Securing homenets in the IoT

Cristian Hesselman

BotLeg Workshop | Amsterdam | June 1, 2018

SIDN LABS

Internet of Things

- Trillions of (tiny) special-purpose devices
- Continually sense and act upon users' physical environment
- Encode people's offline activities and send over the Internet
- Novel (data analysis) applications to ease our lives
  - Domains: human, home, retail, offices, factories, work sites, vehicles, cities, outside (ISOC)
  - Apps: health control, disease management, safety systems, energy control, traffic control

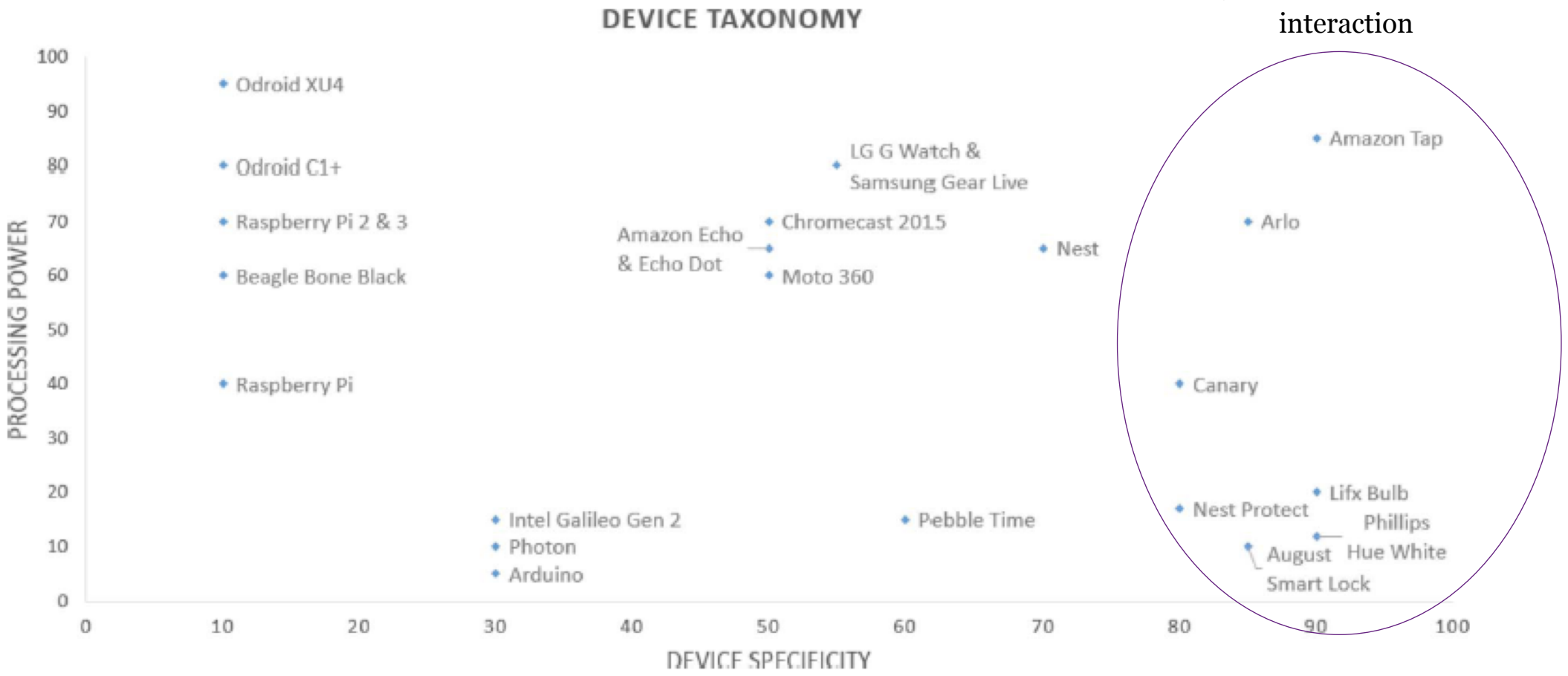
SDN LABS

IoT devices widely heterogeneous

- Often tailored to a specific task (e.g., lighting, traffic sensing)
- Varying capabilities (hard/software, OS, configurations, UI)
- Autonomous operation (unattended, extended periods of time)
- Invisibly integrated into physical structures
- Intermittent connectivity (to the Internet and between devices)
- Cross-device interactions (networked or physical)
- Often no security protocols (e.g., SSL/TLS) or weak crypto
- Many manufacturers from various industries
- Many operators with widely varying networking skills

SIDN LABS

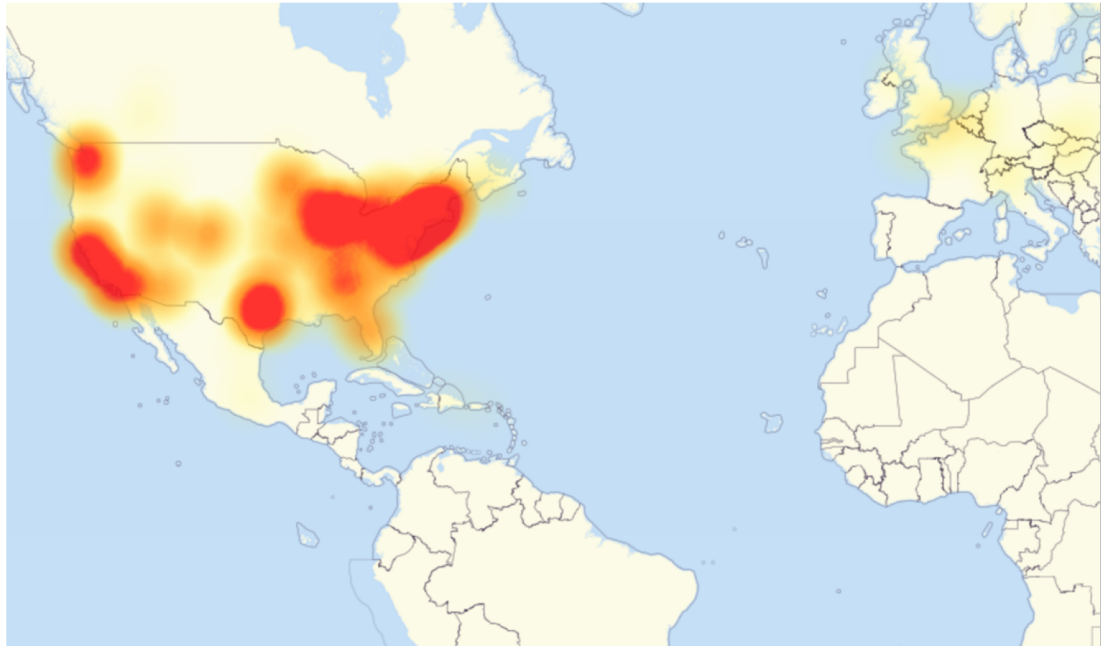
Example: device capabilities

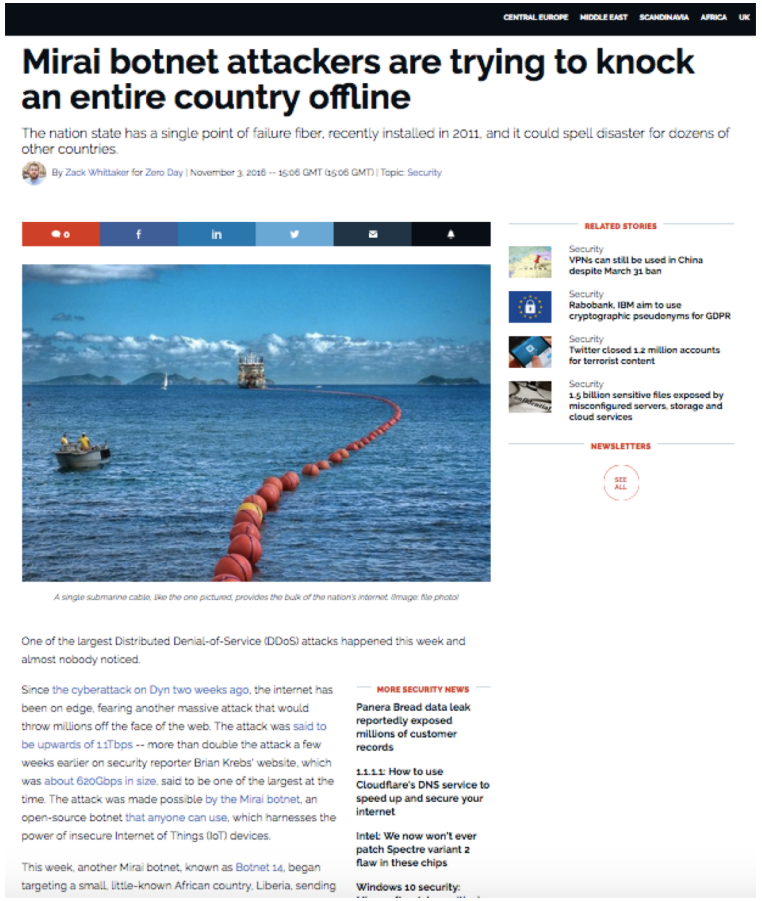


Most attractive to attackers, because limited user interaction

Javid Habibi, Daniele Midi, Anand Mudgerikar, and Elisa Bertino, "Heimdall: Mitigating the Internet of Insecure Things", IEEE Internet of Things Journal, Vol. 4, No. 4, Aug 2017

IoT-powered DDoS attacks (Mirai)





CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK

Mirai botnet attackers are trying to knock an entire country offline

The nation state has a single point of failure fiber, recently installed in 2011, and it could spell disaster for dozens of other countries.

By Zack Whittaker for Zero Day | November 3, 2016 -- 15:06 GMT (15:06 GMT) | Topic: Security

A single submarine cable, like the one pictured, provides the bulk of the nation's internet. (Image: file photo)

One of the largest Distributed Denial-of-Service (DDoS) attacks happened this week and almost nobody noticed.

Since the cyberattack on Dyn two weeks ago, the internet has been on edge, fearing another massive attack that would throw millions off the face of the web. The attack was said to be upwards of 1.1Tbps -- more than double the attack a few weeks earlier on security reporter Brian Krebs' website, which was about 620Gbps in size, said to be one of the largest at the time. The attack was made possible by the Mirai botnet, an open-source botnet that anyone can use, which harnesses the power of insecure Internet of Things (IoT) devices.

This week, another Mirai botnet, known as Botnet 14, began targeting a small, little-known African country, Liberia, sending

RELATED STORIES

Security
VPNs can still be used in China despite March 31 ban

Security
Rabobank, IBM aim to use cryptographic pseudonyms for GDPR

Security
Twitter closed 1.2 million accounts for terrorist content

Security
1.5 billion sensitive files exposed by misconfigured servers, storage and cloud services

NEWSLETTERS

SEE ALL

MORE SECURITY NEWS

Panera Bread data leak reportedly exposed millions of customer records

1.1.1.1: How to use Cloudflare's DNS service to speed up and secure your internet

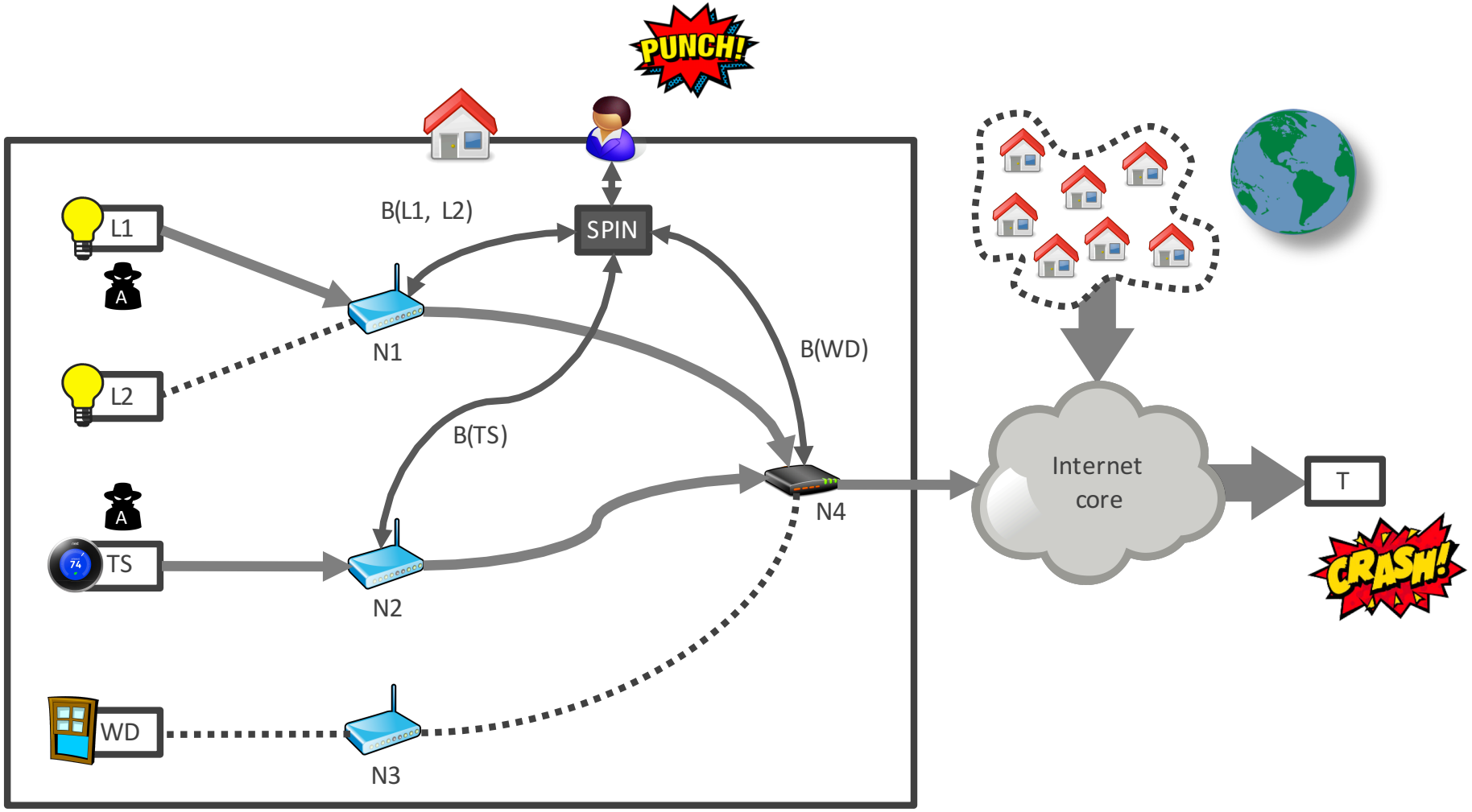
Intel: We now won't ever patch Spectre variant 2 flaw in these chips

Windows 10 security:

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
https://www.arbornetworks.com/blog/asert/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/
Stephen Herzog, “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses”, Journal of Strategic Security, Vol. 4, No. 2, Summer 2011

SDN LABS

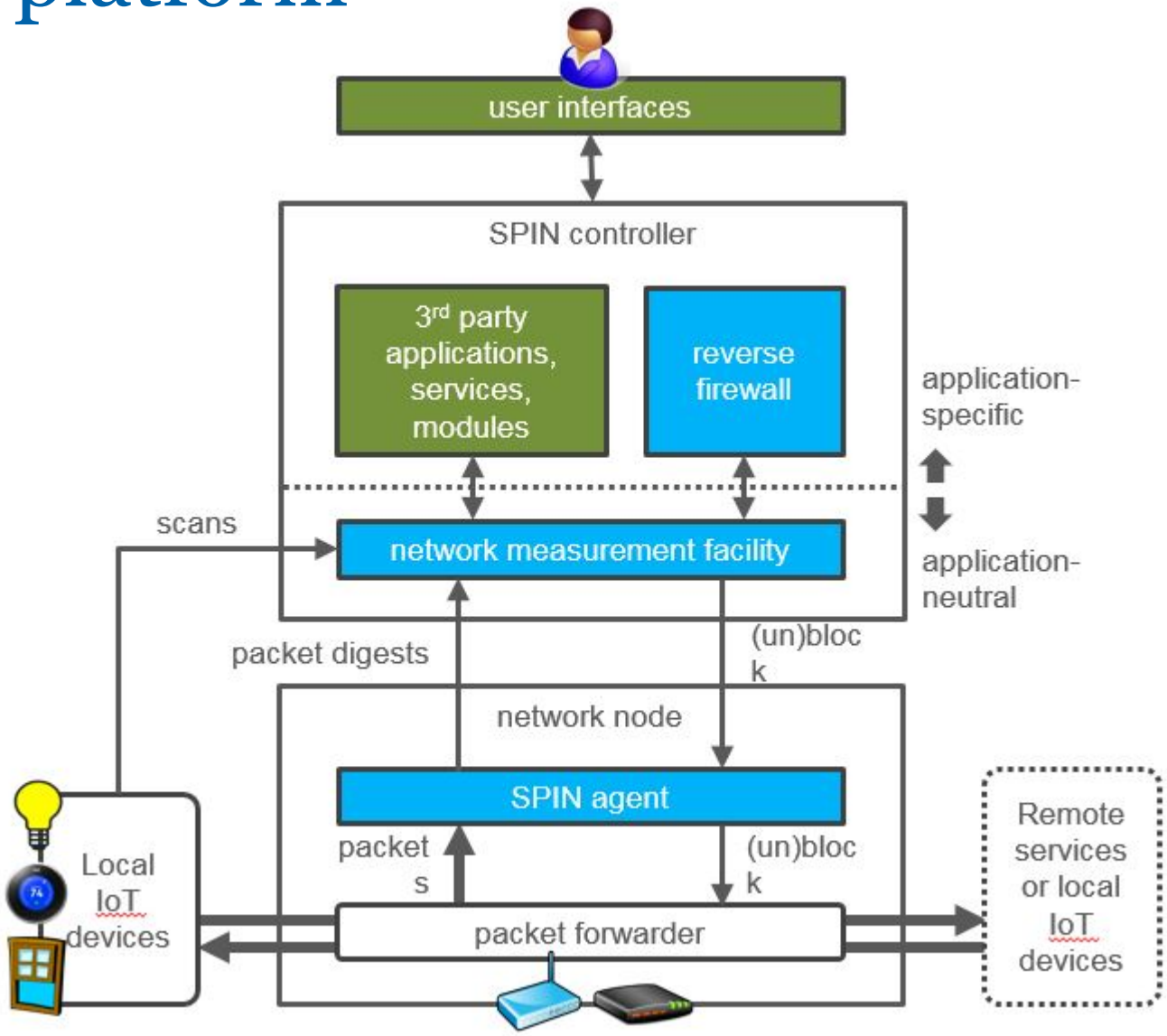
SPIN = Security and Privacy for In-home Networks



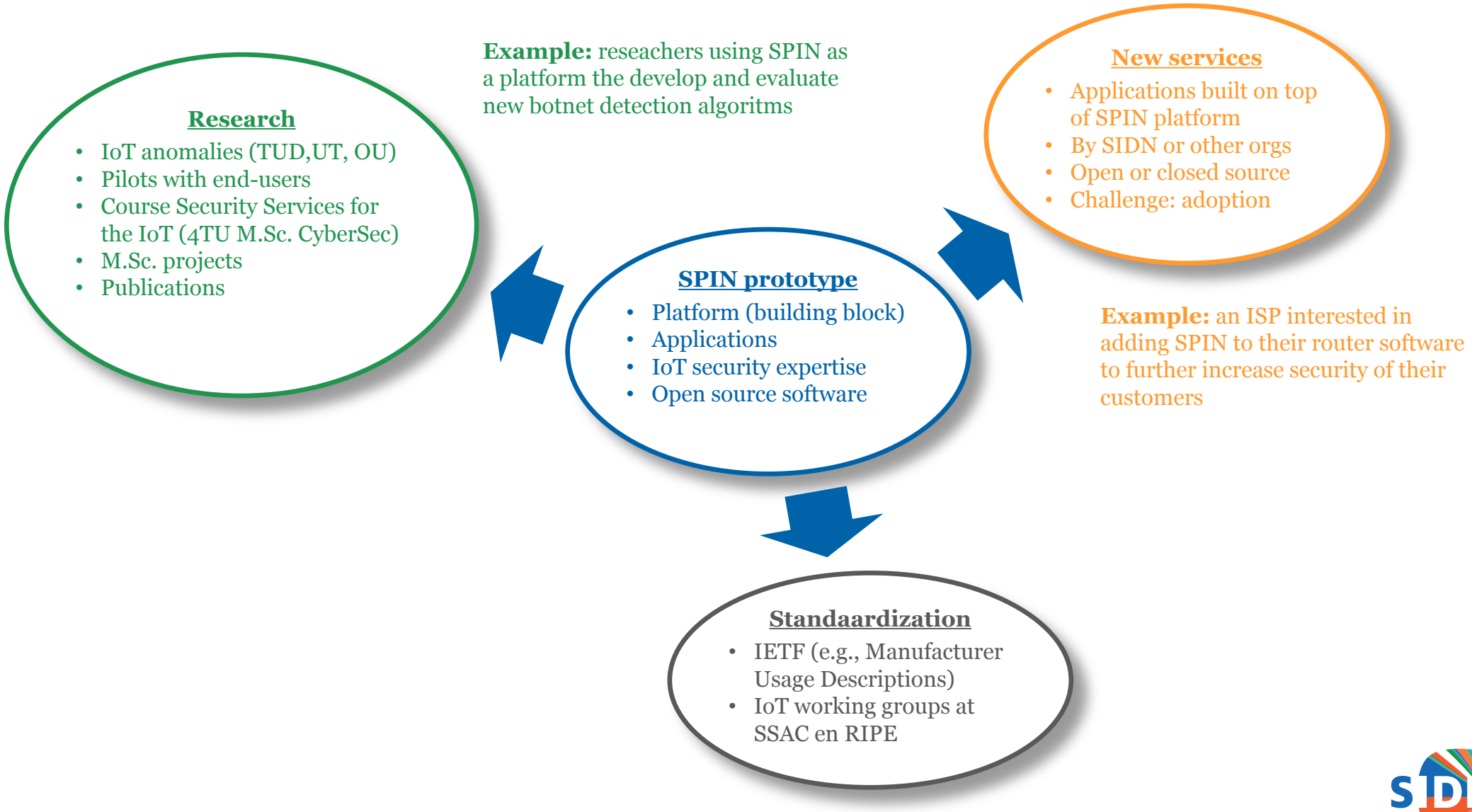
Protect the Internet/DNS (sources of DDoS attacks) and end-users
Research and prototyping

SDN LABS

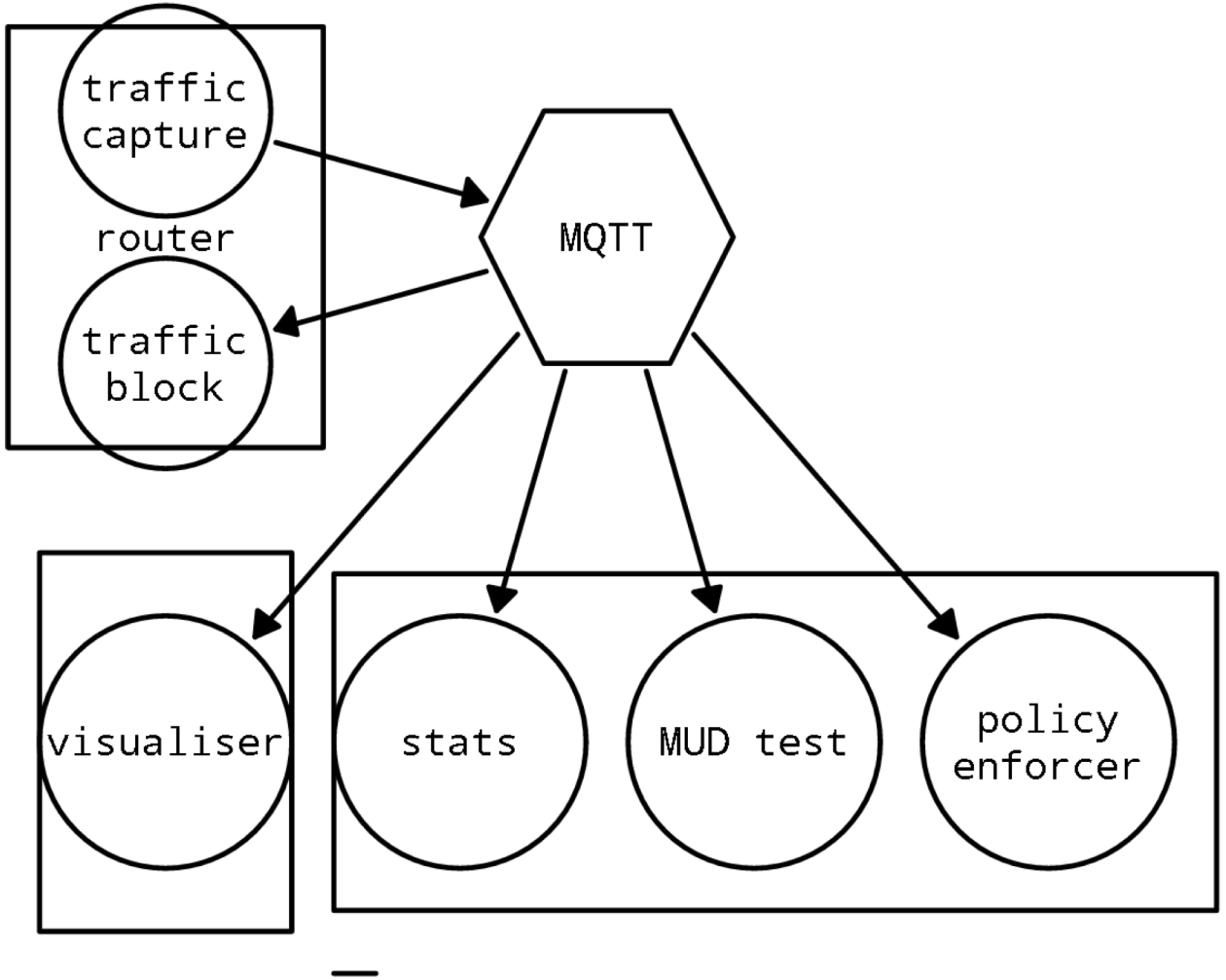
SPIN = open platform



SPIN position and targeted use



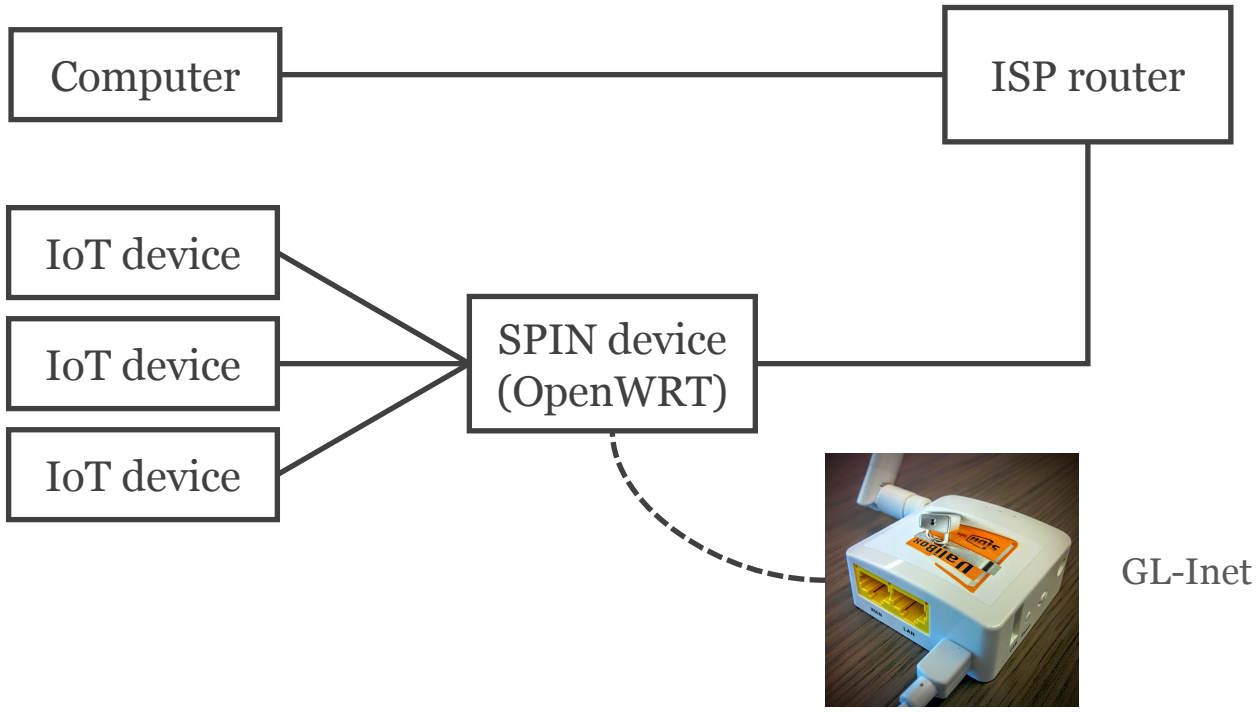
SPIN implementation (May 2018)



Prototype

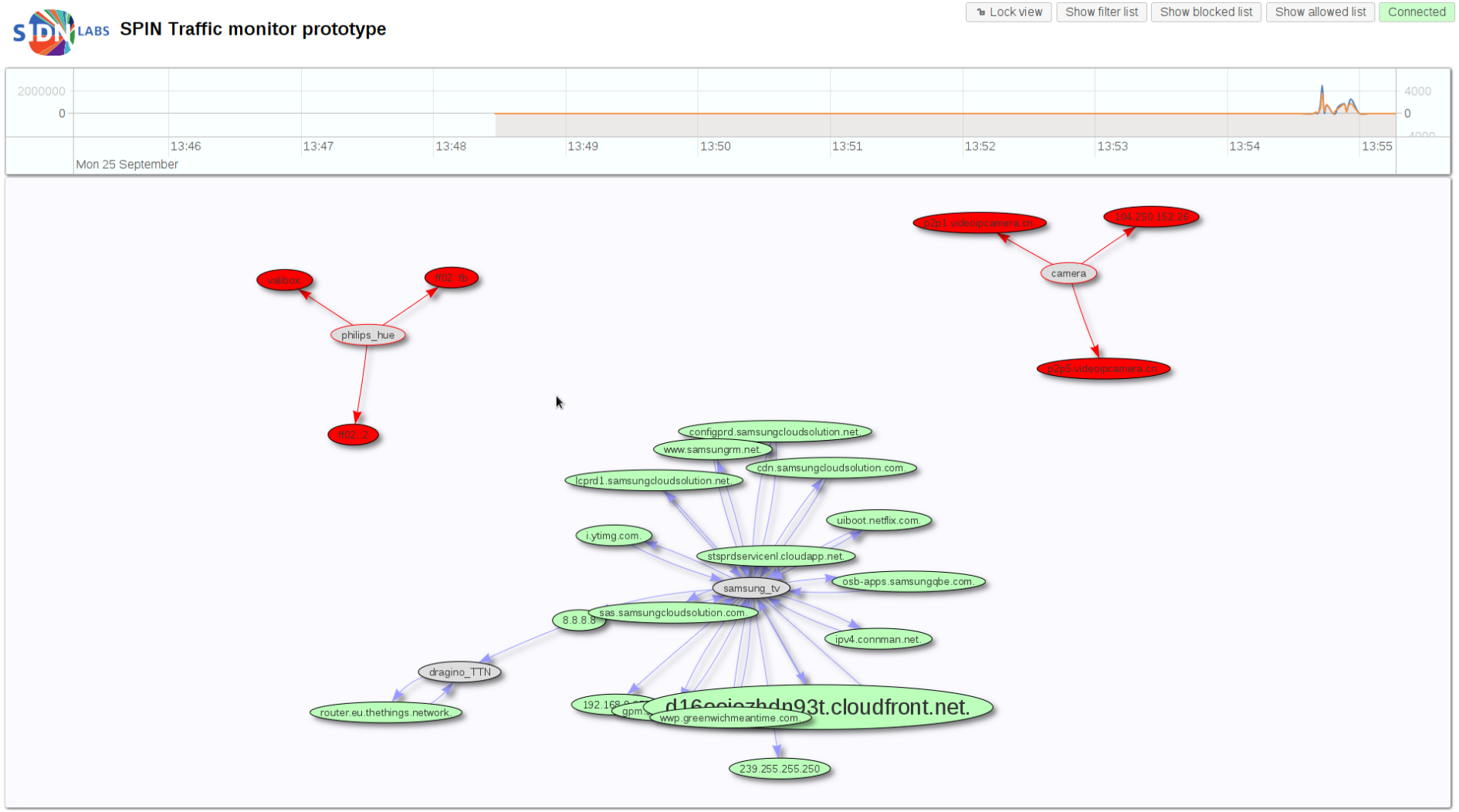
- Currently bundled with Valibox: http://valibox.sidnlabs.nl

- Source at https://github.com/SIDN/spin

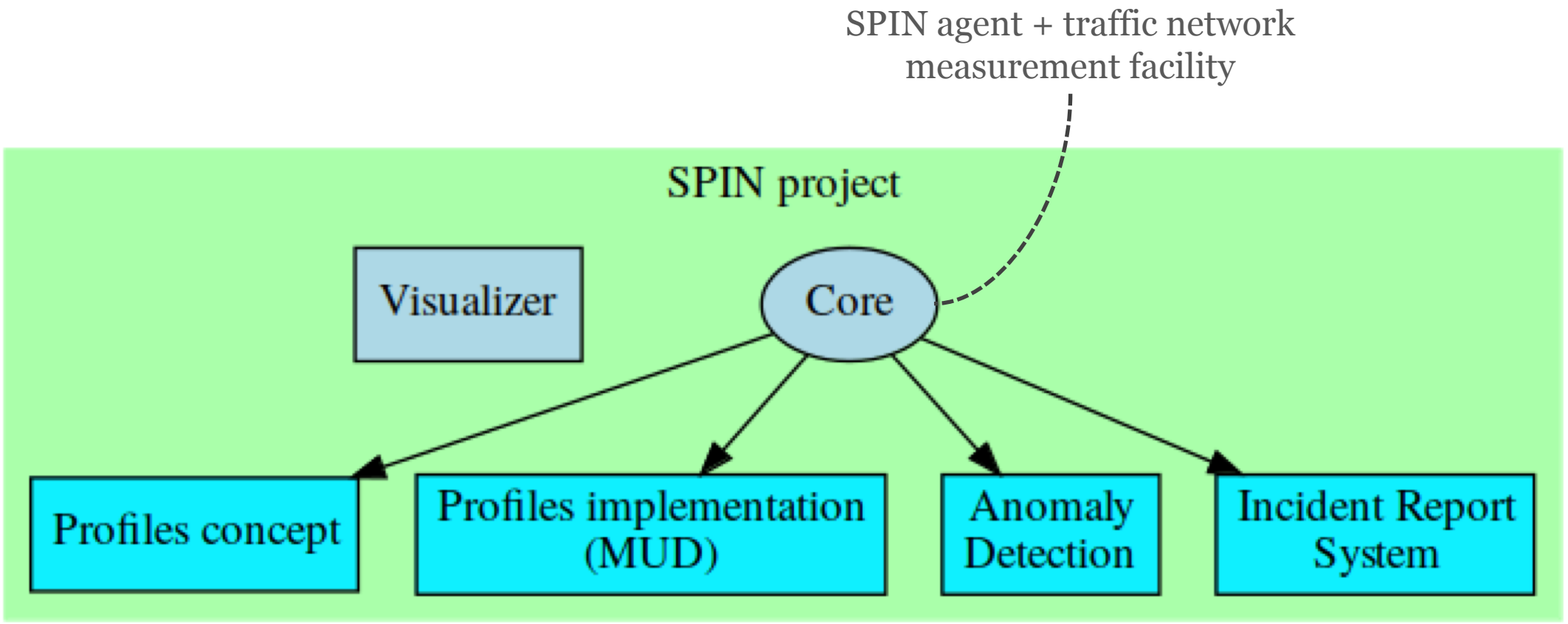


GL-Inet hardware

SPIN privacy manager (a.k.a “visualizer”)



Ongoing work



Anomaly detection

- Status: “anomaly detector” fires if a device scans more than X addresses-port combinations in Y seconds and then blocks the device
- Goal: provide framework that enables researchers and 3rd parties to plug in anomaly detectors + include one or two examples
- Model and analyze traffic, and create and test anomaly detection approaches
- Status: early implementation in Go, live stream of data available over MQTT, historic data in (local) database

SIDN LABS

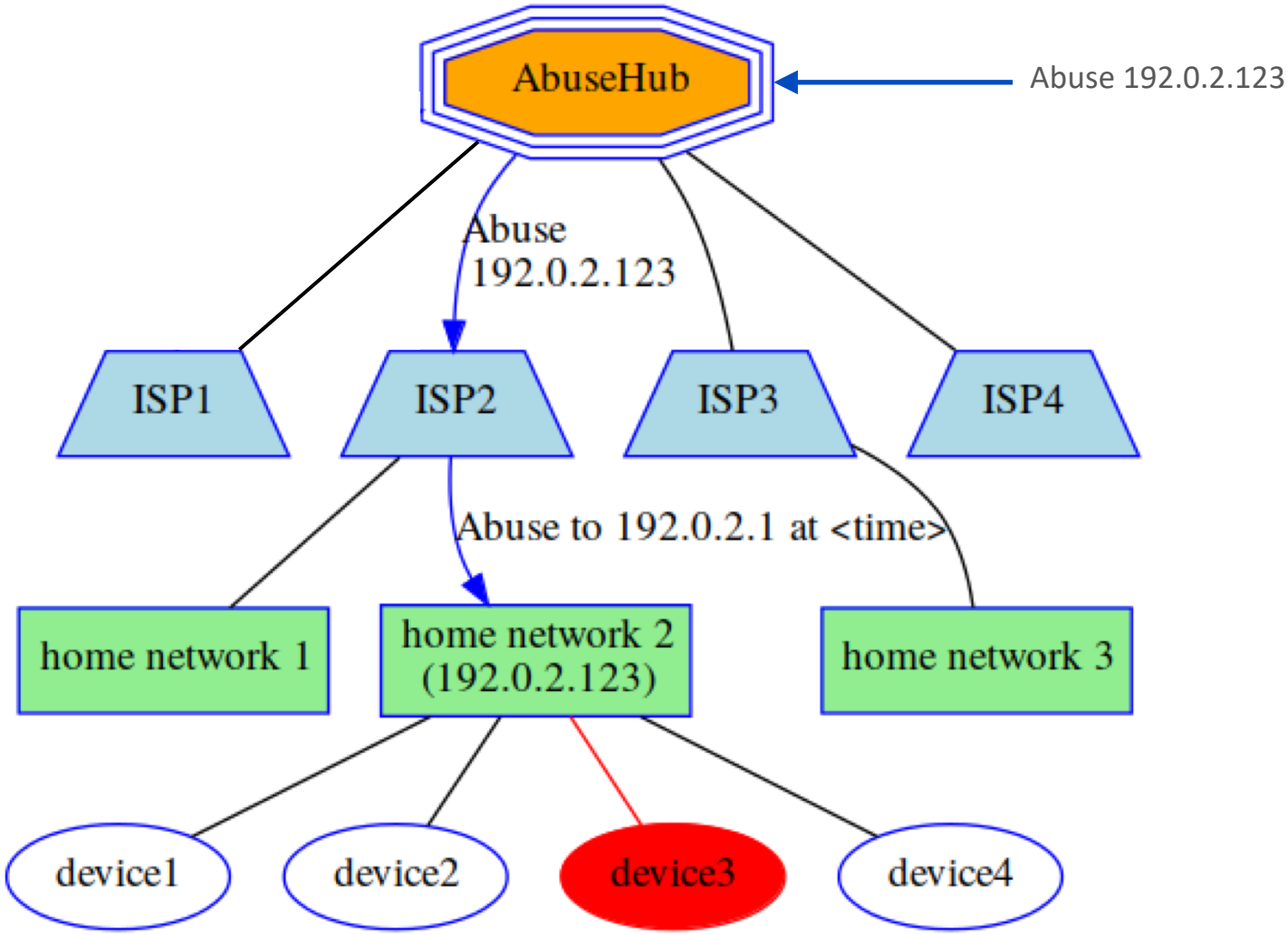
MUD profiles

- Manufacturer Usage Description (MUD), IETF Internet Draft
- JSON description of internet traffic that is or is not allowed from and to the device
- Translates almost directly to firewall rules
- Our work: automatic generation and extensions (e.g., add a bandwidth limitation or enable user-enriched profiles)

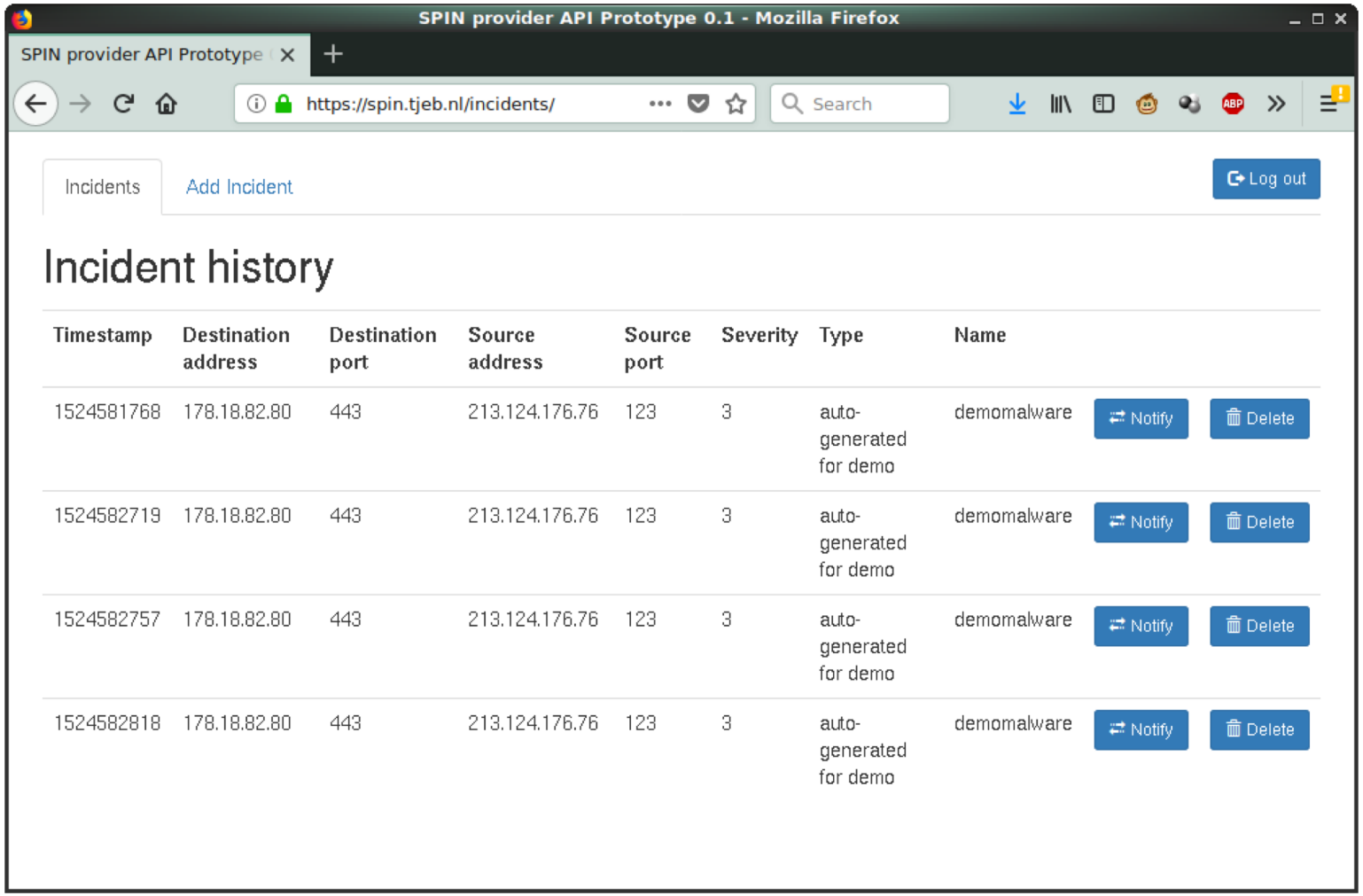
```
"ietf-mud:mud": {
  "mud-version": 1,
  "mud-url": "https://lighting.example.com/lightbulb2000",
  "last-update": "2018-03-02T11:20:51+01:00",
  "cache-validity": 48,
  "is-supported": true,
  "systeminfo": "The BMS Example Lightbulb",
}
...
"name": "mud-76100-v6fr",
"type": "ipv6-acl-type",
"aces": {
  "ace": [
    {
      "name": "cl0-frdev",
      "matches": {
        "ipv6": {
          "ietf-acldns:dst-dnsname": "test.example.com",
          "protocol": 6
        },
        "tcp": {
          "ietf-mud:direction-initiated": "from-device",
          "destination-port": {
            "operator": "eq",
            "port": 443
          }
        }
      },
      "actions": {
        "forwarding": "accept"
      }
    }
  ]
}
```

Allow outbound TCP traffic from lightbulb to port 443

Incident reporting system



Running prototype (v0.1)



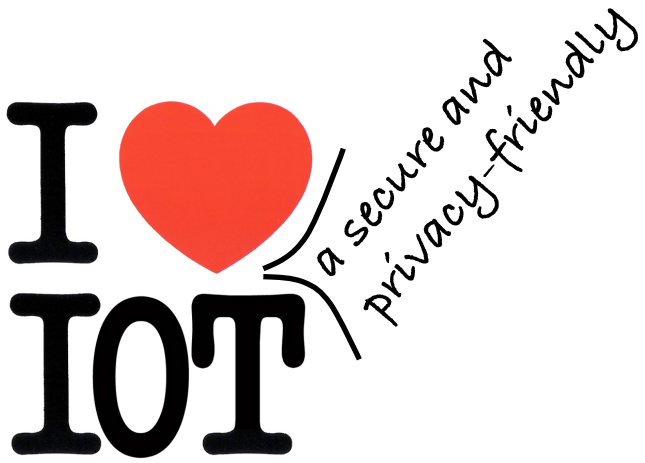
Summary

- Open platform for IoT security in homenets for researchers and developers
- Aims to protect the Internet and end-users
- Key challenge: maximize deployment
- Work ahead: pilot, extend prototype, IETF, talk to ISPs/manufacturers

SIDN LABS

Potential legal-tech talking points

- Implications of temporarily limiting traffic to and from IoT devices
- Implications of fine-grained filtering vs. quarantining homenets as a whole
- Sharing security info (e.g., DDoS fingerprints) with SPIN devices
- Gathering (partial) DDoS fingerprints at SPIN devices
- Perhaps enough substance for a follow-up project?



Questions and discussion

Cristian Hesselman | Head of SIDN Labs
+31 6 25 07 87 33 | cristian.hesselman@sidn.nl | @hesselma

SIDN LABS