Mitigation of IoT-based DDoS attacks

Cristian Hesselman

APTLD76 | Iskander Puteri, Malasya | Sep 5, 2019

Operator of the .nl TLD

- *Stichting Internet Domeinregistratie Nederland* (SIDN)
  - Manage fault-tolerant and distributed DNS and registration infrastructure for .nl
  - Increase value of the Internet in the Netherlands and elsewhere

- SIDN Labs = research team (~11 FTE)
  - Advance operational security and resilience of .nl, the DNS, and the Internet through measurements and technology development
  - Research challenges: core Internet systems (including IoT security) and Internet evolution
  - Daily work: help operational teams, write open source software, analyze vast amounts of data, run experiments, write academic papers, work with universities, give presentations ☺

.nl = the Netherlands
17M inhabitants
5.8M domain names
3.1M DNSSEC-signed
1.3B DNS queries/day

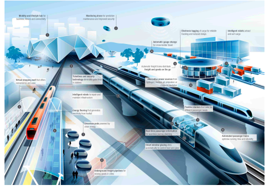
SIDN fonds

SIDN LABS

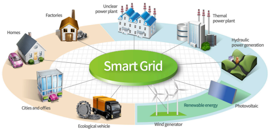
Internet of Things

- Internet application that extends “network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers” [ISOC]

- Differences with “traditional” applications [ISOC, SAC105]
  - IoT continually senses, interprets, and acts upon physical world
  - Often without user awareness or involvement (passive interaction)
  - 20-30 billion devices operating “in the background” of people’s daily lives
  - Widely heterogeneous (hardware, operating systems, network connection)
  - Longer lifetimes (perhaps decades) and unattended operation



Intelligent Transport Systems



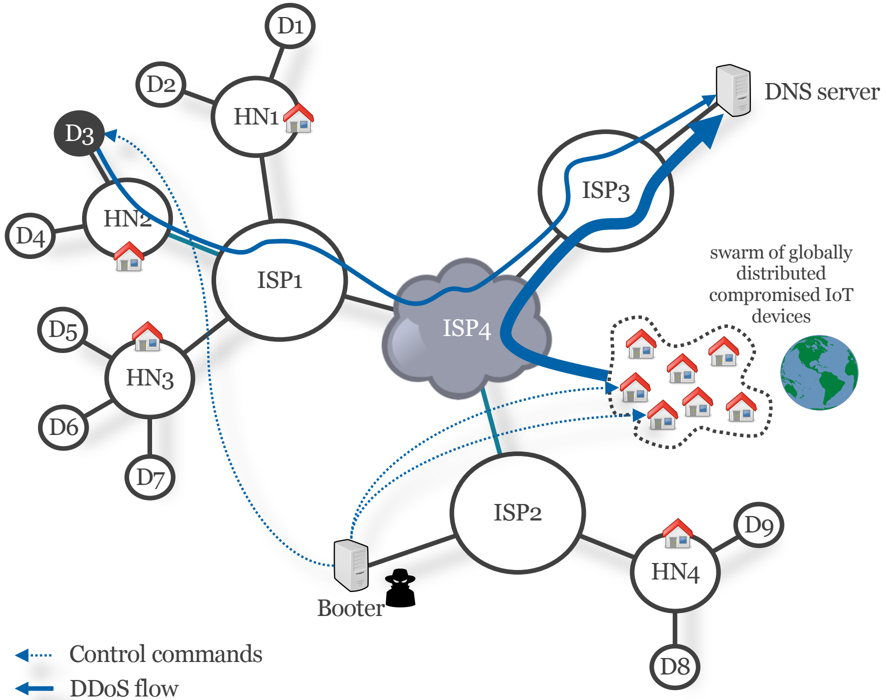
Smart energy grids

Smart homes and cities

- IoT promises a safer, smarter, and more sustainable society, but IoT security is a major challenge

[ISOC] K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things: an Overview", ISOC, Oct. 2015
[SAC105] T. April, L. Chapin, kc claffy, C. Hesselman, M. Kaeo, J. Latour, D. McPherson, D. Piscitello, R. Rasmussen, and M. Seiden, “The DNS and the Internet of Things: Opportunities, Risks, and Challenges”, SSAC report SAC105, June 2019

Cliché but relevant example: Mirai-powered DDoS attack

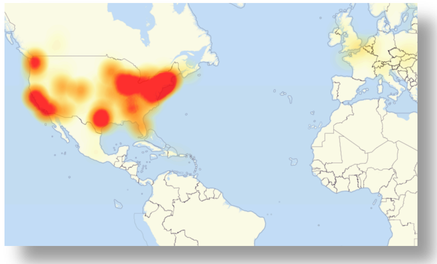


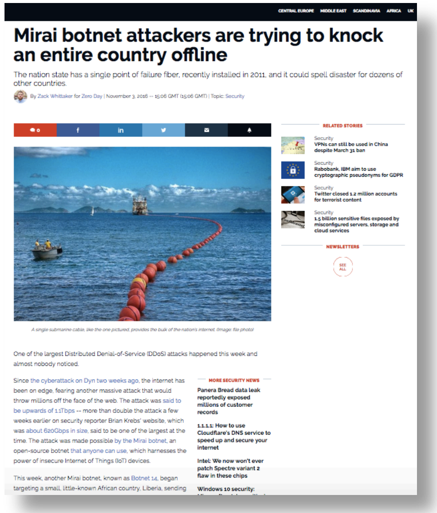
◂┈ Control commands

◀━ DDoS flow

HN = Home Network

D = IoT device





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:

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

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

IoT botnets

- DDoS traffic from large numbers of bots (Mirai 600K, Hajime 400K)
- High propagate rates (e.g., Mirai from 42K to 71K bots in 1 hour)
- Complex traffic (e.g., bot churn, volumetric/TCP state exhaustion)
- Easy to launch through booters/stressers (Mirai)
- Reflection attacks (e.g., Mirai and Reaper botnets)
- Difficult to clean infected devices (e.g., deployment of fixes, device heterogeneity)

Further reading:

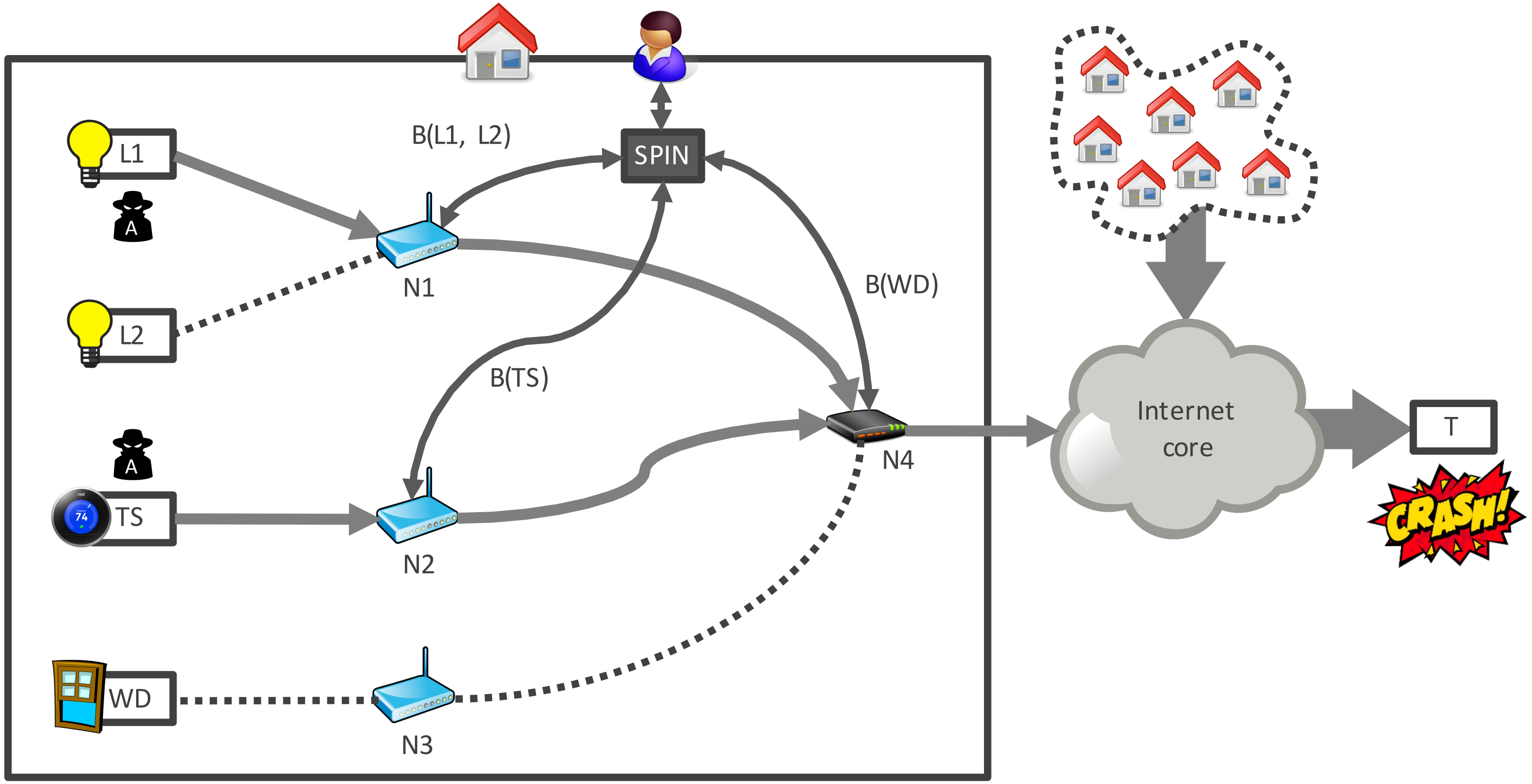
- M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z., Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the Mirai Botnet”, 26th USENIX Security Symposium, 2017
- S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, “Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet”, Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA, February 2019
- T. April, L. Chapin, kc claffy, C. Hesselman, M. Kaeo, J. Latour, D. McPherson, D. Piscitello, R. Rasmussen, and M. Seiden, “The DNS and the Internet of Things: Opportunities, Risks, and Challenges”, SSAC report SAC105, June 2019

IoT security is a “multi-stakeholder” challenge

What	Examples of mechanisms
Empower users	• Validate security state of devices • “Explainable security” for IoT products (e.g., security levels A-F) • Support services that help users cleaning their devices
Secure IoT devices	• Train IoT engineers on Internet security (and Internet engineers on IoT) • Open source security libraries for IoT operating systems • Behavior specifications (e.g., MUD) • Support for remote attestation
Security intelligence in edge networks	• Anomaly detection and intelligent quarantining • Deployment through integration in CPEs • Interaction with abuse handling processes • Examples: SPIN, CIRA’s SHGW, Heimdall
Sharing security information	• DDoS fingerprints and IoT botnet characteristics • Proven traffic filtering rules • Examples: DDoS clearing house, 3DCOP, autoreporter, AbuseHUB
DDoS handling	• Share mitigation capacity across operators
Regulation	• Reduce regulatory uncertainty (e.g., for automated f/w updates) [Silva]

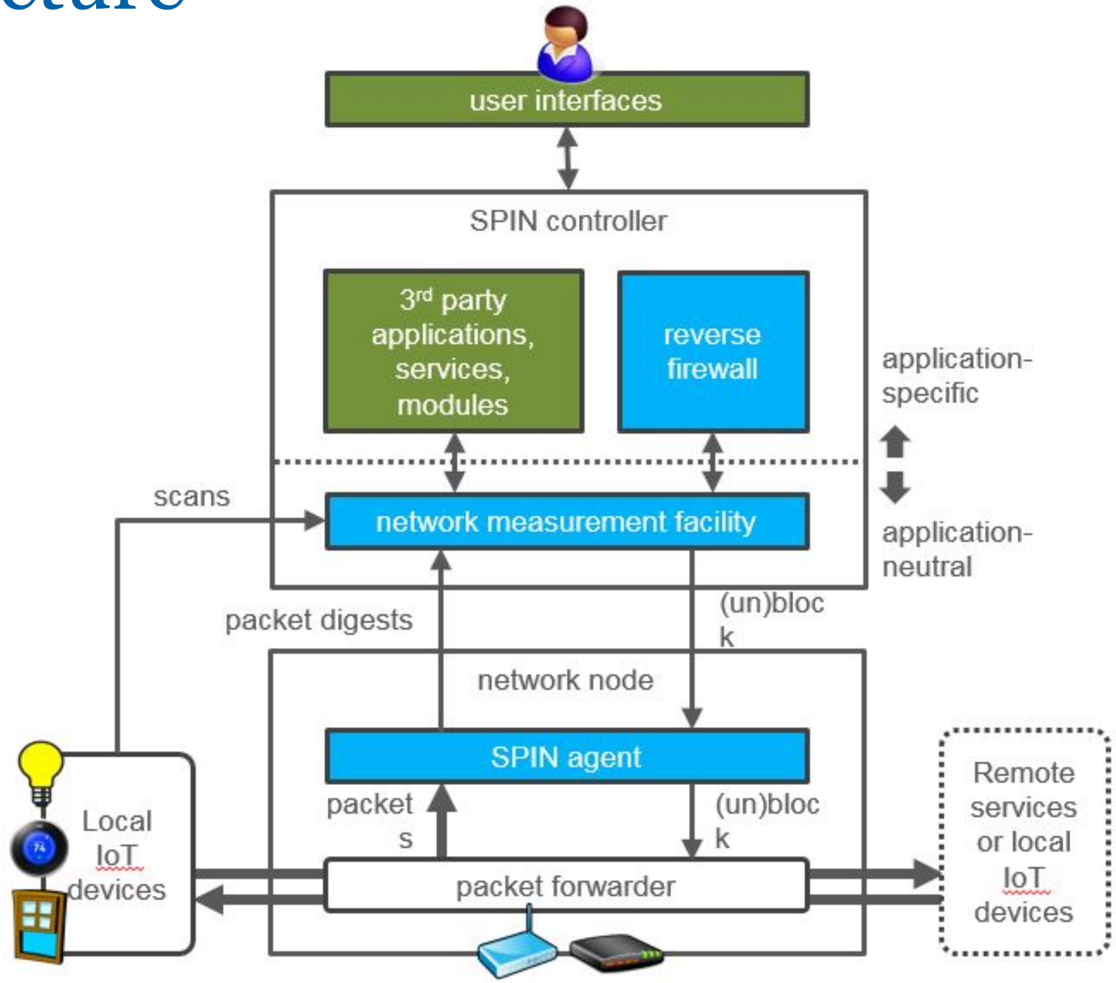
[Silva] K. e Silva, “Mitigating botnets: Regulatory solutions for industry intervention in large-scale cybercrime”, Ph.D. thesis (submitted), Tilburg University, the Netherlands

Security and Privacy for In-home Networks (SPIN)

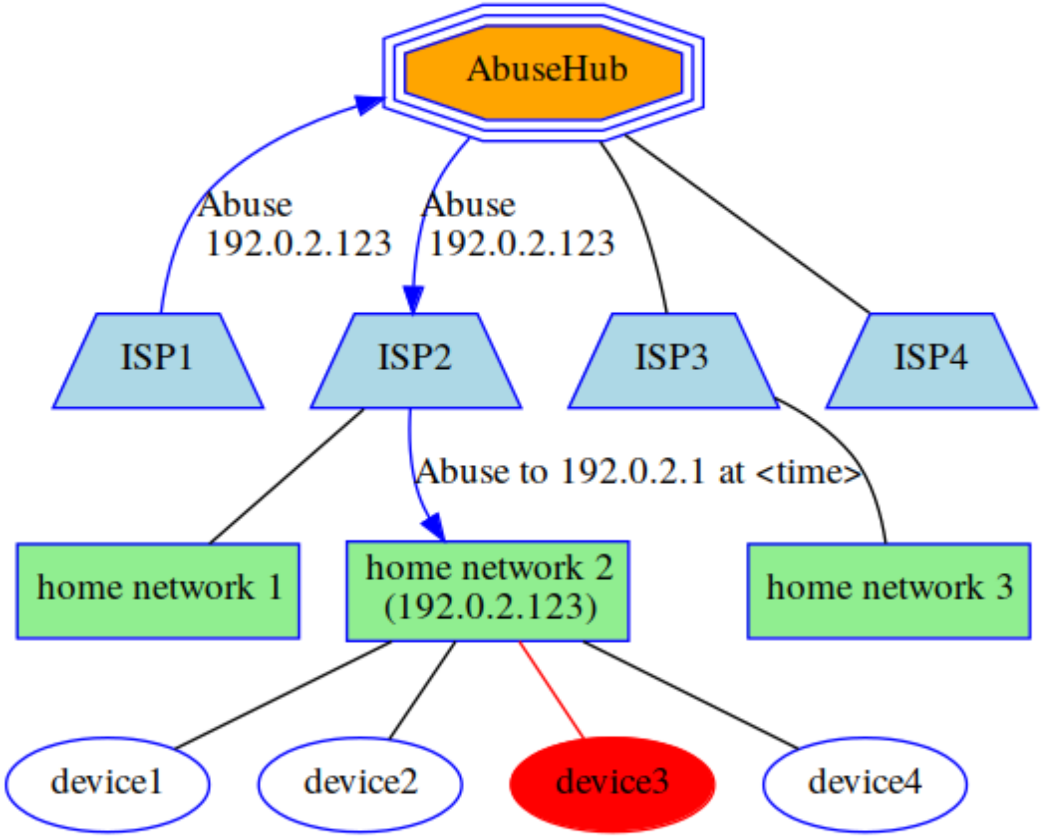


https://www.sidnlabs.nl/a/weblog/redesigning-spin-to-a-reference-platform-for-secure-and-privacy-enabled-iot-home-networks?language_id=2

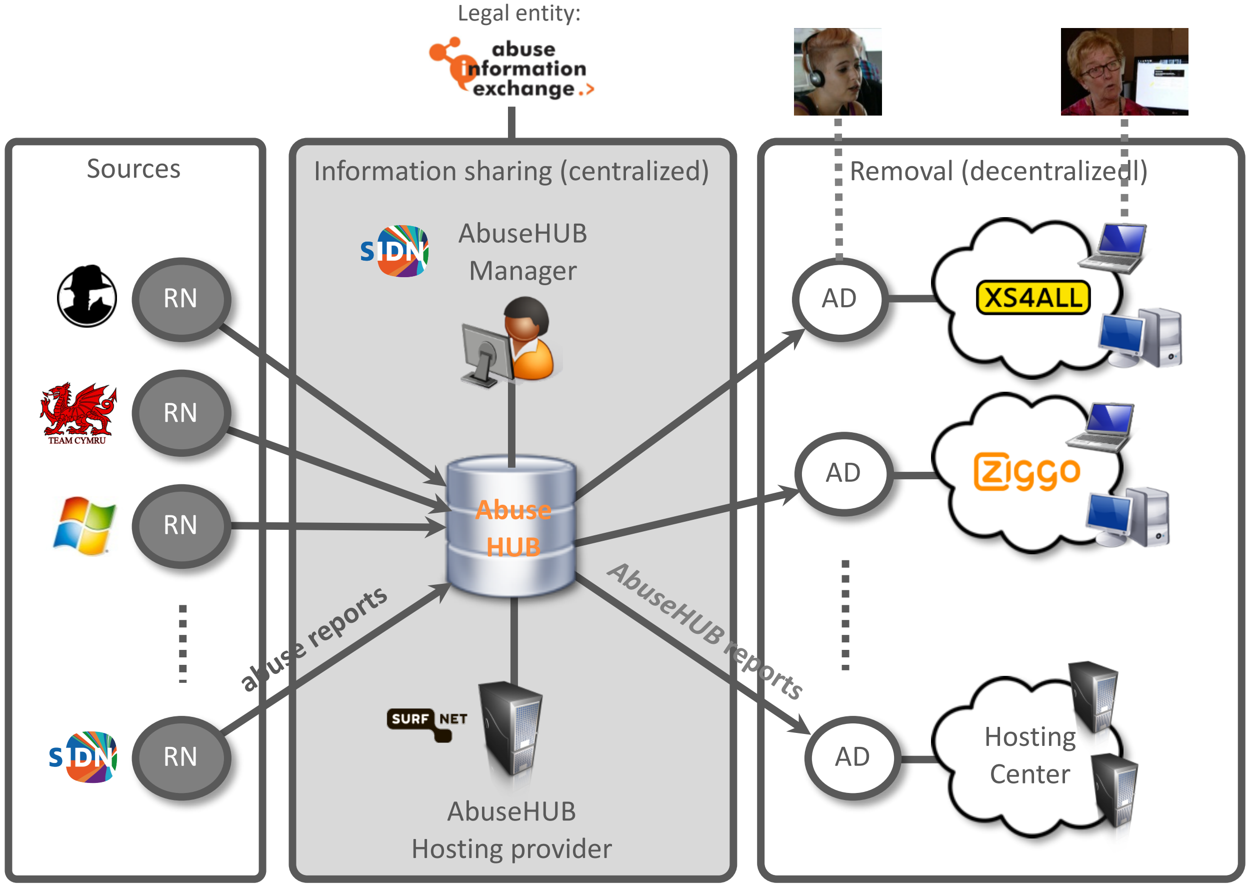
SPIN architecture



Incident report system (under development)



Botnet info sharing (since 2014)



ABUSEIO

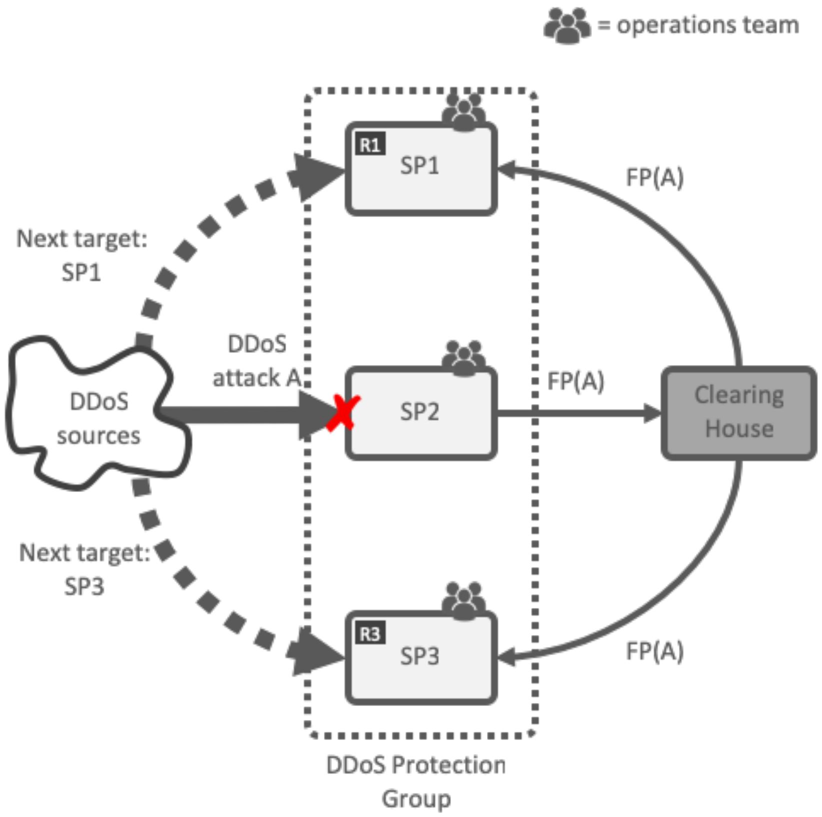
Open Source abuse management

SIDN LABS

Netherlands’ national DDoS clearing house

WORK IN PROGRESS

- Continuous and automatic sharing of “DDoS fingerprints” buys providers time (proactive)
- Extends DDoS protection services of critical service providers, does not replace them
- Improves attribution, allowing for better prosecution and increased deterrent effects
- Open to all critical providers in the Netherlands (Internet, financial, energy, water, etc.)

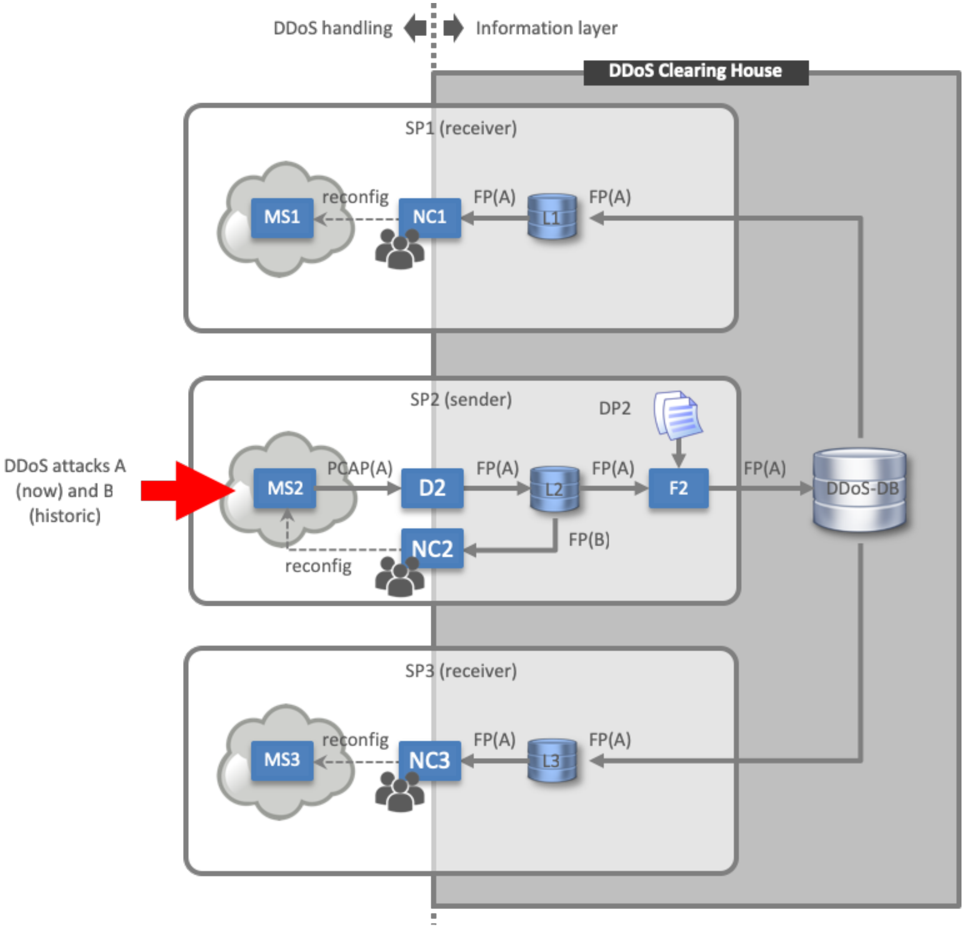


SIDN LABS

Clearing house architecture (draft)

- Joint effort of NBIP-NaWas, KPN, THTC, NCSC-NL, Dutch Payment Association, VodafoneZiggo, NL-ix, SIDN, SURF, and the University of Twente

- Scale up to a European level through CONCORDIA, research project partly funded through the EU's Horizon 2020 Research and Innovation program



My position

- IoT will bring us lots of new services that will improve ease of life, make society more sustainable, safer, smarter

- **But** we'll need a broad range of measures from different parties to mitigate DDoS attacks, such as
  - Information sharing (e.g., AbuseHUB-like) and edge security systems (e.g., SPIN-like)
  - Security libraries for IoT operating systems (e.g., for privilege management)
  - Internet security awareness in the IoT industry (and vise versa)
  - Regulatory instruments (e.g., guidance when automated firmware updates are lawful)
  - Consumer awareness and communication ("explainable security")

- Technology alone is not the answer!

Volg ons

.nl SIDN.nl

@SIDN

in SIDN

Q&A

www.sidnlabs.nl | stats.sidnlabs.nl

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

The work of SIDN, SURFnet, and the University of Twente on the DDoS clearing house was partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927.