

# The IoT and the DNS

**Jelte Jansen (SIDN)**

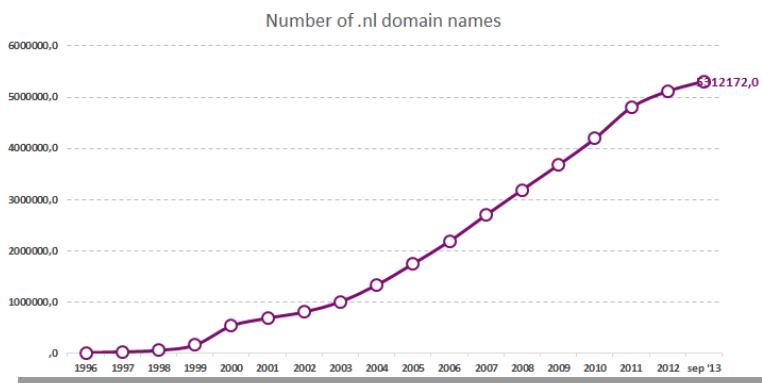
ETNO wg meeting

Wed Feb 19, 2020



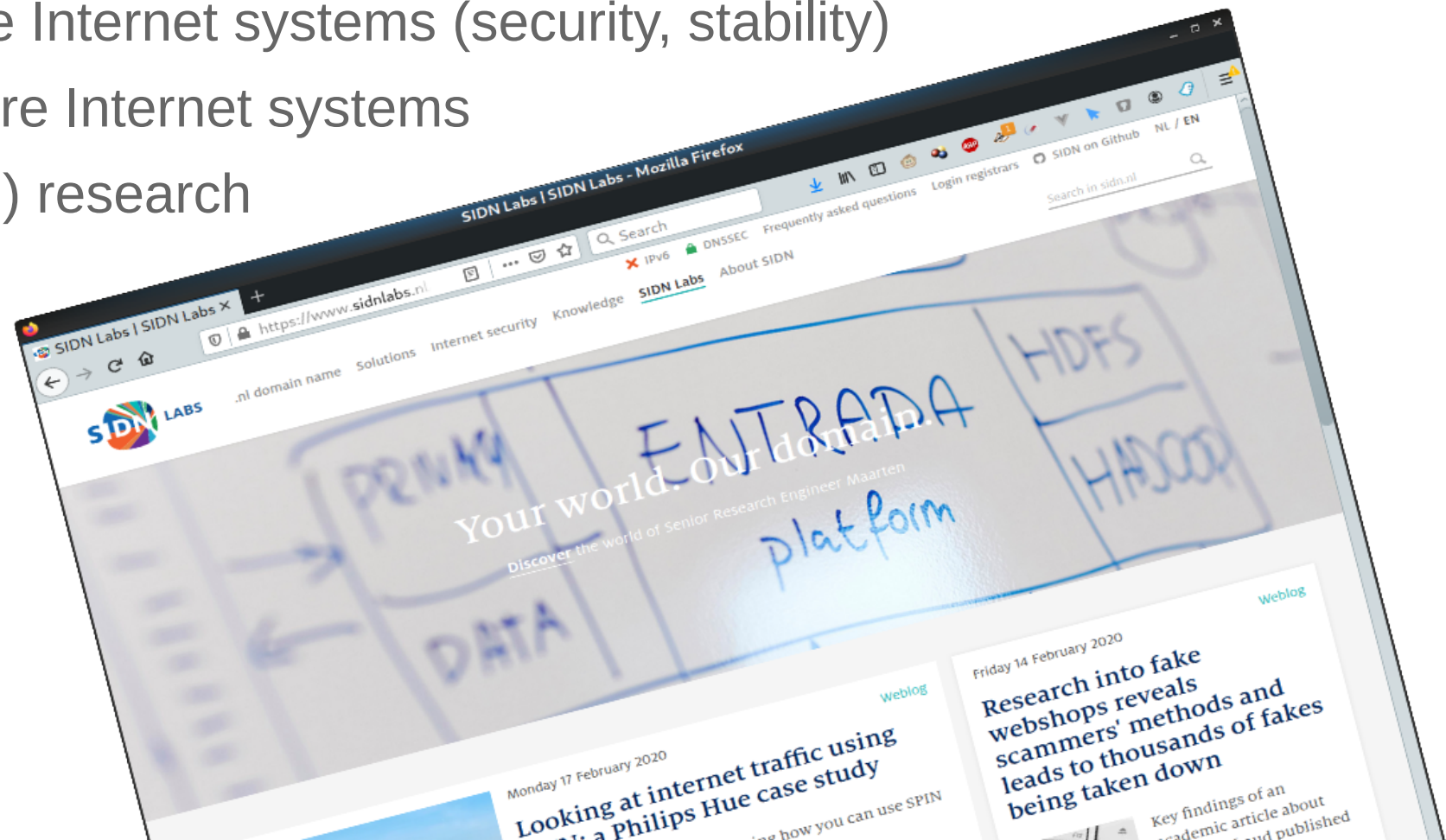
# Introduction: Me & SIDN

- Research Engineer at SIDN
- Domain name registry for the .nl ccTLD
- 5.9 million domain names
- 3.2 million domain names signed with DNSSEC



# Introduction: SIDN Labs

- <https://www.sidnlabs.nl/en/about-sidnlabs>
- R&D team of SIDN
- Research into core Internet systems (security, stability)
- Research into future Internet systems
- Facilitate (external) research



# So, about that IoT



# 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



# So, about that IoT

threat **post**

CATEGORIES

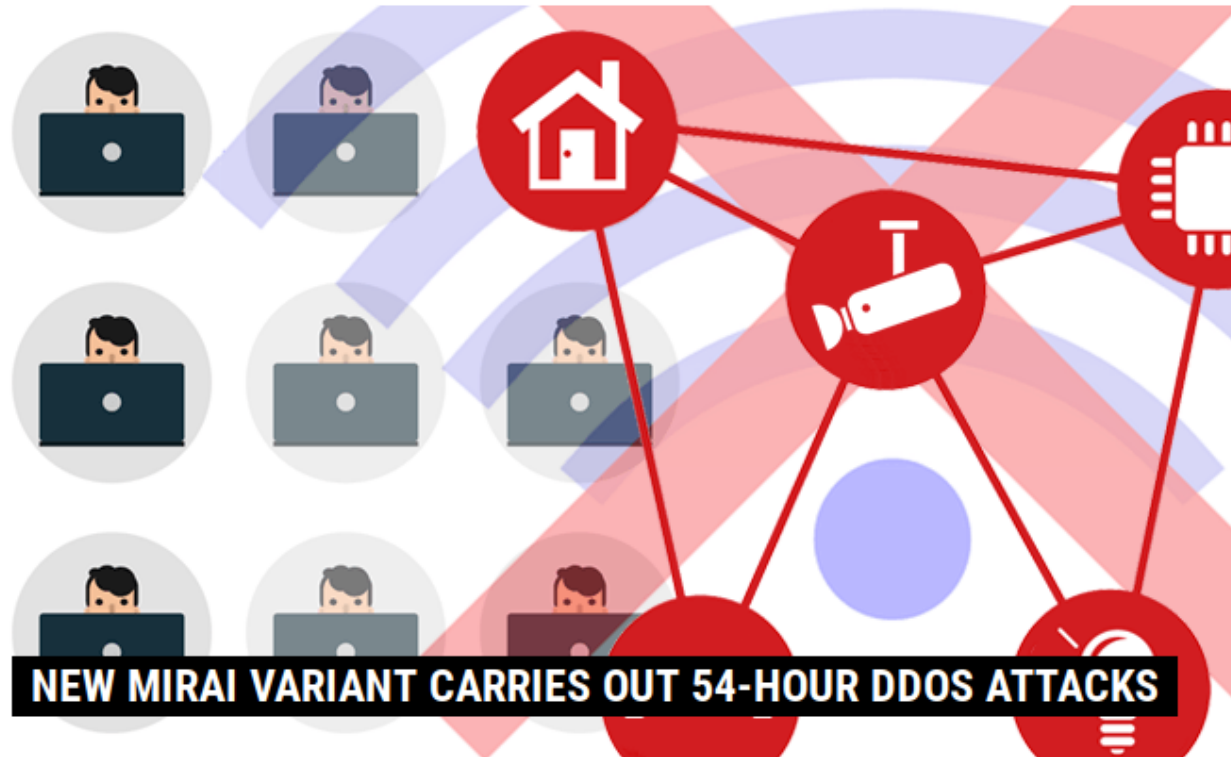
FEATURED

PODCASTS

VIDEOS



[Welcome](#) > [Blog Home](#) > [Hacks](#) > [New Mirai Variant Carries Out 54-Hour DDoS Attacks](#)



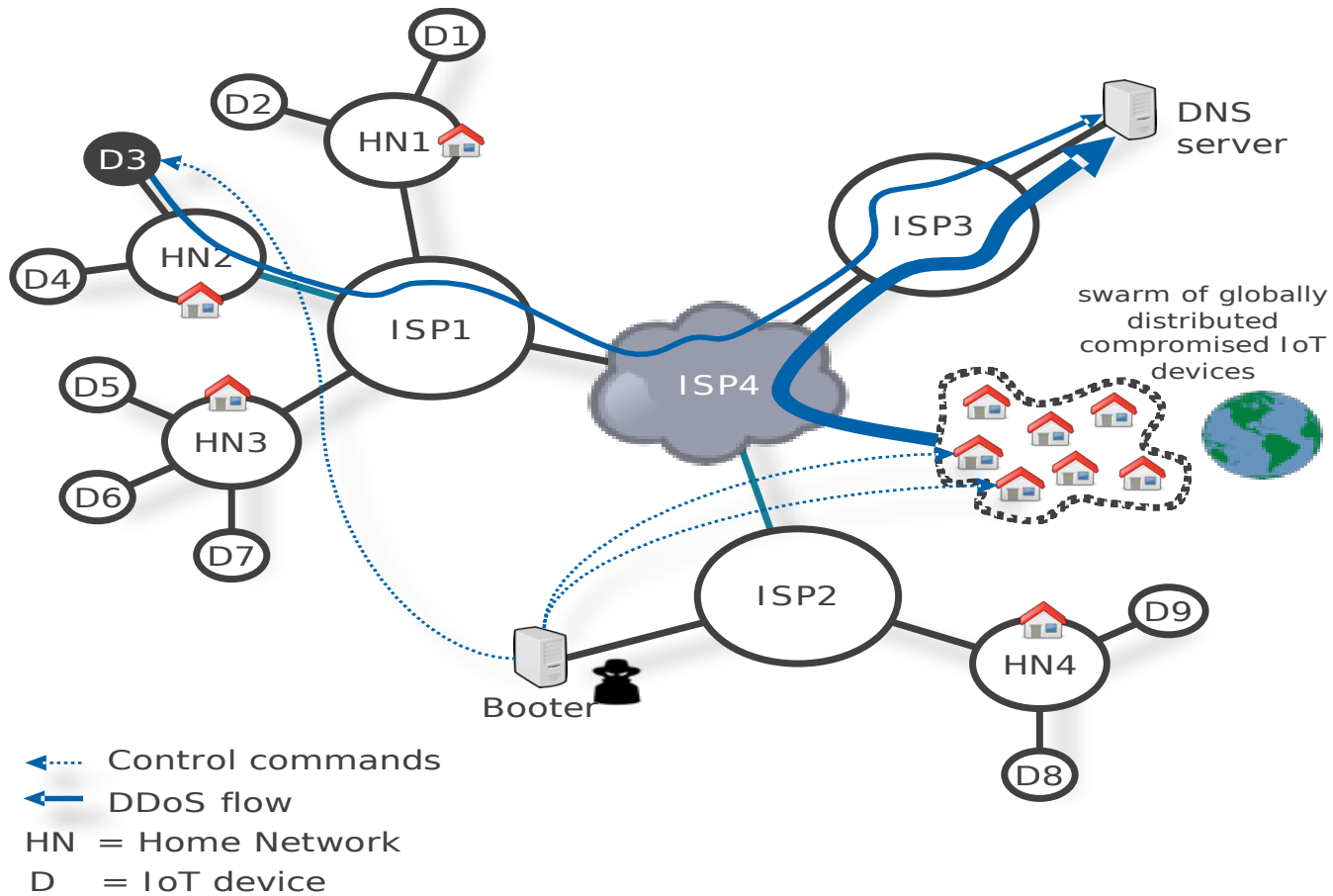
by [Tom Spring](#)

March 30, 2017 , 2:50 pm





# IoT wakeup call for ccTLDs and other operators: Mirai-powered DDoS attacks



Other targets: OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

Sources:  
 [Mirai17], [Hajime19], [SAC105]  
[https://en.wikipedia.org/wiki/2016\\_Dyn\\_cyberattack](https://en.wikipedia.org/wiki/2016_Dyn_cyberattack)  
<https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/>





# What should we (the world) 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?

# What should we (the world) 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”

# What should we (the world) 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

**ICANN Security and Stability Advisory board publication:**

**The DNS and the Internet of Things: Opportunities,  
Risks, and Challenges (SAC105)**

<https://www.icann.org/en/system/files/files/sac-105-en.pdf>



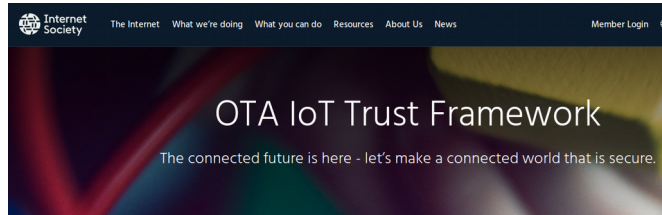
# Excerpt from SAC105: issues

- DNS-unfriendly programming at IoT scale
  - TuneIn app example: 700 iPhones generating random queries filled resolver cache of mobile operator, took weeks to update
  - Imagine millions of unsupported devices that operate unattended for decades
- Larger and more complex DDoS attacks by IoT botnets
  - IoT botnets currently around 400-600K bots (Mirai, Hajime), may increase in the future
  - Higher propagation rates (e.g., Hajime exploited vulnerability in 10 days and increased by 50K bots in 24 hours)
  - Vulnerabilities more difficult to fix quickly at scale, botnet infections go unnoticed
- DDoS amplification
  - 23-25 million open resolvers
  - Amplification factors in the range 29-64

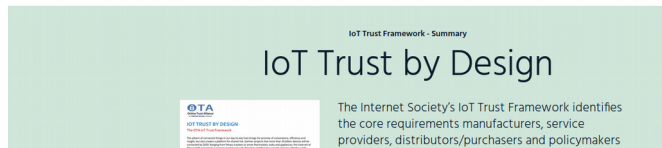
# Excerpt from SAC105: challenges

- Develop a DNS security library for IoT devices
  - Such as DNSSEC validation, DoH/DoT support
  - User control over DNS security settings and services used
- Train IoT and DNS professionals
  - IoT folks: understand IoT botnets, open resolvers, “DNS friendly” programming and security (e.g., DNSSEC)
  - DNS folks: understand IoT changes domain registration model and security
- Collaboratively handle IoT-powered DDoS attacks
  - Share DDoS “fingerprints” across operators
  - DDoS mitigation broker to flexibly share mitigation capacity
  - Security systems in edge networks, such as home routers
- Develop a system to measure the evolution of the IoT
  - Device-to-domain name database
  - DNS operators provide coarse grained stats

# (Other) Initiatives around the world, on many levels



The Internet of Things (IoT) offer consumers, businesses, and governments across the globe countless benefits. As is true with most emerging technology, however, there remain some significant challenges. The Online Trust Alliance (OTA), an Internet Society initiative, believes that through **leadership, innovation, and collaboration**, we can overcome these challenges and create a safer and more trustworthy connected world. This requires a shared responsibility including industry embracing security and privacy by design, and adopting responsible privacy practices.



## OPEN SECURITY KNOWLEDGE

### FOR COMPLETE SOLUTIONS: END-TO-END

The IoT Security Initiative provides comprehensive guidance and tools for ensuring that the right levels of security and privacy are instilled into created and deployed products, systems, and services.

The security controls and guidelines recommended here are based upon an understanding of overall threat and risk to the technology asset, and how this risk can be mitigated in both the direct system and broader solution context.

The IoT Security Initiative provides broad, high-level material - that is at the same time direct, specific and actionable - to practitioners in various roles of solution development, management, IT, and information security.

### AVAILABLE SECURITY GUIDANCE

[Cybersecurity Principles of IoT](#)

[Security Design Best Practices](#)

[Device Security Level Agreement](#)

[Privacy Design Best Practices](#)

[Secure-Me: Digital-OPSEC](#)

\*\* [Product Security Pre-Launch Checklist](#)

\*\* [Cybersecurity Health-Check: Network & Cloud](#)

\*\* [Cybersecurity Health-Check: Product Development](#)

Home • [Blogs en Nieuws](#) • Naar geautomatiseerde DDoS-bescherming met MUD

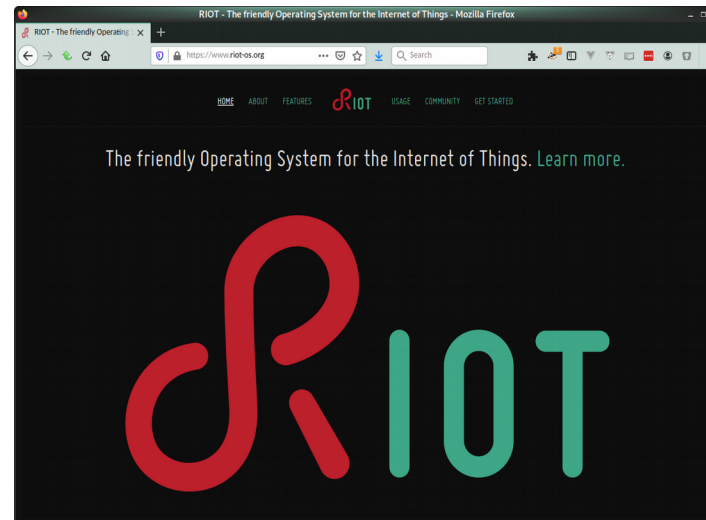
## Naar geautomatiseerde DDoS-bescherming met MUD

Gepubliceerd op: maandag 29 oktober 2018

Onveilige Internet of Things apparaten (IoT-apparaten) worden gebruikt om Distributed Denial of Service (DDoS) aanvallen uit te voeren. Een bekend voorbeeld hiervan is de Mirai-botnet aanval op DNS-operator Dyn, die leidde tot grootschalige uitval van DNS-diensten. Om het schaderisico van onveilige IoT-apparaten te beperken, lanceerde SIDN Labs het SPIN-project. Hierbij evalueerden we de bruikbaarheid van de Manufacturer Usage Description (MUD) specificatie, die momenteel wordt ontwikkeld door de Operations and Management Area Working Group (OPSAWG) binnen de Internet Engineering Task Force (IETF).

De achterliggende gedachte hierbij is dat wanneer een IoT-apparaat verbinding zoekt met een netwerk, het apparaat doorgeeft welke resources het nodig heeft om goed te kunnen functioneren. Deze informatie wordt vastgelegd in een MUD-profiel, dat het beoogde netwerkgedrag van het apparaat beschrijft op basis van een 'whitelist'. Deze whitelist zou compleet moeten zijn en dus kan de toegang tot andere netwerkresources worden geweigerd zonder dat dit de goede werking van het apparaat belemmert.

In dit onderzoek bestudeerden we de toepasbaarheid van MUD voor het beveiligen van IoT-apparaten tegen hackpogingen. Ook onderzochten we of de bruikbaarheid van IoT-apparaten voor DDoS-aanvallen afneemt door een profiel te handhaven. De MUD-specificatie is echter nog niet klaar voor gebruik en dus nog ergens geïmplementeerd. Om MUD-profielen te



## Accountability in the Internet of Things (IoT): Systems, law & ways forward

Jatinder Singh\*\*, Christopher Millard\*, Chris Reed\*, Jennifer Cobbe\*, Jon Crowcroft\*

\*Dept. of Computer Science & Technology (Computer Laboratory), University of Cambridge

\*\*Centre for Commercial Law Studies, Queen Mary University of London

### Abstract

Accountability is key to realising the full potential of the IoT. This is for reasons of adoption and public acceptability, and to ensure that the technologies deployed are, and remain, appropriate and fit for purpose. Though technology generally is subject to increasing legal and regulatory attention, the physical, pervasive and autonomous nature of the IoT raises specific accountability challenges; for instance, relating to safety and security, privacy and surveillance, and general questions of governance and responsibility. This article considers the emerging 'systems of systems' nature of the IoT, giving the broad legal context for these concerns, to indicate technical directions and opportunities for improving levels of accountability regarding technologies that will increasingly underpin and pervade society.





# What should we (the world) 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?

# Paper: Cleaning up the Internet of Evil things

[https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019\\_02B-2\\_Cetin\\_paper.pdf](https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02B-2_Cetin_paper.pdf)

Paper by TUD, YNU, and NICT into the effectiveness of remediation strategies, such as notification and quarantining infected networks.

Tracked Mirai infections through several sources, and the rate of cleanup for several methods.

# Cleaning up the Internet of Evil things: Mirai

- 87% of infections in broadband access networks
- 58-74% natural cleanup rate (no action taken) over several control groups
- 77% cleanup on email notification
- 92% cleanup on quarantine
- Only 5% reinfection rate after 5 months

# Quarantined by ISP

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

Your computer is infected

Your computer is infected

You have been quarantined

You have

is infected

You have been quarantined

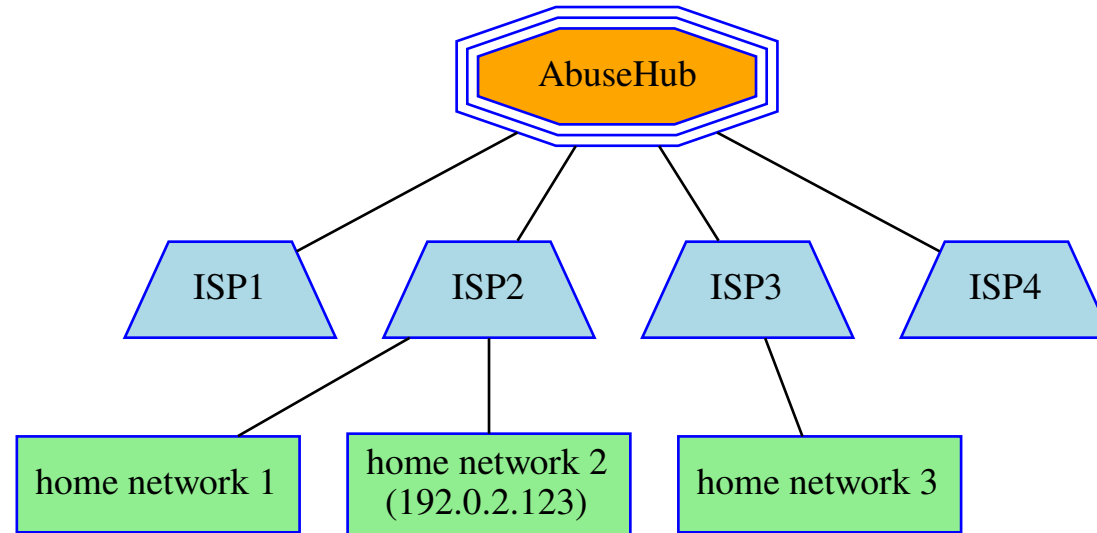


# Conclusion:

- Quarantines work!
- But please, do it right:
  - Specify issue and reason
  - Specify date and time
  - Specify what to do

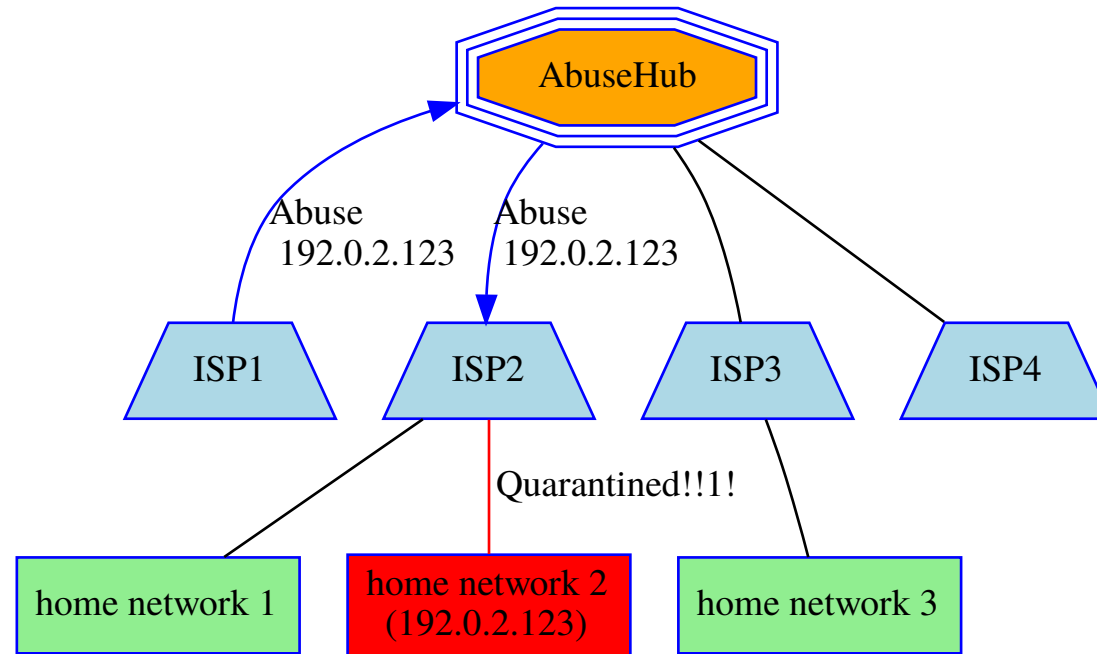
Can we do even better?

# Incident report system

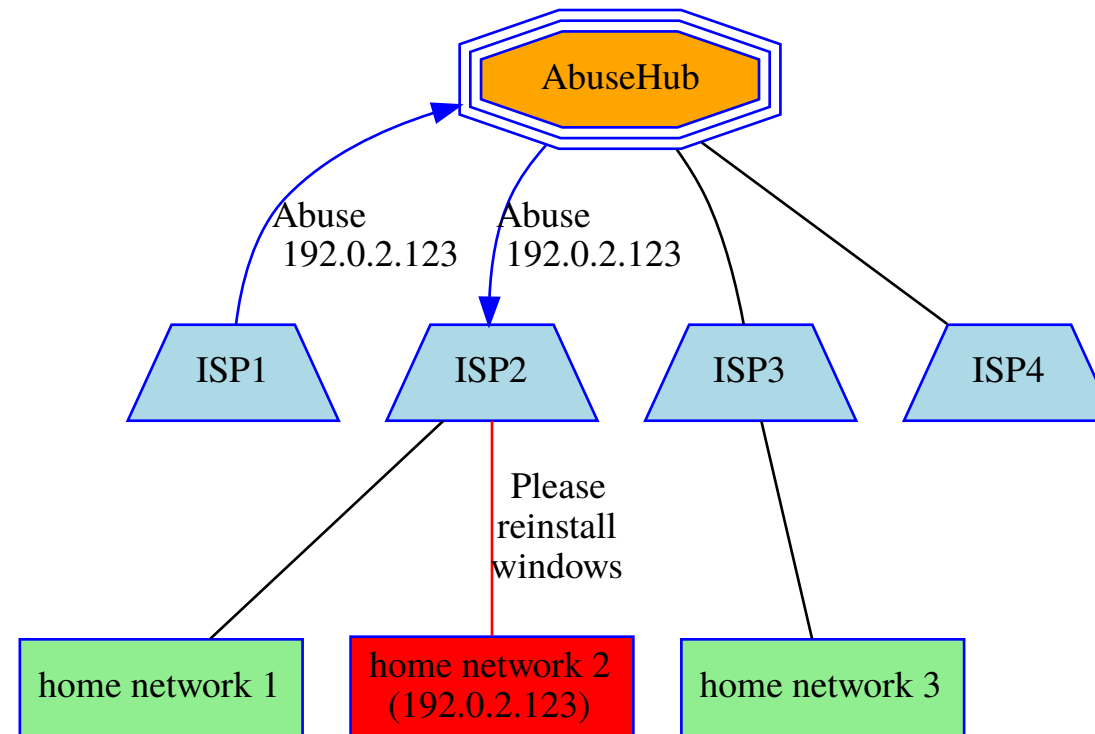




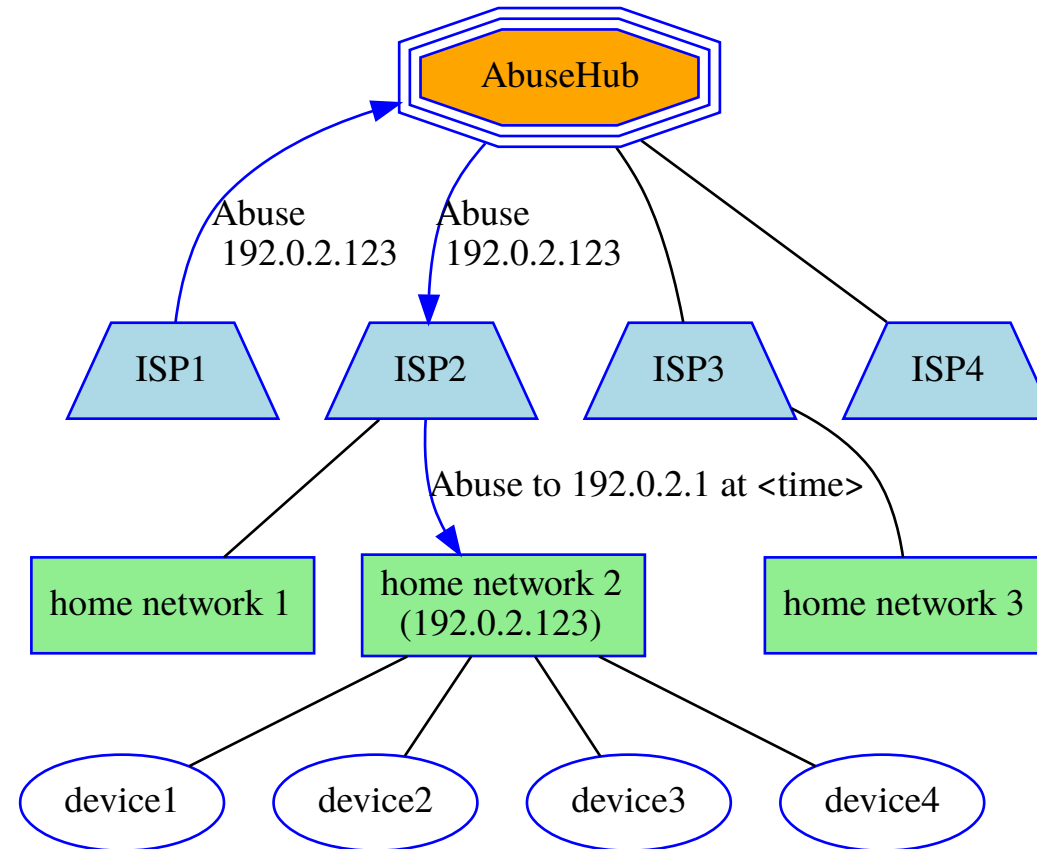
# Incident report system



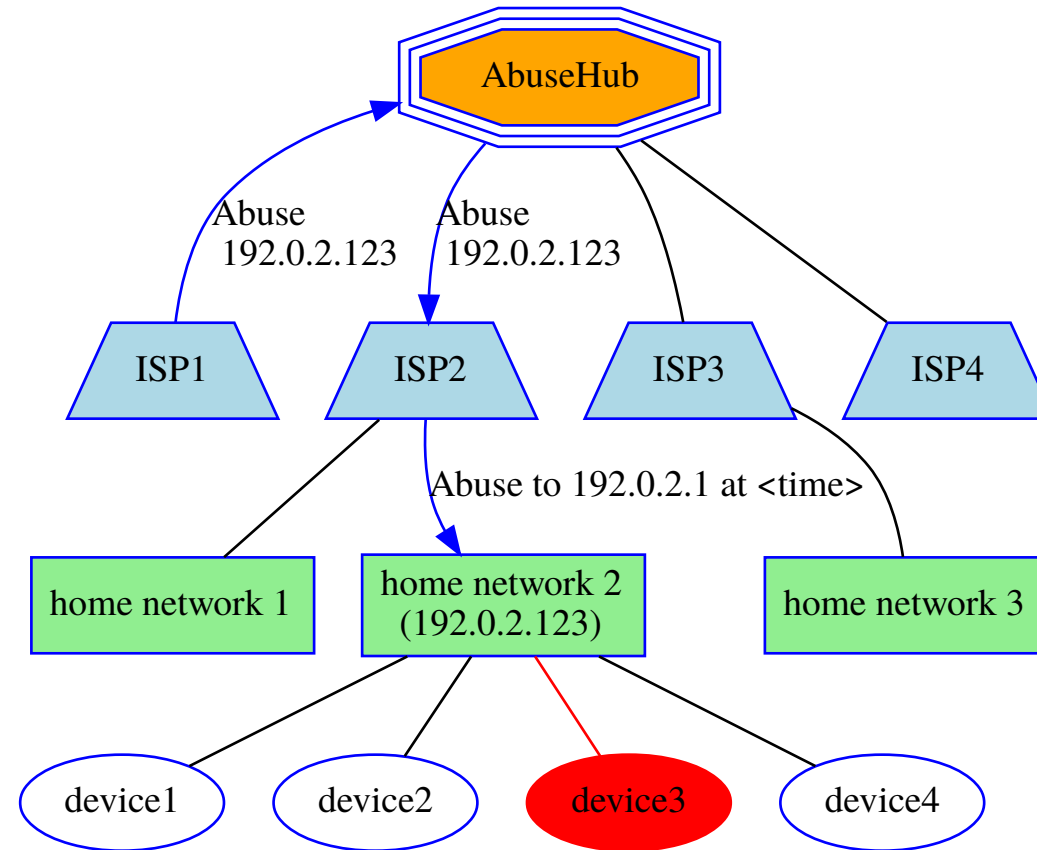
# Incident report system



# Incident report system



# Incident report system



# More granular quarantining:

- Specify the bad behaviour (time, target, ports, etc.)
- Router should figure out how to mitigate:
  - Preventative firewall rules (dots-signal-call-home)
  - Active response to behaviour (SPIN approach)

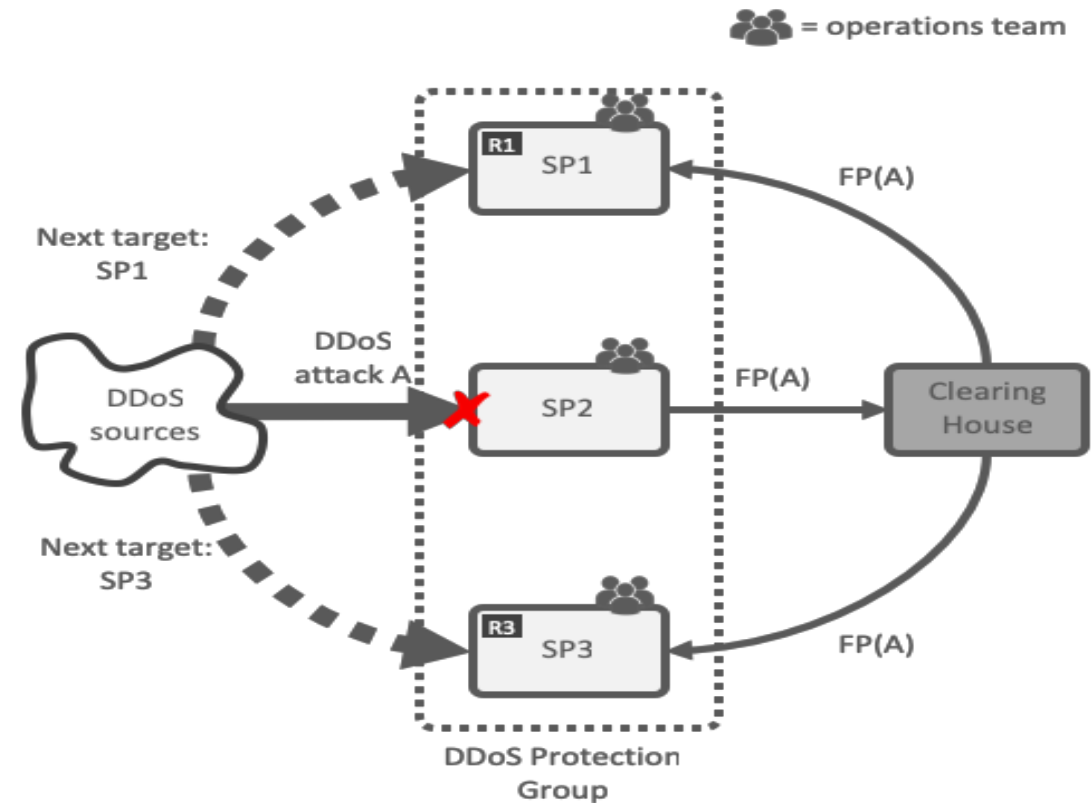
dots: DDoS Open Threat Signaling (dots) work at IETF:

- <https://datatracker.ietf.org/wg/dots/charter/>
- <https://datatracker.ietf.org/doc/draft-ietf-dots-signal-call-home/>

# The IoT and the DNS @ .nl

# National DDoS clearing house

- Continuous and automatic sharing of “fingerprints” of (IoT-powered) DDoS attacks buys providers time (proactive)
- Extends DDoS protection services of critical service providers, not a replacement
- Pilot with 10 NL partners, then scale up to EU-level as part of CONCORDIA project [DDoS19]





# What should we (the world) 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?**

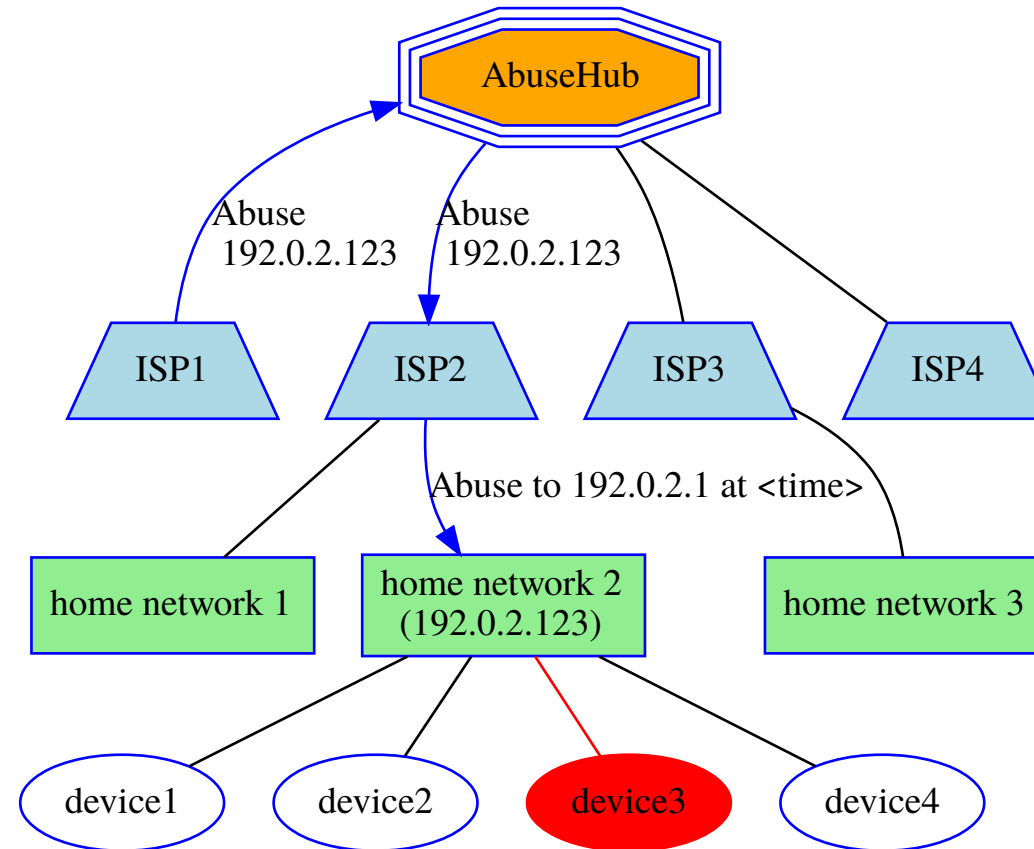
# The SPIN project at SIDN Labs

- Security and Privacy for In-home Networks
- Research and prototype of SPIN functionality:
  - Visualise network traffic
  - Signal problems based on traffic patterns
  - Perform measurements on (IoT) devices
- Goal: Protect the Internet by protecting the home
- Get functionality like this into deployed routers

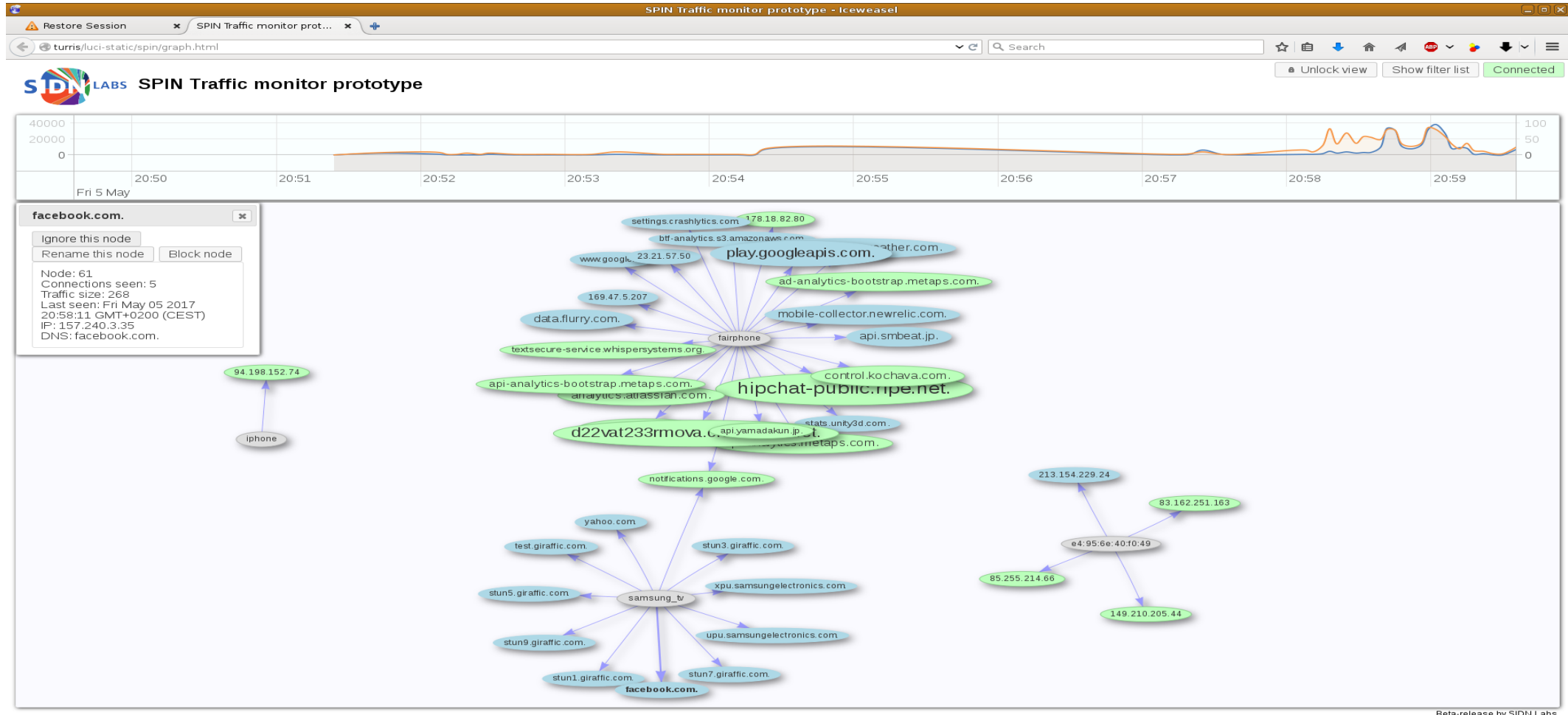
# The SPIN project at SIDN Labs

- Open source in-home router/AP software that
- Provides insight into device activity on the Internet
- Serves as platform for research and experimentation

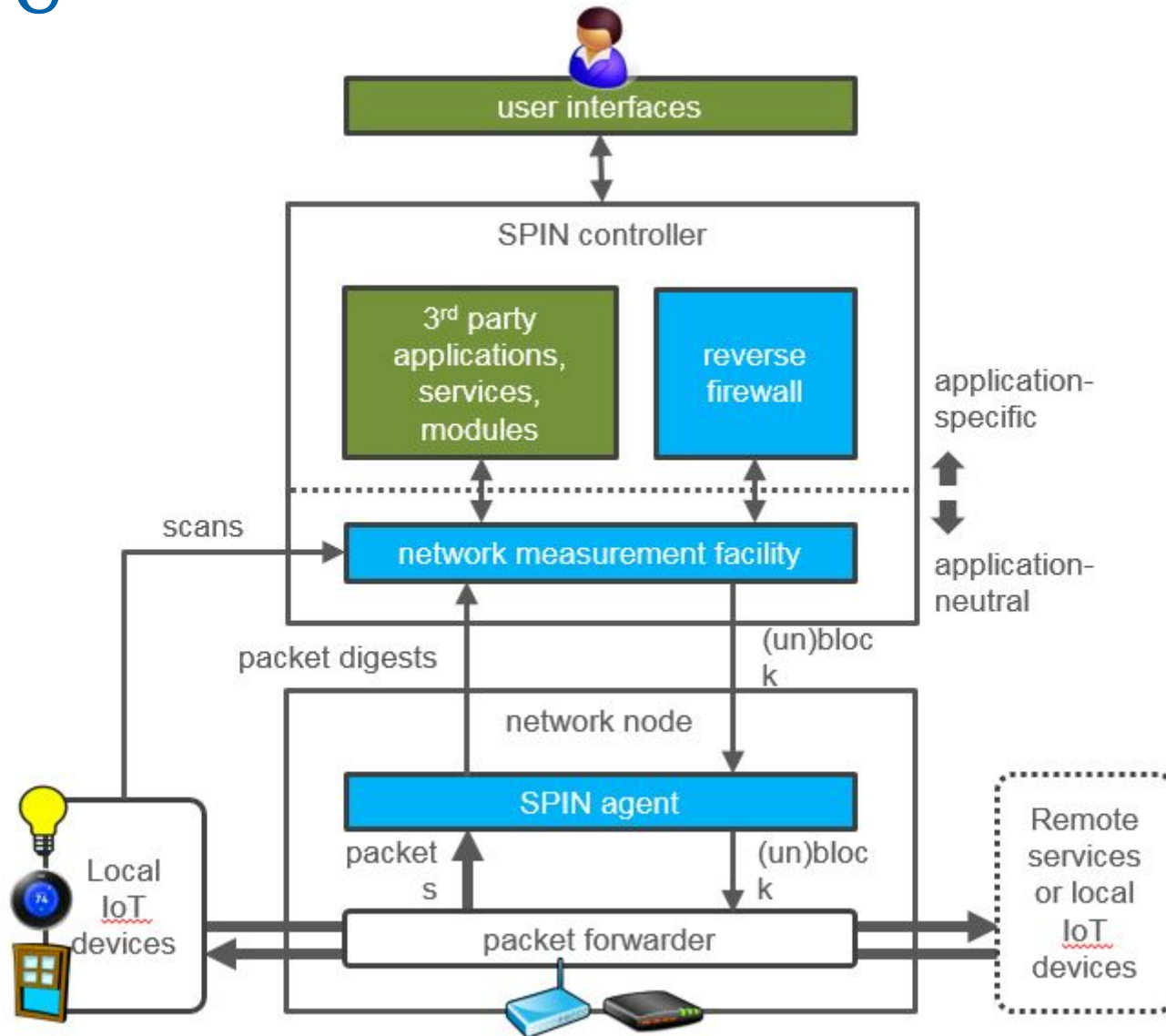
# Fine-grained blocking of vulnerable IoT devices through SPIN



# SPIN DNS traffic monitor for IoT users

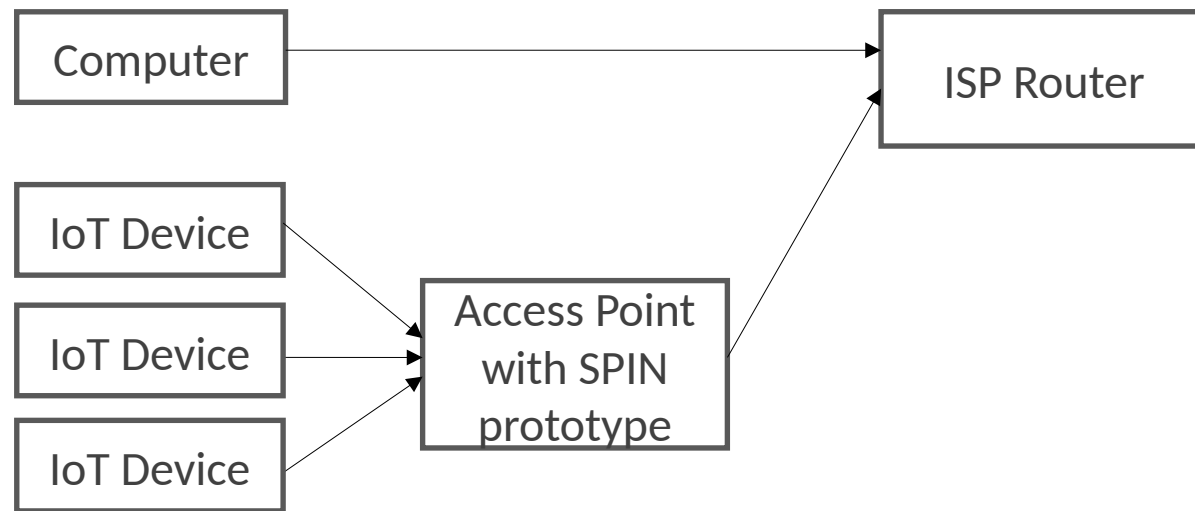


# Architecture



# Prototype built on OpenWRT

- Currently bundled with Valibox:  
<http://valibox.sidnlabs.nl>
- Source at <https://github.com/SIDN/spin>
- Also runs on Debian and Raspberry Pi (with some hammering)



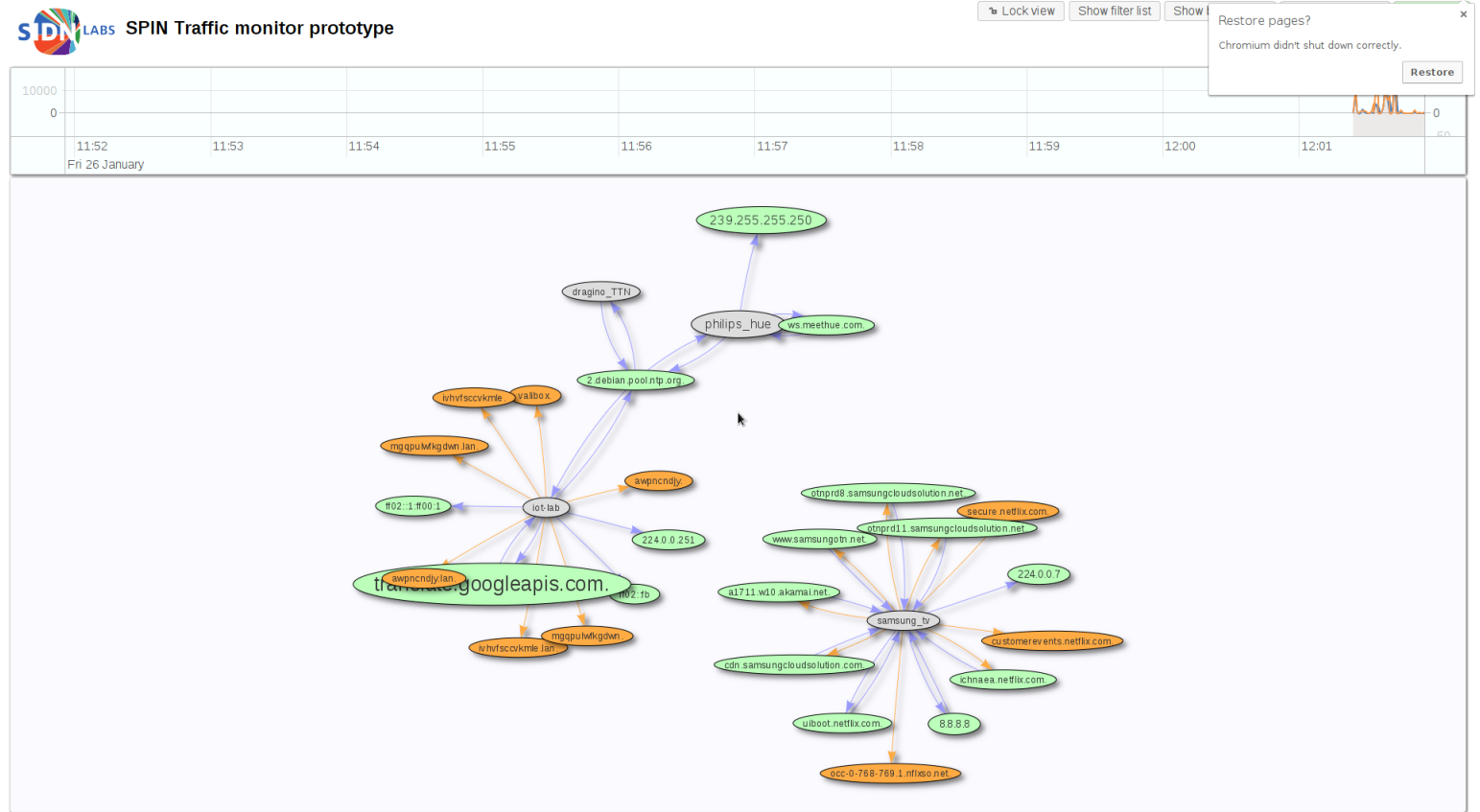
prototype 2, GL-Inet hardware

# Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based on source or destination
- Download traffic from specific devices

Next research topics:

- In-depth device traffic analysis
- Time-series based analysis





If time permits,  
show SPIN in action here

Thank you for your attention!

Any questions?

*Follow us*

 sidnlabs.nl

 @SIDN @sidnlabs @twitjeb

 SIDN



# Fora to discuss approaches on technical level

- IETF
  - IETF dots working group
  
- RIPE: <https://www.ripe.net>
  - RIPE IoT Working group
  - RIPE Abuse working group
  - RIPE Routing working group

Next RIPE meeting: May 11-15, Berlin  
<https://ripe80.ripe.net>

# References and related reading

- SAC-105 - The DNS and the Internet of Things: Opportunities, Risks, and Challenges  
<https://www.icann.org/en/system/files/files/sac-105-en.pdf>
- SPIN website:  
<https://spin.sidnlabs.nl>
- RIPE IoT working group  
<https://www.ripe.net/participate/ripe/wg/iot>
- ISOC IoT information  
<https://www.internetsociety.org/iot/getiotsmart/>