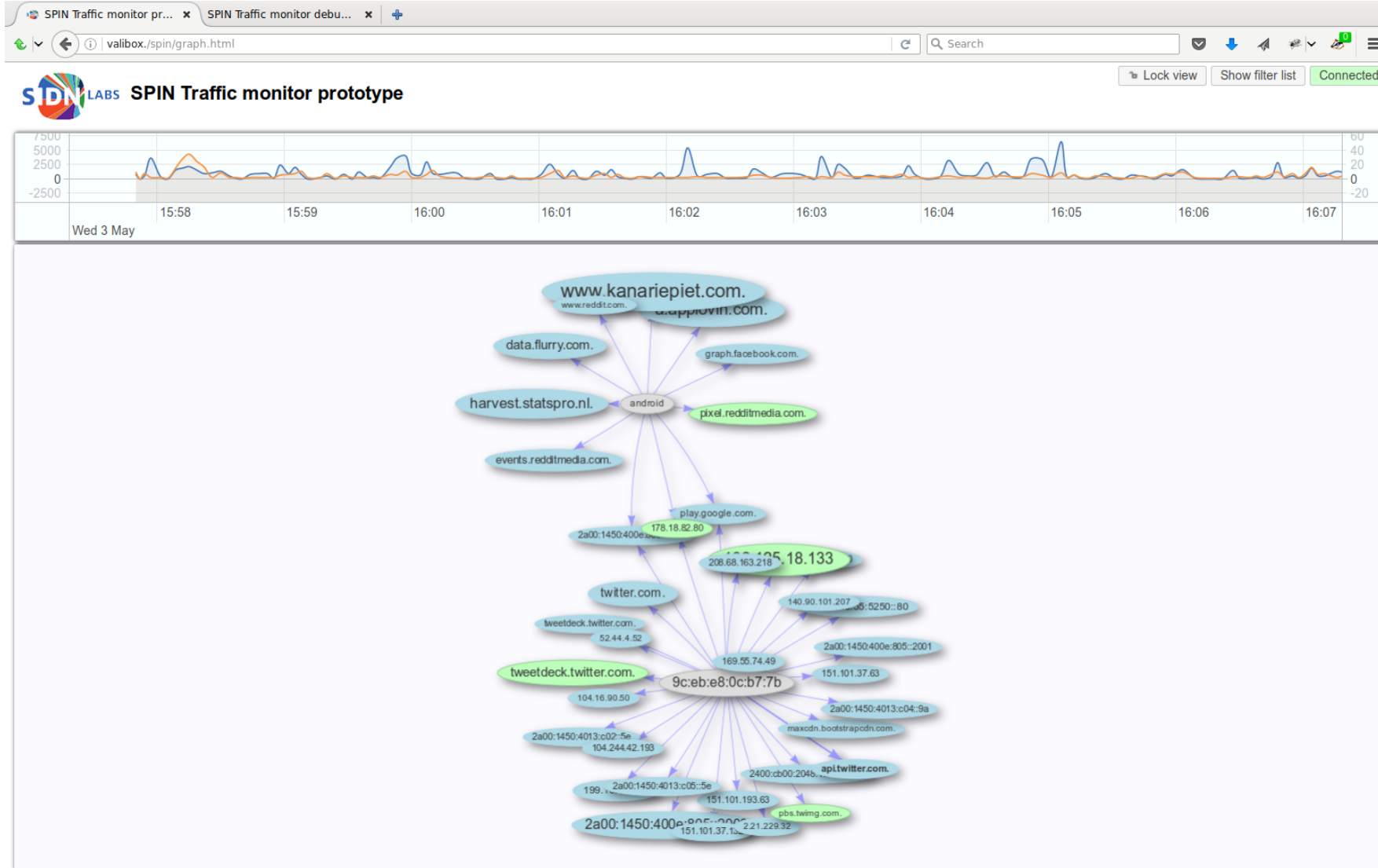
Current high-level topics of interest

- Standardization
- Pilot for large scale evaluation
- Business models based on SPIN platform
- SPIN as a platform for IoT research projects

Deployment

- We cannot do this alone!
- Get it into deployed devices?
- Maybe even standard home routers at ISPs?
- Free software, go get it ;)

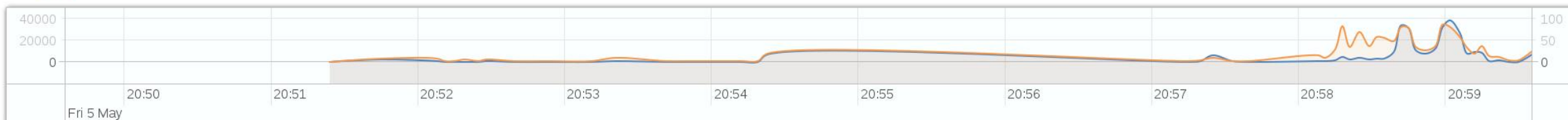
Visualiser



Beta-release by SIDN Labs.



SPIN Traffic monitor prototype



facebook.com.

Ignore this node

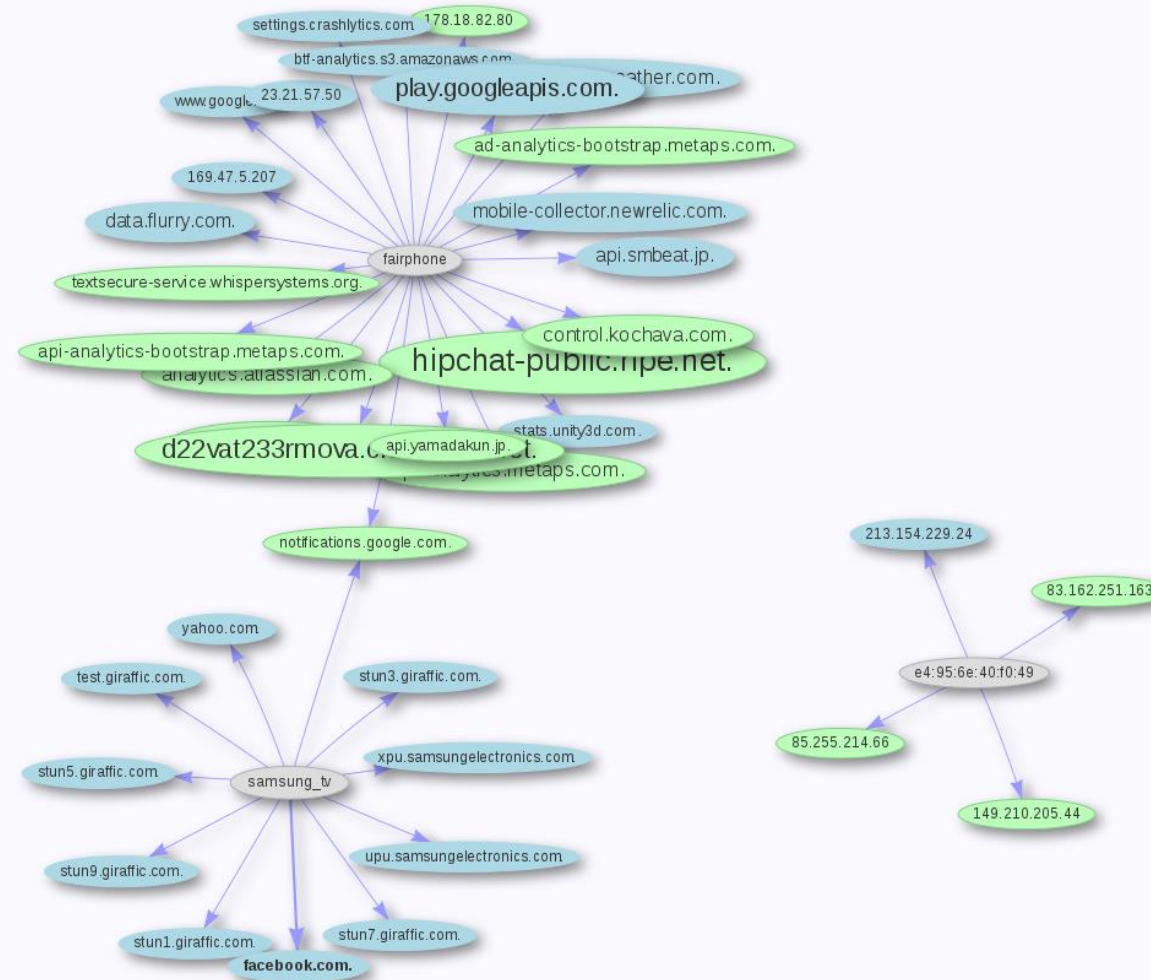
Rename this node

Block node

Node: 61
Connections seen: 5
Traffic size: 268
Last seen: Fri May 05 2017
20:58:11 GMT+0200 (CEST)
IP: 157.240.3.35
DNS: facebook.com.

94.198.152.74

iphone



Questions/ideas/suggestions?

