

Securing Home Networks with SPIN

Elmer Lastdrager – SIDN Labs

31 May 2018



What **is** the IoT?

- A simple definition: “Stuff that was not networked before”



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

threat **post**

CATEGORIES

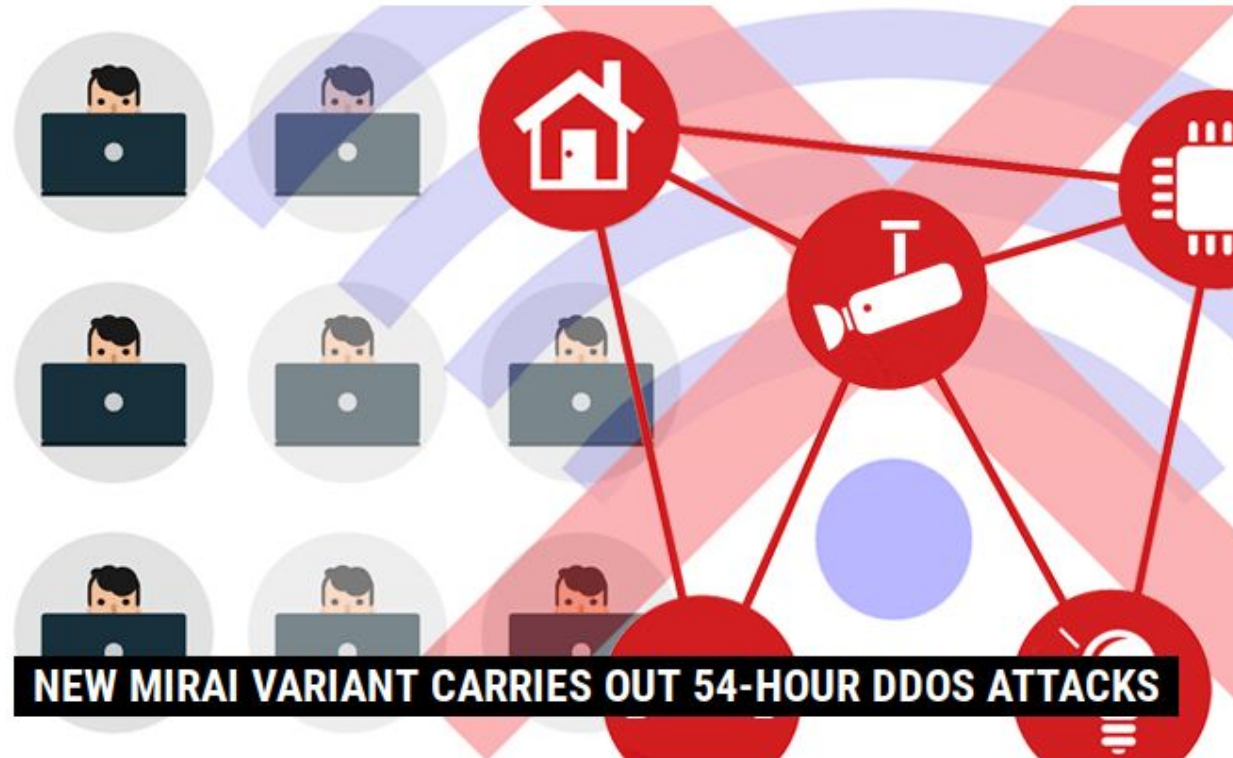
FEATURED

PODCASTS

VIDEOS



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



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?

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”

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: SPIN**

The SPIN project at SIDN Labs

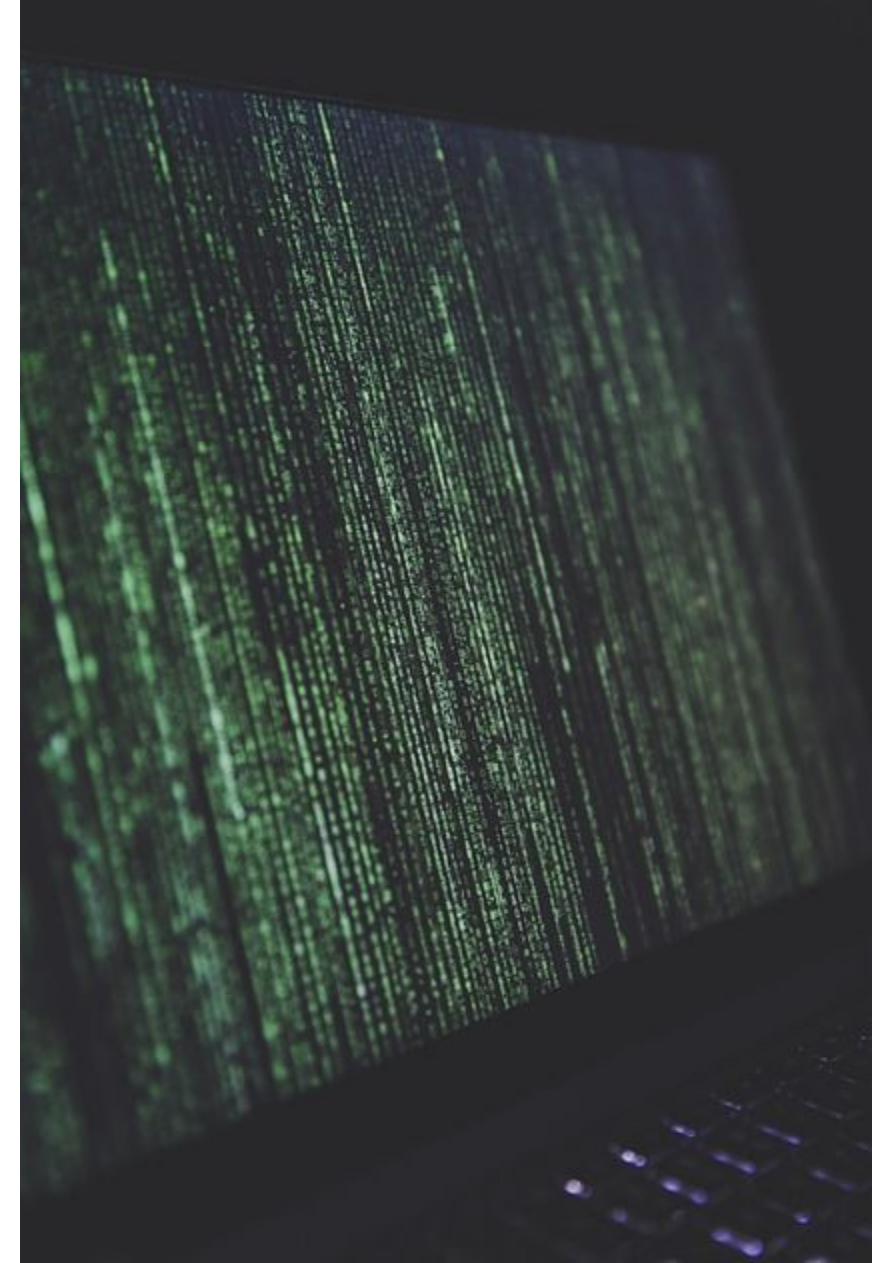
- Security and Privacy for In-home Networks
- Research and prototype of SPIN functionality:
 - Visualising network traffic
 - (Automatic) blocking of 'bad' traffic
 - Allow 'good' traffic



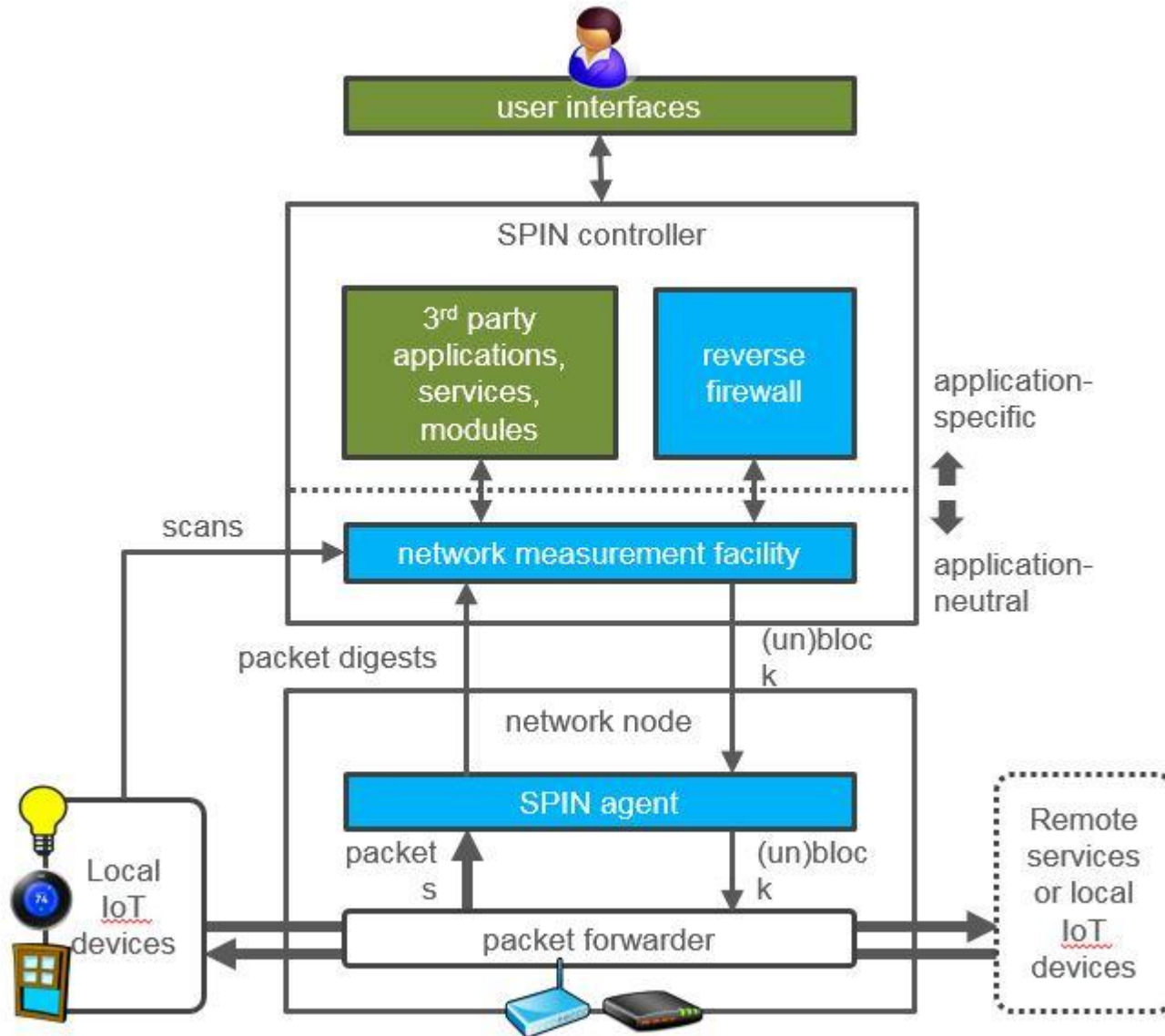
The SPIN project at SIDN Labs

Open source in-home router/AP software that

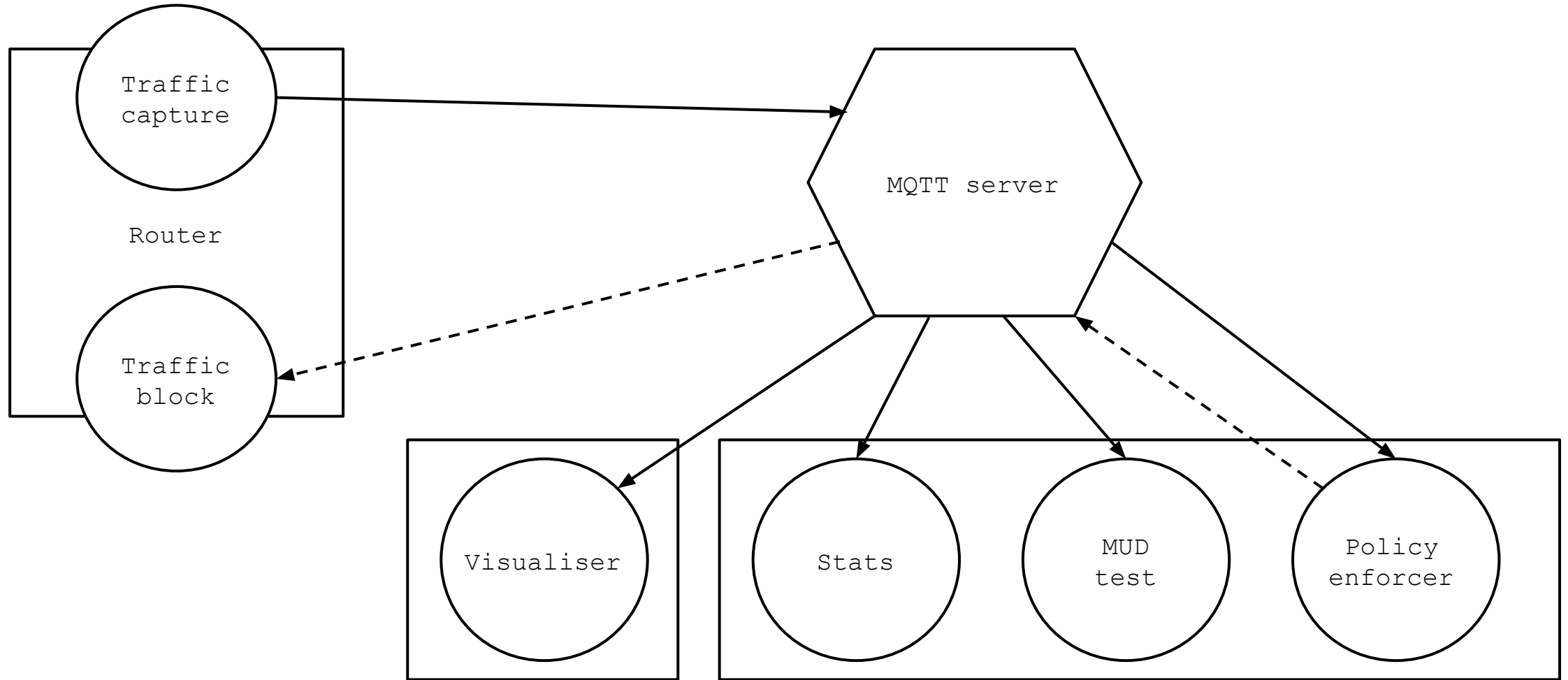
1. helps protect DNS operators (like SIDN!) and other service providers against IoT-powered DDoS attacks
2. helps end-users controls the security of their home networks



Architecture



Architecture



Prototype built on OpenWRT

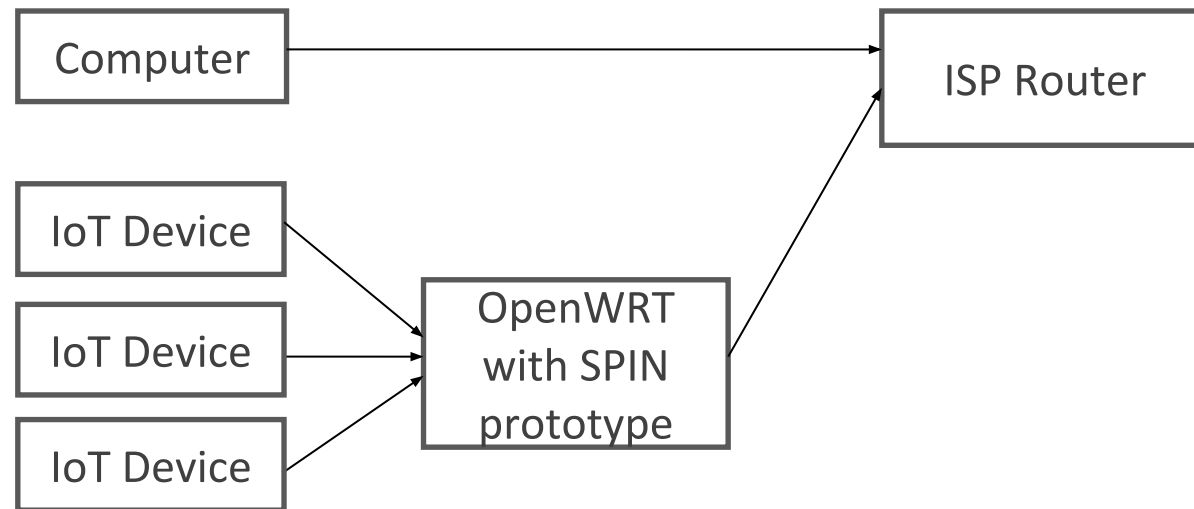
Currently bundled with Valibox:

<https://valibox.sidnlabs.nl>

Source at <https://github.com/SIDN/spin>



prototype 2, GL-Inet hardware

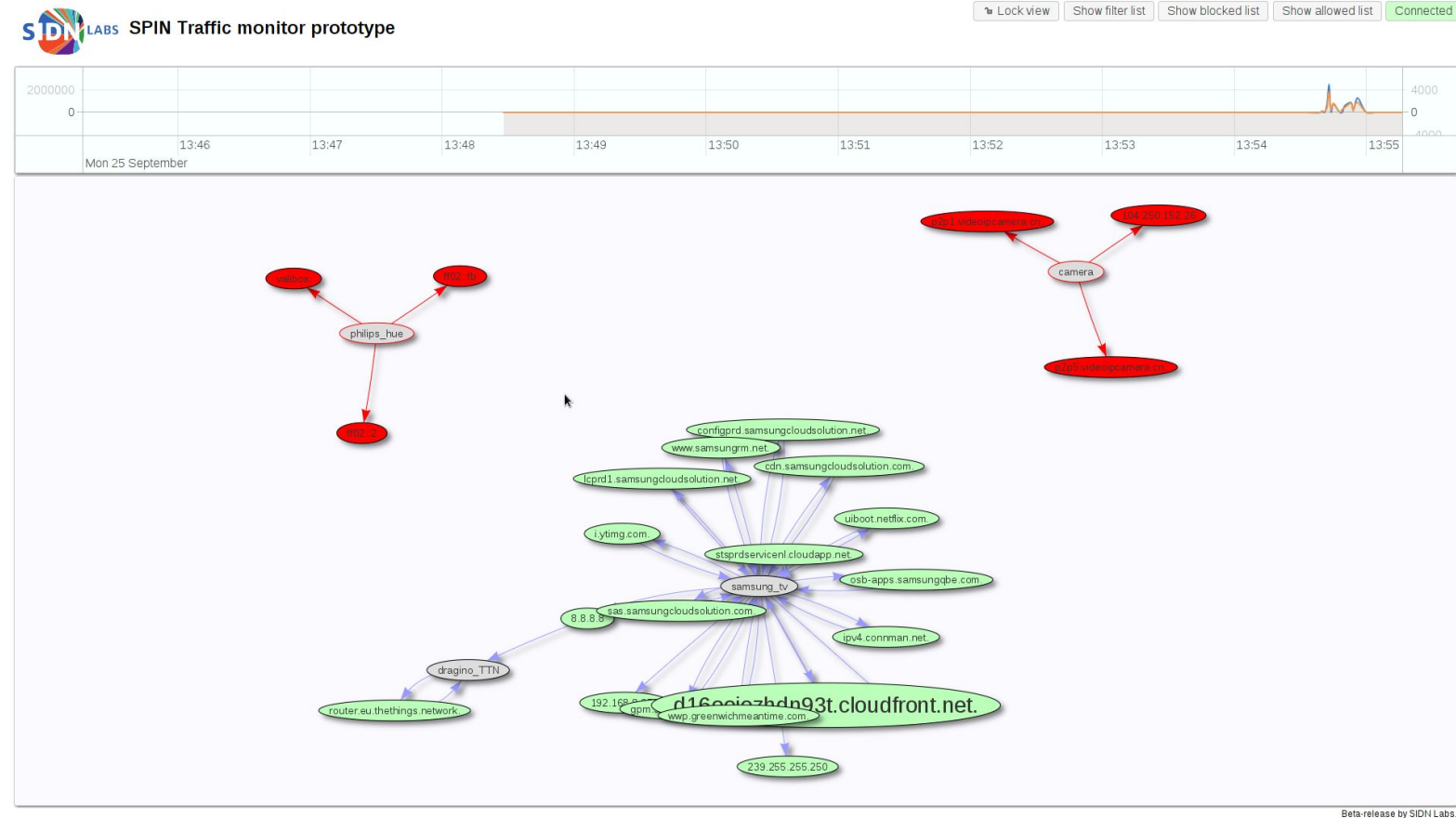


Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based on source or destination

In beta:

- Select device and download (live) pcap for selected device

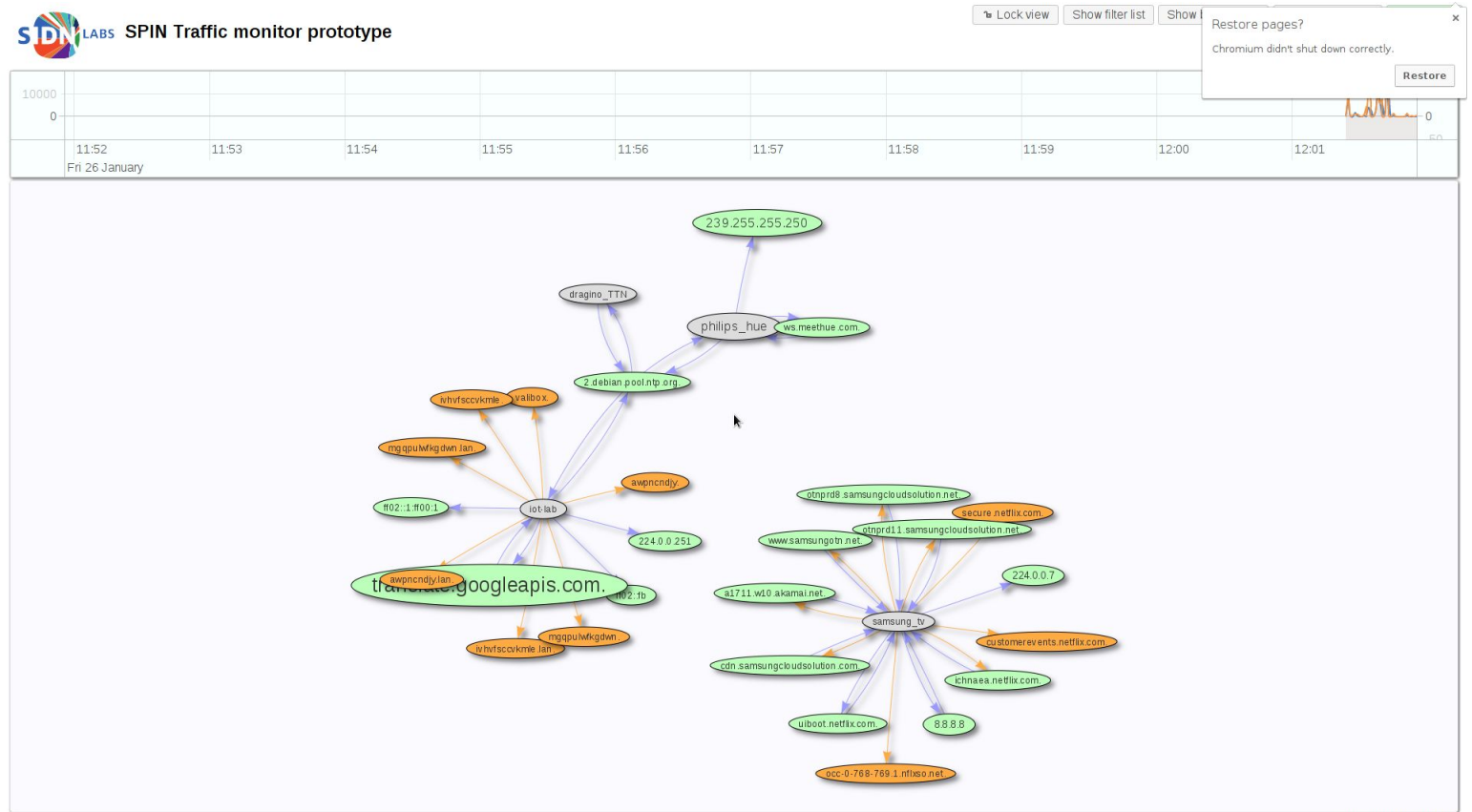


Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based on source or destination

In beta:

- Select device and download (live) pcap for selected device



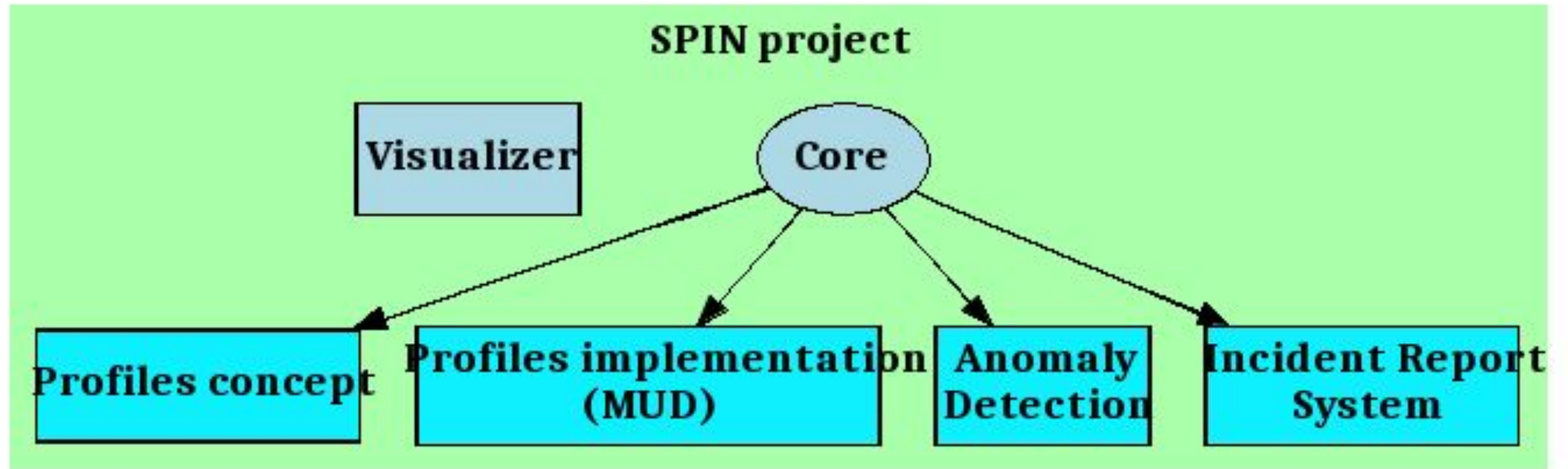
Core components

Currently:

- OpenWRT/Linux kernel module (in C)
 - Captures and blocks traffic
 - Initial aggregation
- User-space daemon (in C)
 - Further aggregation and enrichment of data
 - Sends to MQTT daemon
- MQTT Daemon (Mosquitto)
 - Distributes traffic data to clients (mqtt/websockets)
 - Sends commands back to router
- Several Clients
 - Visualiser (Javascript)
 - Statistics tool (Lua)
 - PoC MUD tool (Lua)
 - PoC (hardcoded) 'bad behaviour' tool (Lua)
 - Recent history storage (currently 10 minutes) (Lua)



Current research/prototype topics:



Profiles: Conceptual

Still very much in the 'idea forming' stage

Base profiles

Social networks

Streaming sites

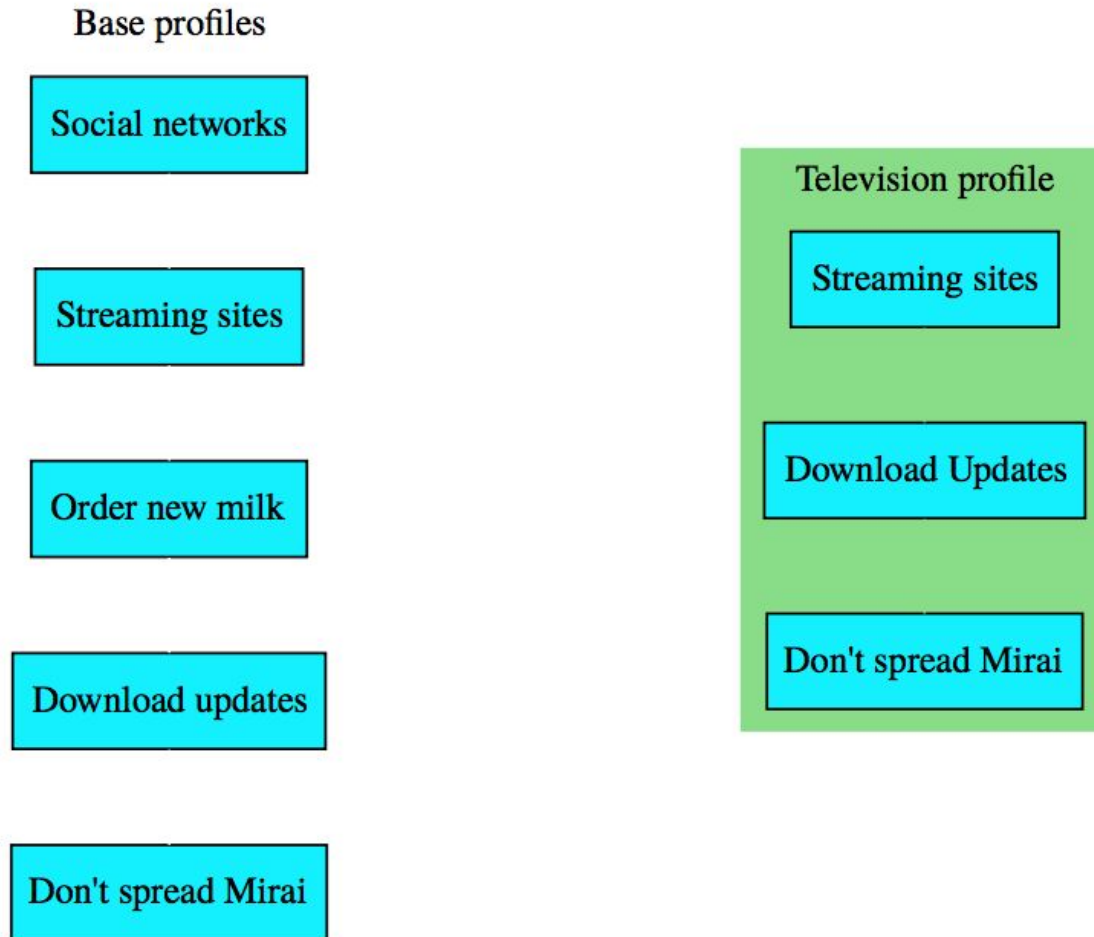
Order new milk

Download updates

Don't spread Mirai

Profiles: Conceptual

Still very much in the 'idea forming' stage



Profiles: Conceptual

Still very much in the 'idea forming' stage

Base profiles

Social networks

Streaming sites

Order new milk

Download updates

Don't spread Mirai

Television profile

Streaming sites

Download Updates

Don't spread Mirai

Refrigerator profile

Order new milk

Download Updates

No virussy stuff

Profiles: Implementation: MUD?

Manufacturer Usage Description (MUD)

- Draft at IETF
- JSON description of internet traffic that is or is not allowed from and to the device
- Translates almost directly to firewall rules

Our work:

- Provide (additional) early implementation for testing
- Looking into automatic generation of basic profiles
- Looking into extending it (e.g. to add a bandwidth limitation)
- Looking into 'reverse' profiles (any device that matches profile X is infected with Y, think IDS rules)

And more wildly:

- A way for users and companies to create and share device profiles (that improve manufacturer-provided ones)

Profiles: Implementation: MUD

Subproject: Lua-MUD

- Small MUD library for Lua
- Tiny subset for now (and pretty much hardcoded)
- Lua-mud-0.1 (on luarocks and github)
- Working on 'full' version.

Master student working on traffic analysis for MUD

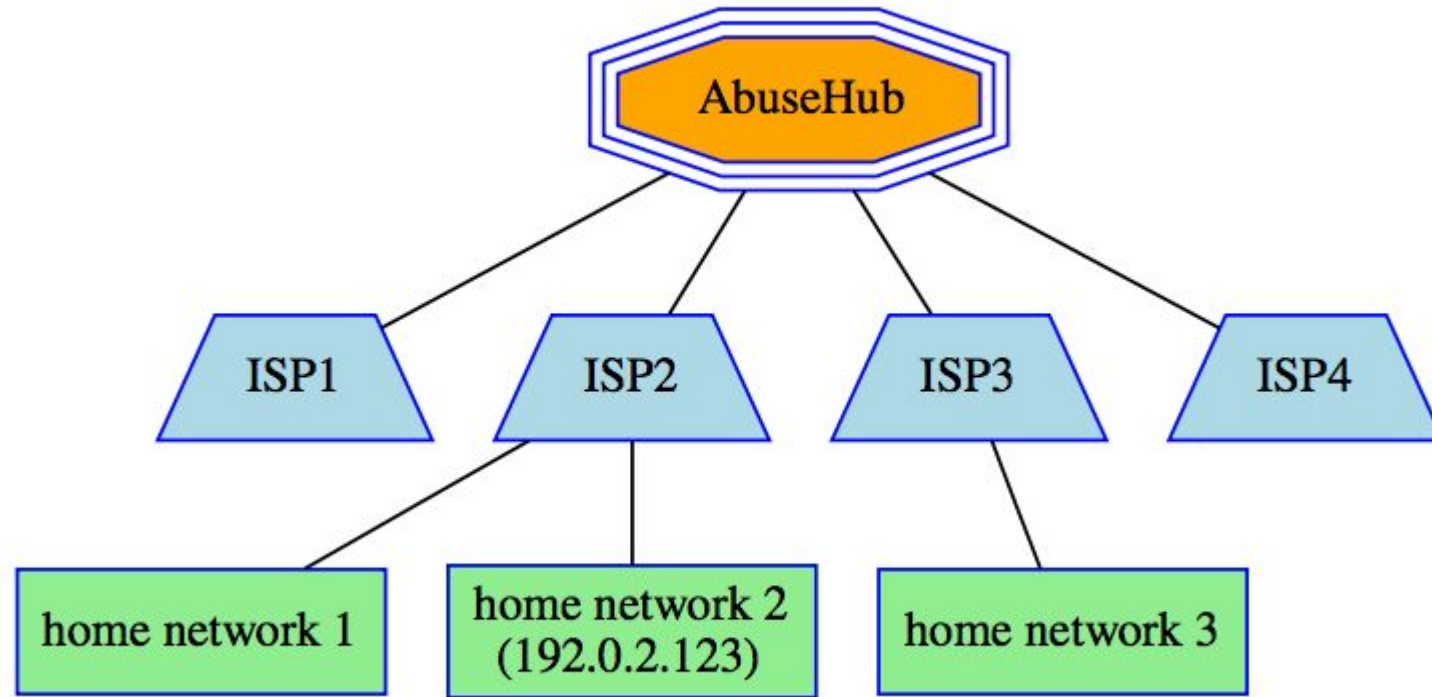
- And generation of profiles like mudgee
- Research question: how much can you deduce from observation?

Incident report system

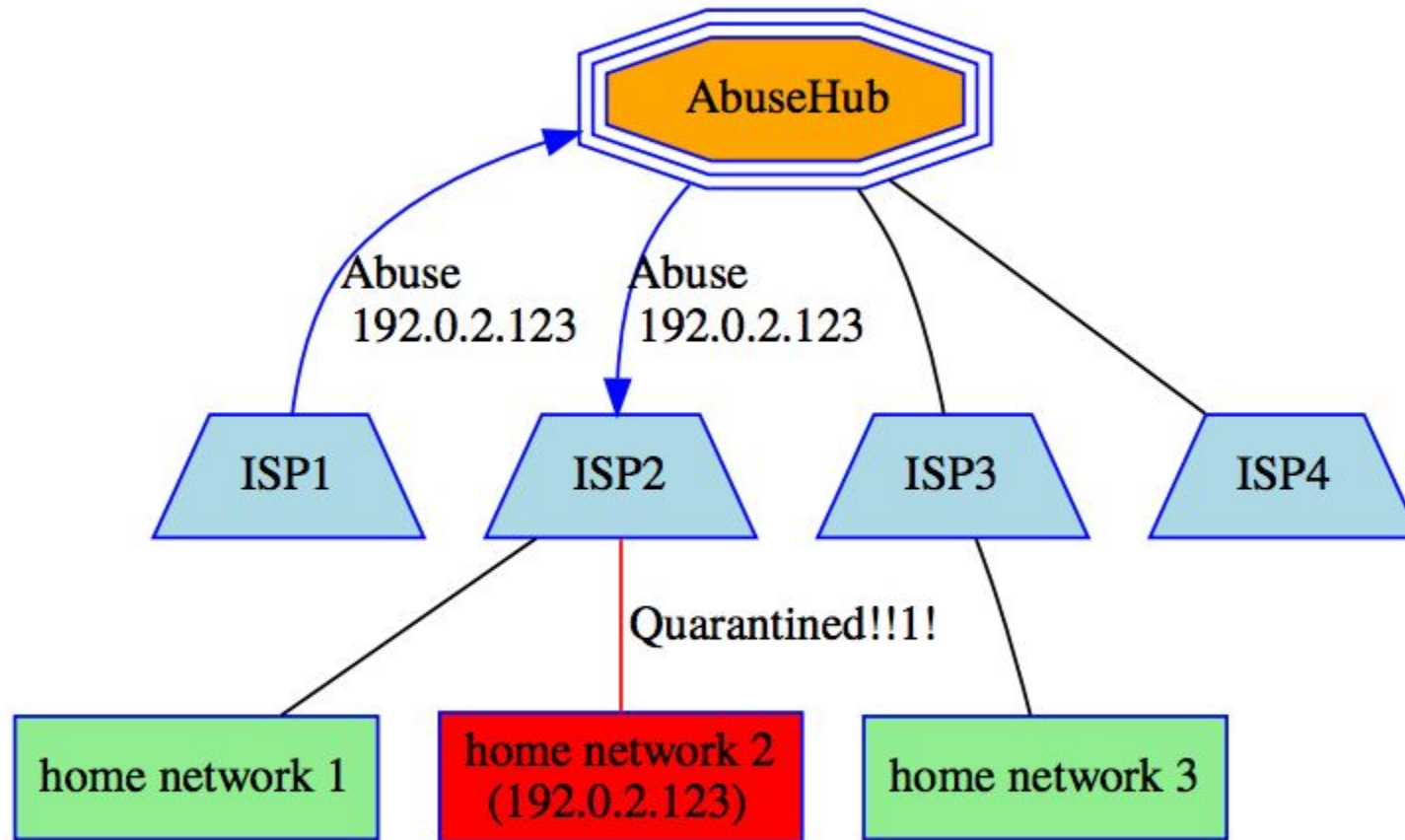
Problem: If ISP's do anything about bad traffic from their customers in the first place, it's generally a full quarantine of the customer.



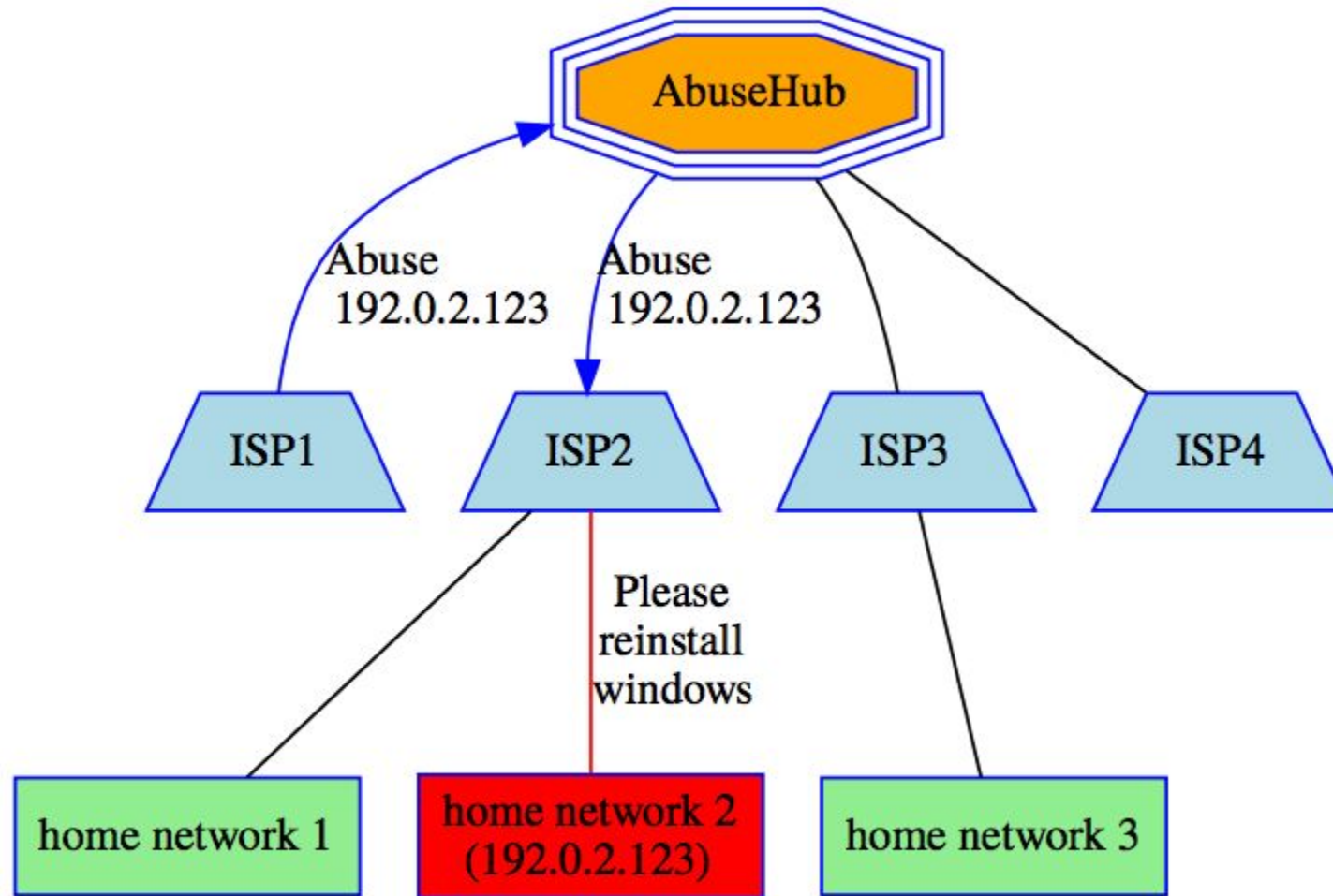
Incident report system



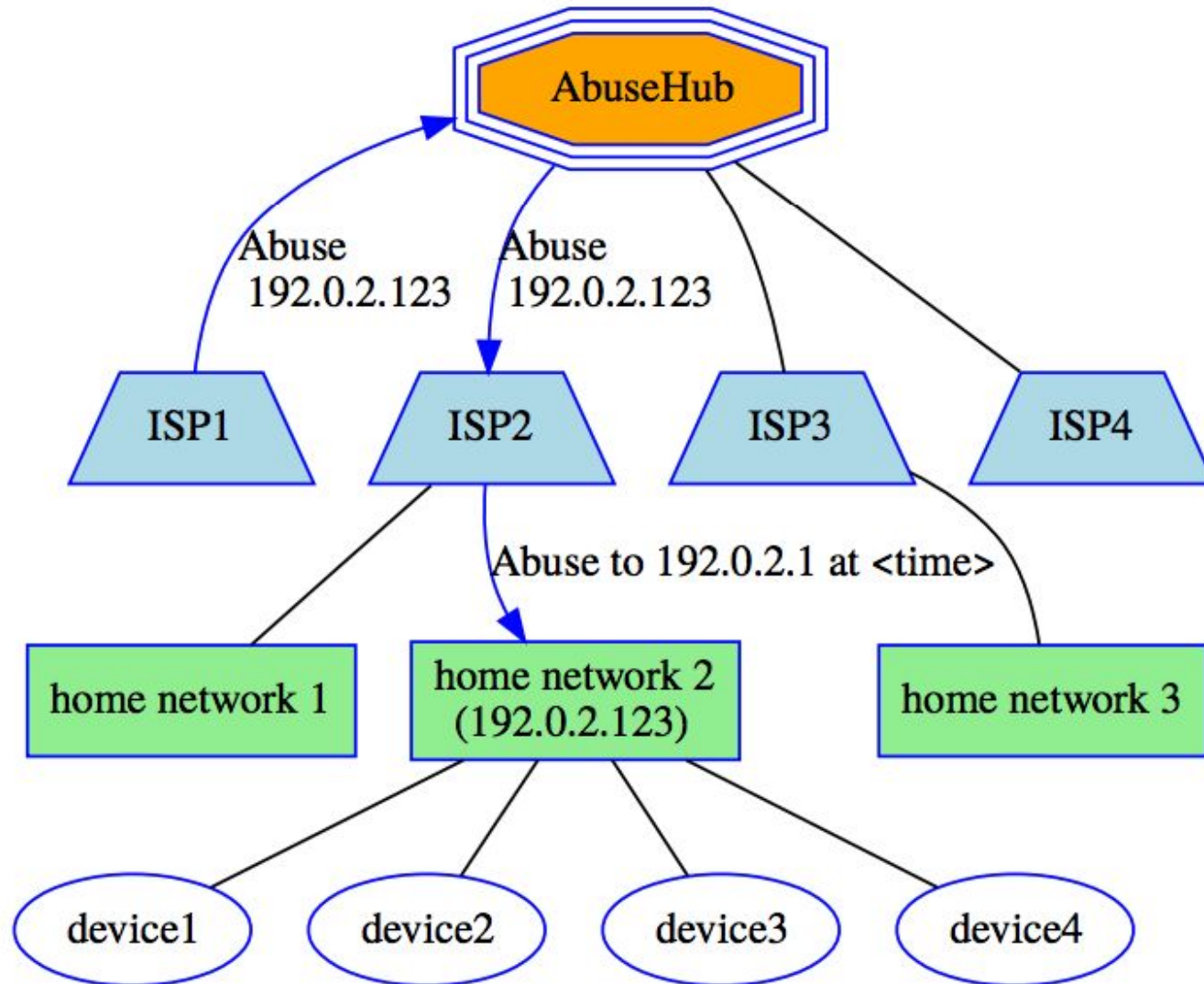
Incident report system



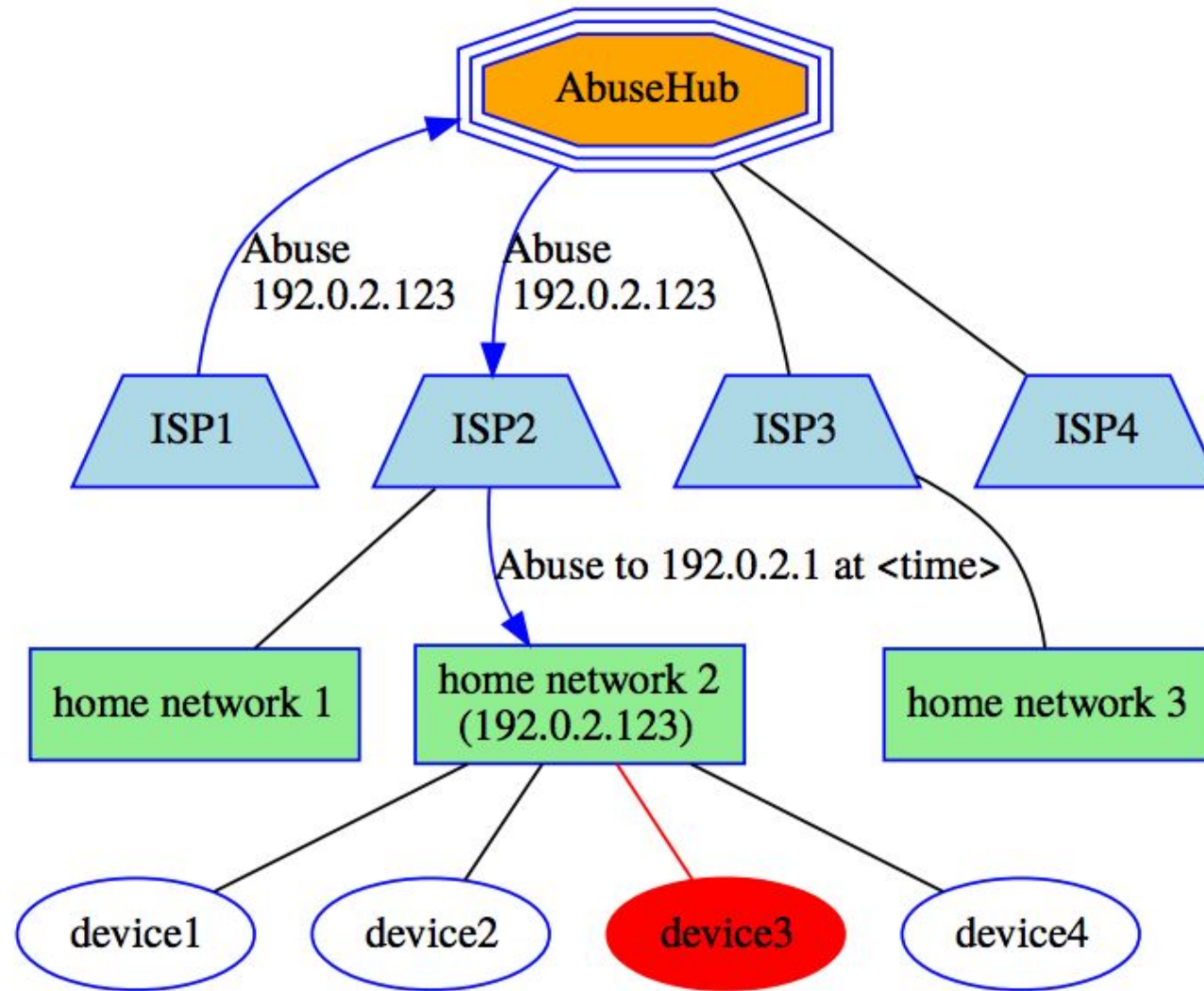
Incident report system



Incident report system



Incident report system



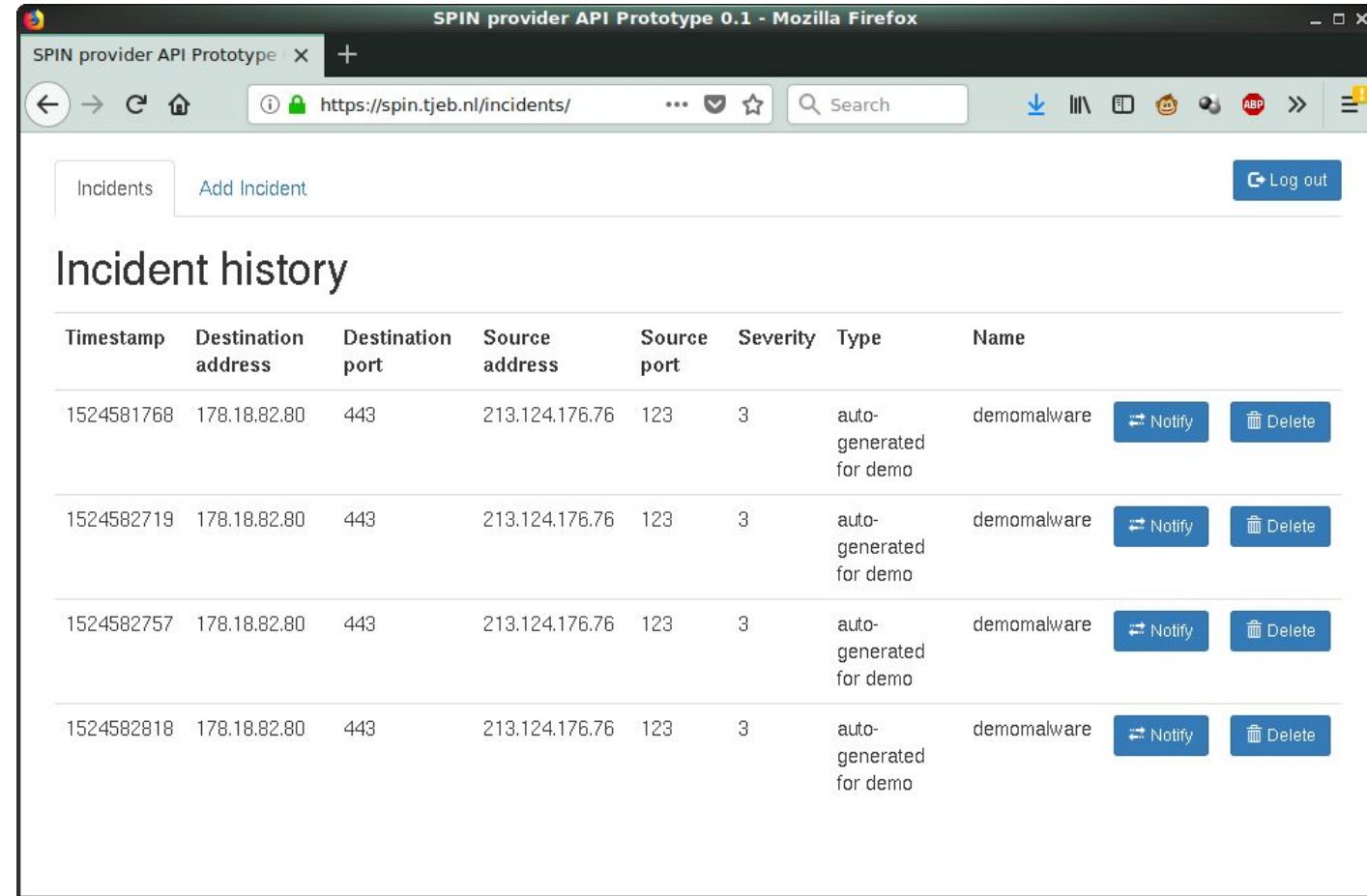
Running prototype

Small (Django) web application for reports

Notification to router (poll or push)

Router finds device in history

Router blocks device



Timestamp	Destination address	Destination port	Source address	Source port	Severity	Type	Name		
1524581768	178.18.82.80	443	213.124.176.76	123	3	auto-generated for demo	demomalware	Notify	Delete
1524582719	178.18.82.80	443	213.124.176.76	123	3	auto-generated for demo	demomalware	Notify	Delete
1524582757	178.18.82.80	443	213.124.176.76	123	3	auto-generated for demo	demomalware	Notify	Delete
1524582818	178.18.82.80	443	213.124.176.76	123	3	auto-generated for demo	demomalware	Notify	Delete

Anomaly detection

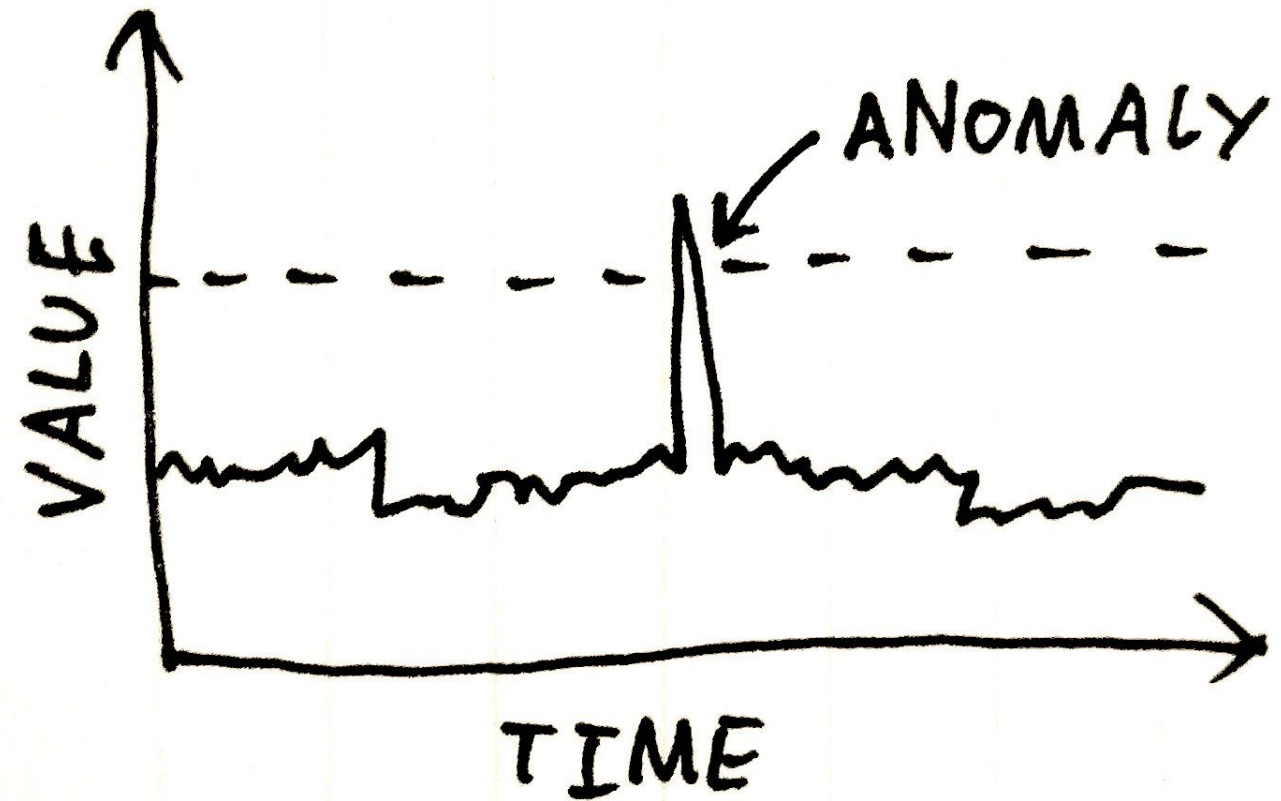
General research topic:

- Can 'bad' behaviour be recognized?
- Perhaps by looking at historic behaviour of device?

We keep a (short) history of device traffic

Extending that into a framework for researchers to do anomaly detection

Currently nothing to show yet, though.



Discussion/questions

Try it out!

<https://valibox.sidnlabs.nl>

<https://github.com/SIDN/spin>

Missing something?

Any other questions or comments?



Elmer Lastdrager
elmer.lastdrager@sidn.nl
@elmerlastdrager

sidn.nl | sidnlabs.nl
@sidnlabs