The DNS and the IoT: security and stability opportunities, risks, and challenges (for ccTLDs)

Cristian Hesselman (.nl and SSAC)
Jacques Latour (.ca and SSAC)

ICANN66
Montréal, Canada
Tue Nov 5, 2019

cira

SIDN LABS

Today's goals

- Provide an overview of interplay between IoT and DNS ecosystems and opportunities, risks, and challenges in terms of DNS security and stability
- Provide a few examples of ccTLD activities (.nl and .ca)
- Trigger and facilitate dialogue in the ccTLD community
- Motivation: overlapping IoT work in SSAC (SAC105) and ccTLDs and strategic issue

cira

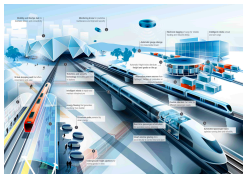
SIDN LABS

Internet of Things

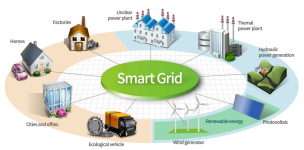
- Internet application that extends "network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers" (ISOC)

- Differences with "traditional" applications
  - IoT continually senses, interprets, acts upon physical world
  - Without user awareness or involvement (passive interaction)
  - 20-30B devices "in the background" of people's daily lives
  - Widely heterogeneous (hardware, OS, network connections)
  - Longer lifetimes (perhaps decades) and unattended operation

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



Intelligent Transport Systems

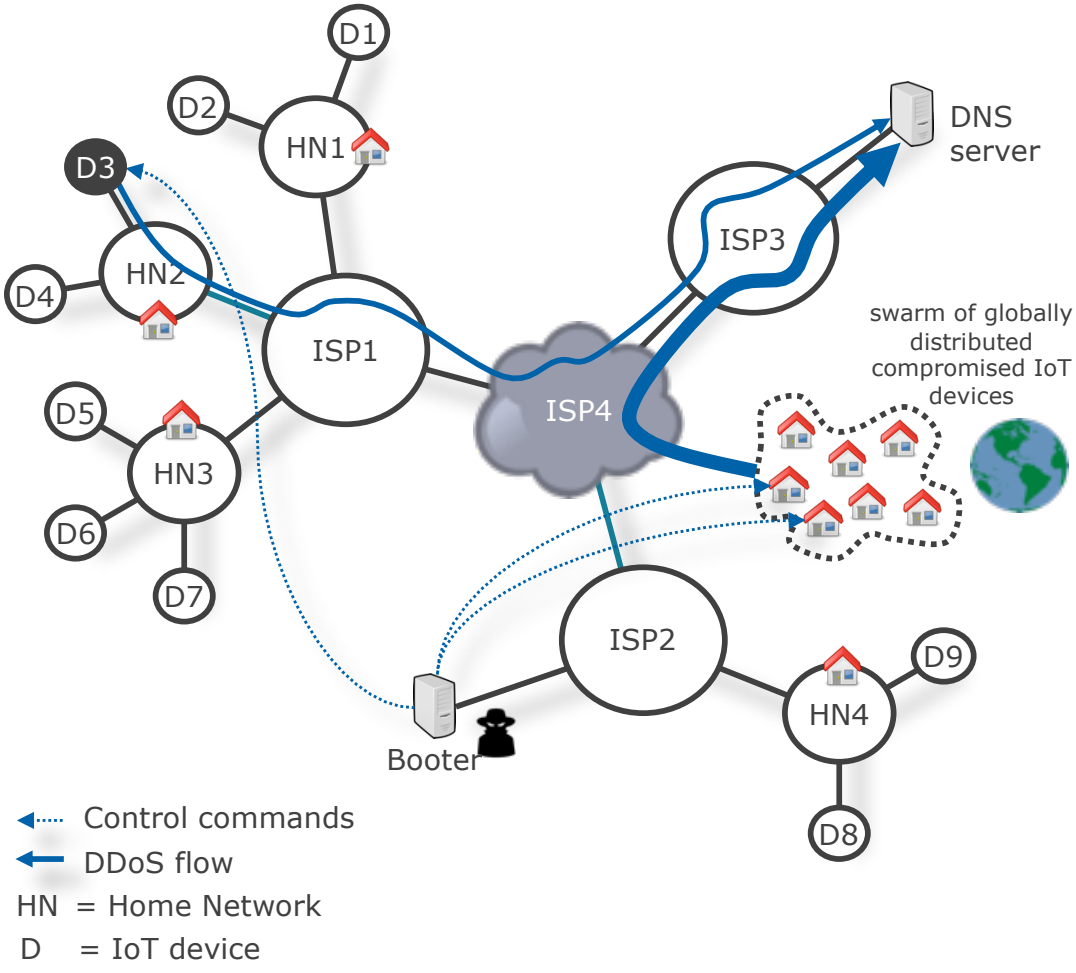


Smart energy grids

Smart homes and cities

Sources: [ISOC15], [SAC105]

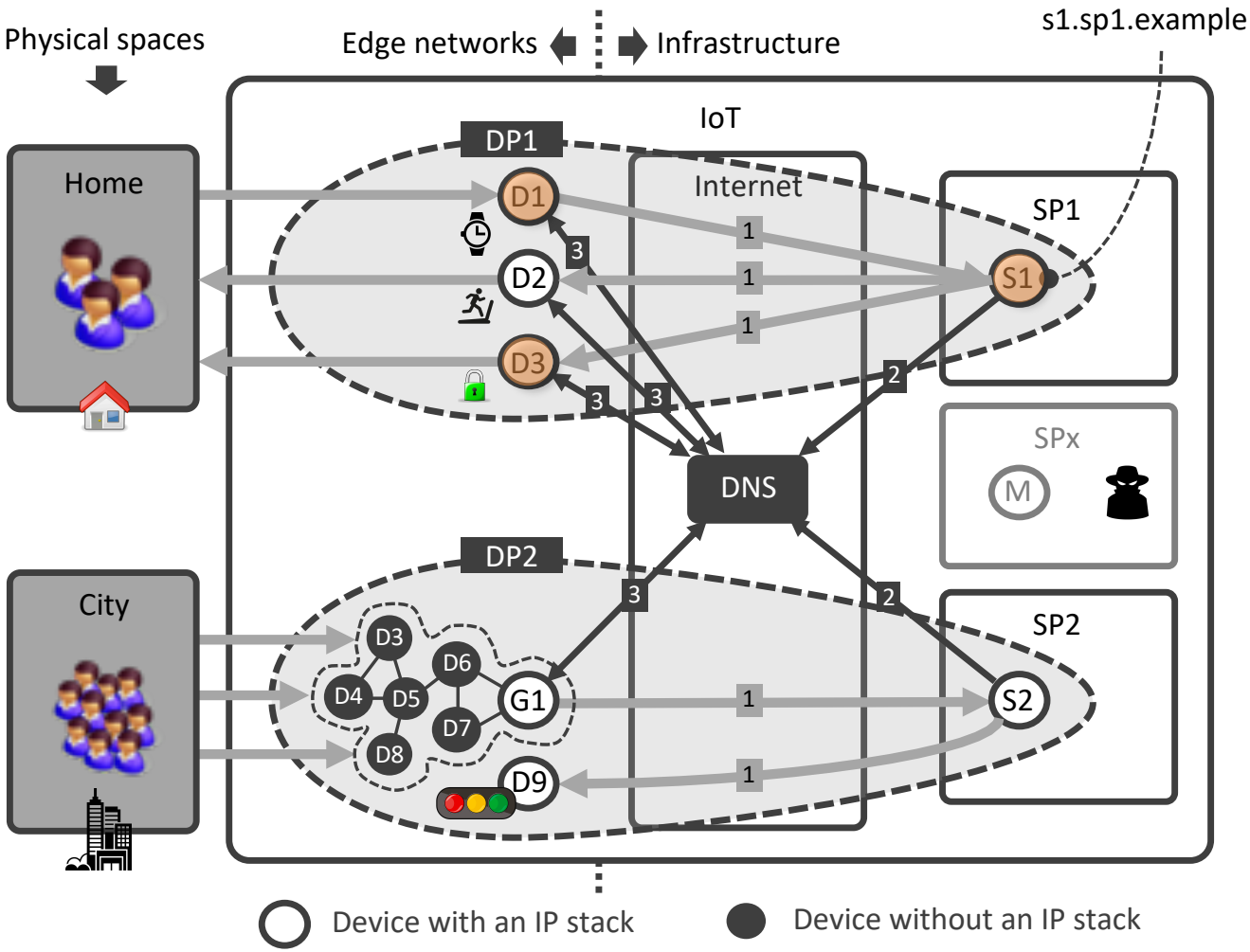
IoT wakeup call for ccTLDs and other operators: Mirai-powered DDoS attacks



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://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

The IoT and the DNS: interacting and co-evolving ecosystems



Sources: [SAC105]

SAC105 opportunities: DNS helps protecting the real world

- Avoid redirections
  - Devices being redirected to malicious resolvers (DoH/DoT) or remote services (using DNSSEC)
  - Protect against (advanced) hijacks of domain names that IoT devices use (using MFA)

- More control over information that IoT devices share
  - Reduce information devices reveal about themselves, such as sense-in.hello.is (using DoH/DoT)
  - Protect user privacy for devices with highly specific tasks, such as a sleep monitor (using DoH/DoT)
  - Visualize services and resolvers IoT devices interact with (using their DNS queries)

SAC105 risks to the DNS from the IoT

- 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

cira SIDN LABS

SAC105 challenges for DNS and IoT industries

- 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

cira

SIDN LABS

Other challenges (in addition to SSAC105)

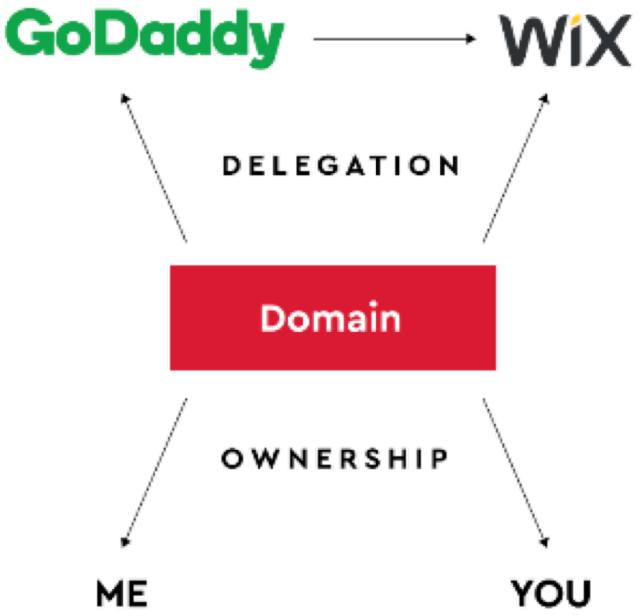
- Empower users
  - ”Explainable security” for IoT products (e.g., levels A-F)
  - Support services that help users cleaning their devices
- Secure IoT devices
  - Traffic obfuscation
  - Support for remote (hardware-based) attestation
- Edge IoT security systems
  - Anomaly detection and intelligent quarantining
  - Deployment through integration in CPEs
  - Interaction with abuse handling processes (e.g., at ISPs)
- Standardization and regulation
  - Interoperable home security systems, baseline security
  - Reduce regulatory uncertainty [eSilva19]

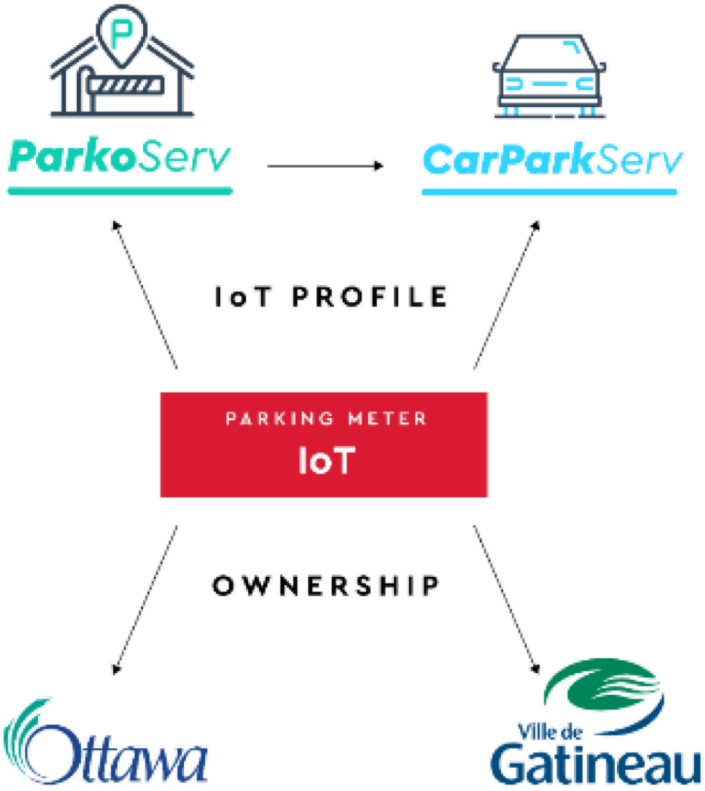
The IoT and the DNS @ .ca

cira

SIDN LABS

Similarity between domain names and (mobile) IoT devices

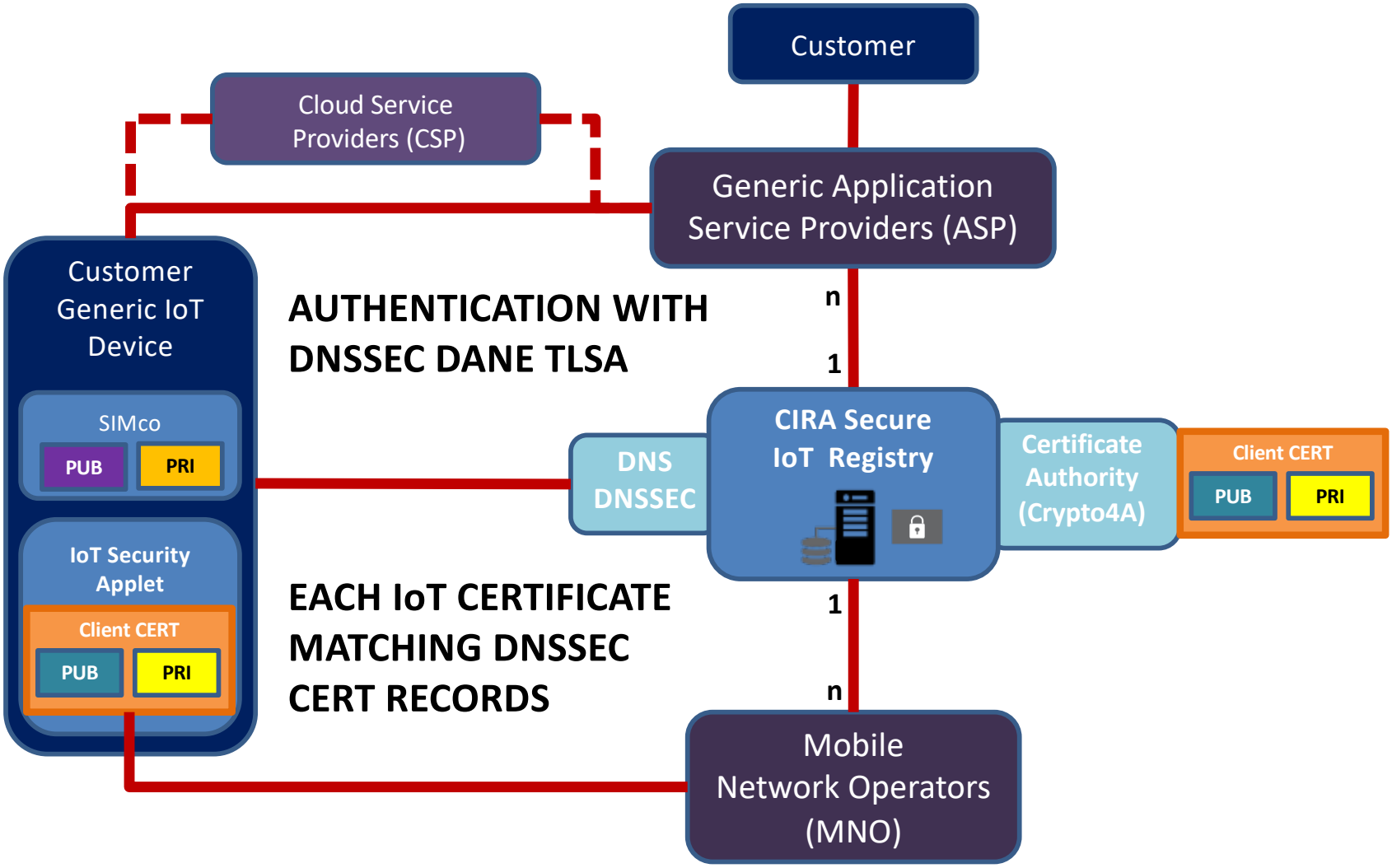




cira

SIDN LABS

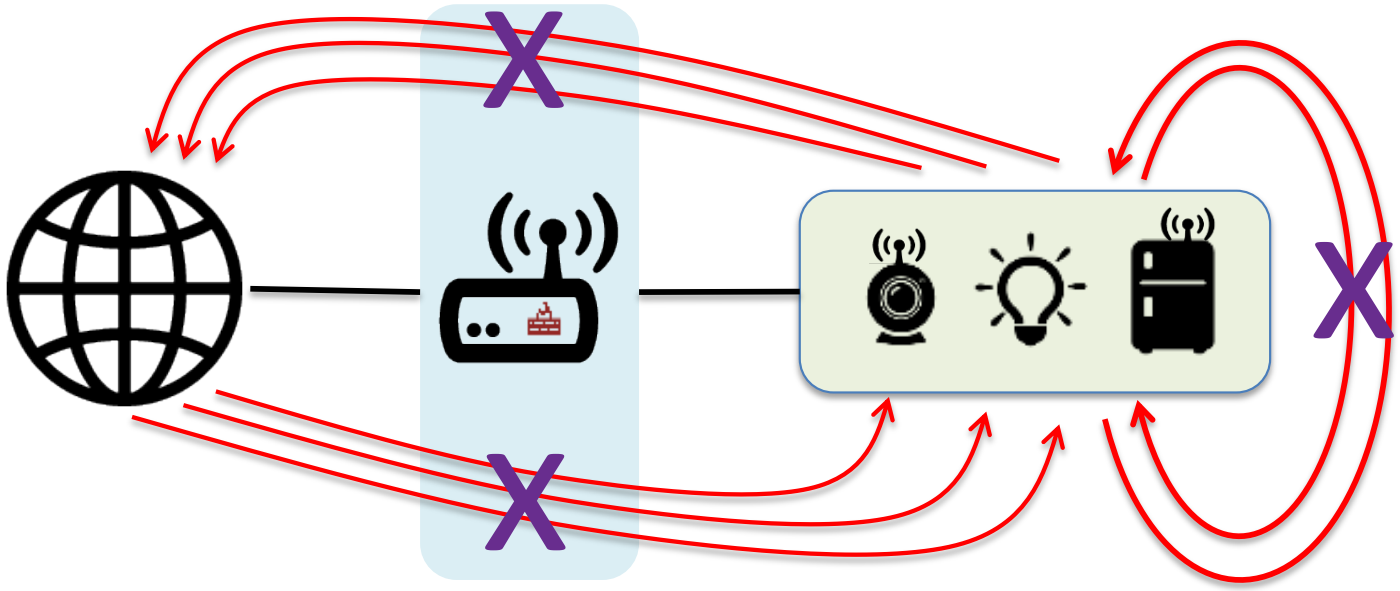
The DNS/DNSSSEC as the new root of trust



Secure IoT Registry Ecosystem

Secure home gateway (SHG)

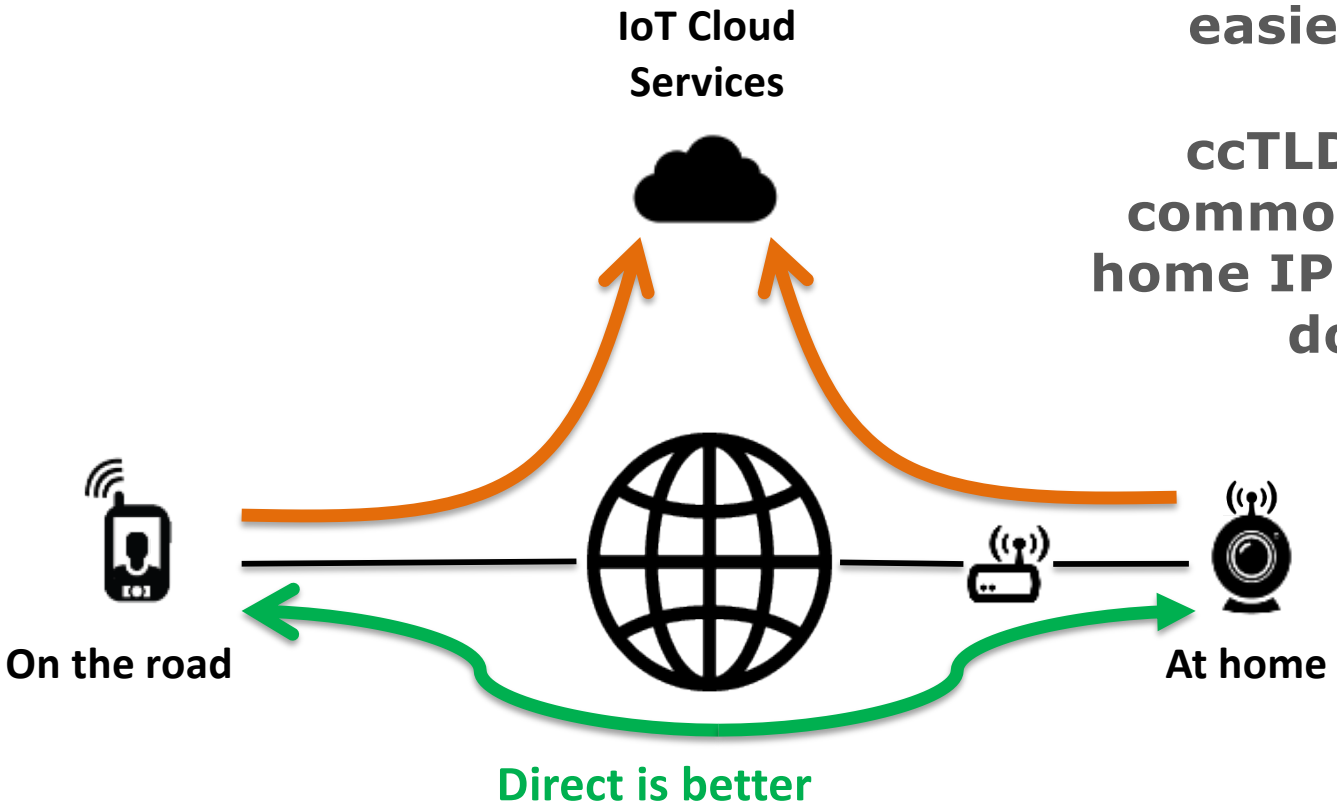
Protect the internet from IoT devices **attacks**



Protect IoT devices from internet **attacks**

Protect IoT devices from internal **attacks**

IoT vendors are creating dependency on cloud architecture



Having a domain name per home gateways makes remote access possible, easier, more secure.

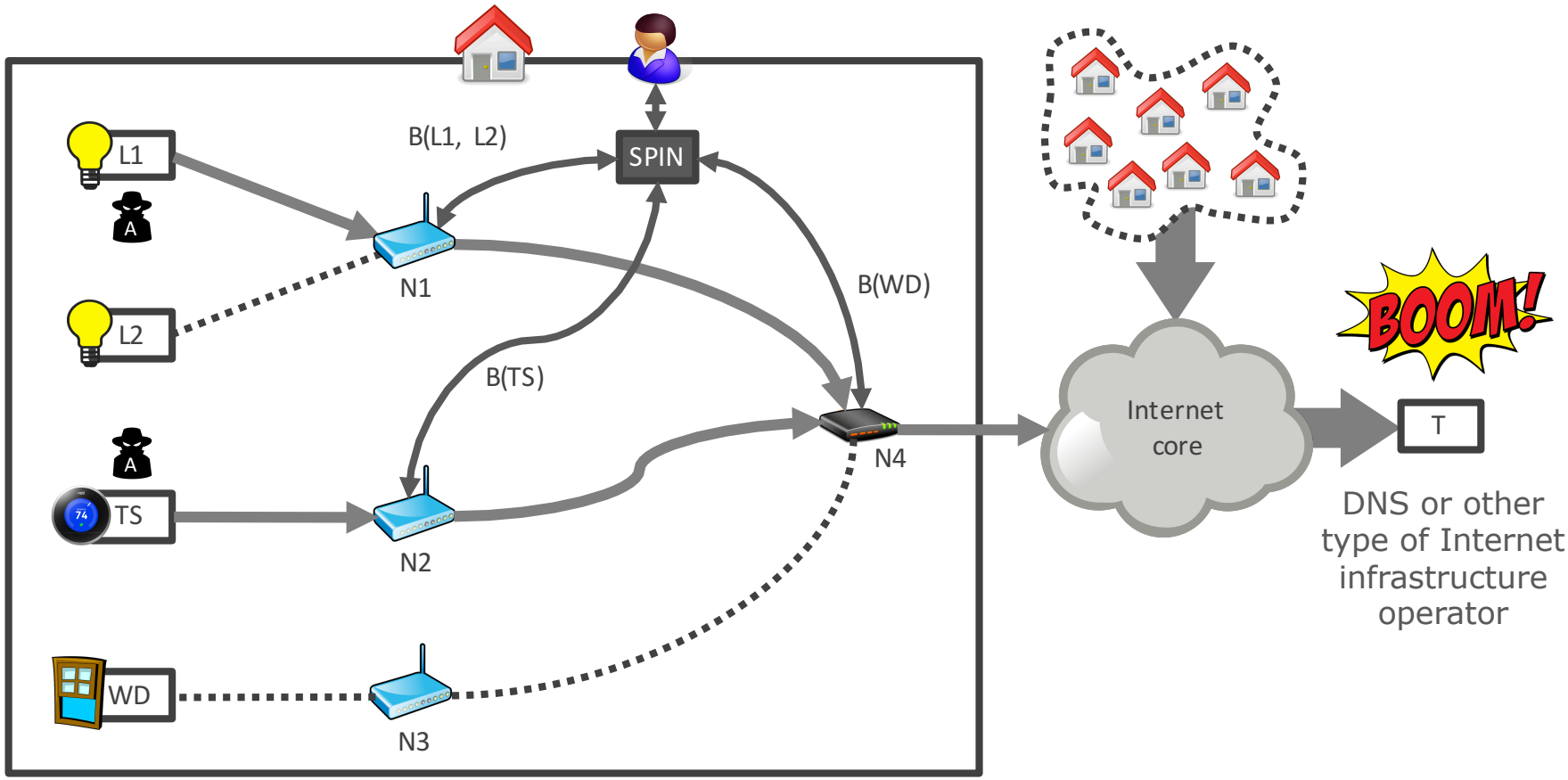
ccTLD should build a common system to track home IP addresses to their domain name

The IoT and the DNS @ .nl

cira

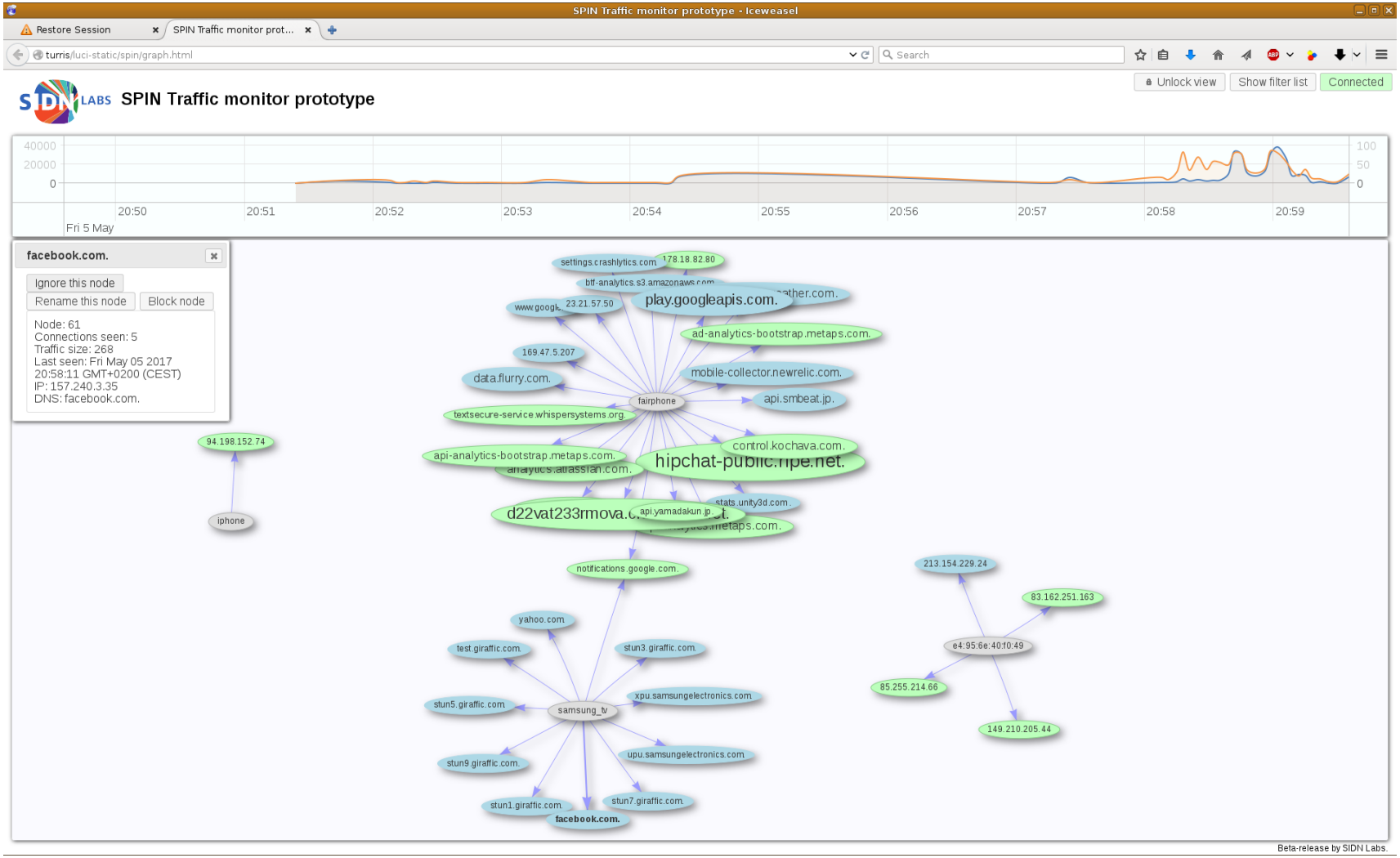
SIDN LABS

Fine-grained blocking of vulnerable IoT devices through SPIN



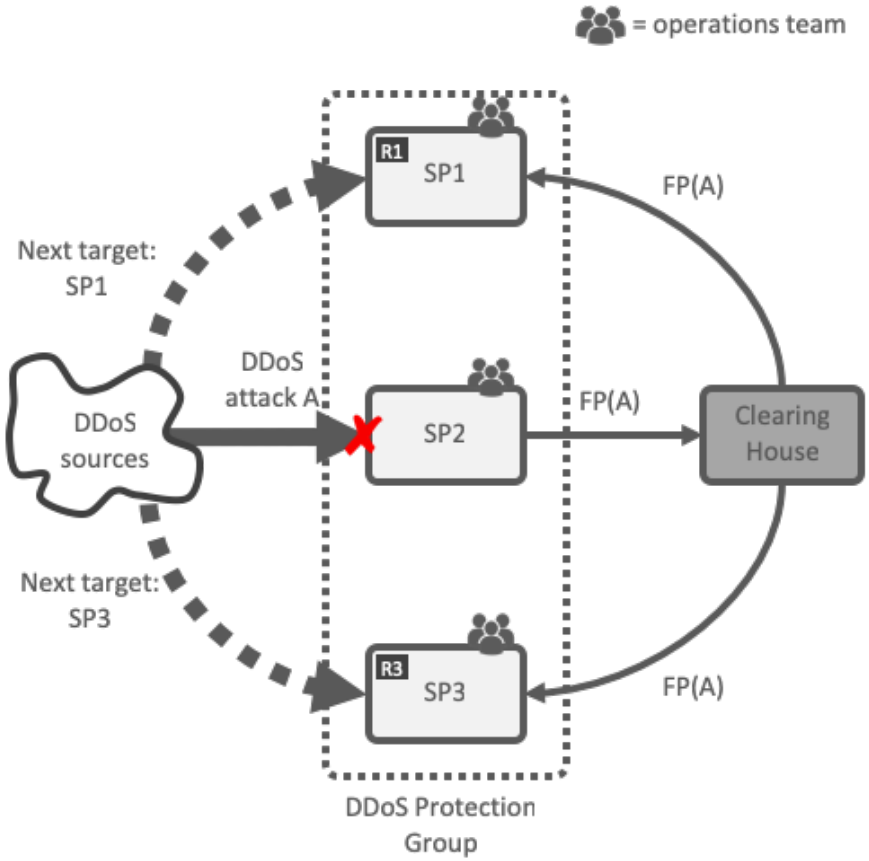
https://www.sidnlabs.nl/a/weblog/redesigning-spin-to-a-reference-platform-for-secure-and-privacy-enabled-iot-home-networks?language_id=2

SPIN DNS traffic monitor for IoT users



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]



CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

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.

cira

SIDN LABS

Conclusions

- IoT will bring us lots of new services that will make society more sustainable, safer, and smarter
- But many challenges ahead to seize DNS opportunities to secure the IoT and protect the DNS from the IoT
- Potential opportunities for ccTLDs
  - As IoT trust anchors (cf. CIRA's secure IoT registry)
  - Initiator of collaborative security efforts (e.g., a national DDoS clearing house)
  - Initiator of IoT security mechanisms for which there's little commercial apatite as yet (cf. SPIN)
  - Carry out research on IoT security to better understand the problem space or stimulate research elsewhere
  - Leverage the mature DNS infrastructure to support ongoing security of IoT devices

cira SIDN LABS

Questions & discussion

Cristian Hesselman
cristian.hesselman@sidn.nl

Jacques Latour
Jacques.Latour@cira.ca

Further reading

[ISOC15] 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

[Mirai17] 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

[Hajim19] 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

[eSilva19] K. e Silva, "Mitigating botnets: Regulatory solutions for industry intervention in large-scale cybercrime", Ph.D. thesis (submitted), Tilburg University, the Netherlands

[DDoS19] C. Hesselman, "Piloting a DDoS Clearing House for Europe", CONCORDIA Open Door Event 2019, Luxembourg City, Luxembourg, Oct 2019, https://www.sidnlabs.nl/downloads/UiROh8kJW62ngdxd1mpX3/3c90e054110a935c463cd4a181a2707c/20191017_CONCORDIA_T3.2_DDoS_Clearing_House_FINAL.pdf

cira

SIDN LABS