ICANN 68
VIRTUAL POLICY FORUM

The DNS & the Internet of Things: Opportunities, Risks & Challenges

23 June 2020

Housekeeping rules

https://cdn.emojidex.com/emoji/seal/female_police_officer.png

- ★ **Please type your questions in Q&A pod.**
- ★ Text written in the chat will not be read aloud.
- ★ Chat sessions are archived.
- ★ Moderator and remote participation manager will manage the queue.
- ★ This meeting is governed under ICANN's Expected Standard of Behavior.

http://www.icann.org/en/news/in-focus/accountability/expected-standards

Welcome

Alejandra Reynoso (.gt)

- ★ Domain Name System (DNS)
- ★ Internet of Things (IoT)
- ★ SAC105
- ★ Goals:
  - ○ How the IoT differs from traditional interactive Internet applications?
  - ○ How DNS and IoT players think of the interaction between their two ecosystems?
  - ○ ICANN community role?

Agenda

- ★ Overview of SAC105 - DNS & IoT
- ★ Experts Panel - Sharing Perspectives
- ★ Peer Review of the Presentations
- ★ Questions and Answers

SAC105 - The DNS & the Internet of Things

Cristian Hesselman
(.nl & SSAC)

- ★ SSAC published SAC105
  - ○ Opportunities
  - ○ Risks
  - ○ Challenges

The DNS and the IoT: security and stability opportunities, risks, and challenges

Cristian Hesselman (SSAC)

ICANN68
Tue Jun 23, 2020
Virtual Meeting

Based on: "The DNS and the Internet of Things: Opportunities, Risks, and Challenges", SSAC report SAC105, June 2019

Shorter version to appear in IEEE Internet Computing magazine, 2020

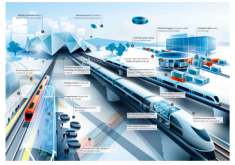
SIDN LABS

Internet of Things

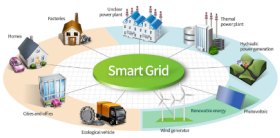
- Internet application that extends "network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers" (ISOC)

- 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

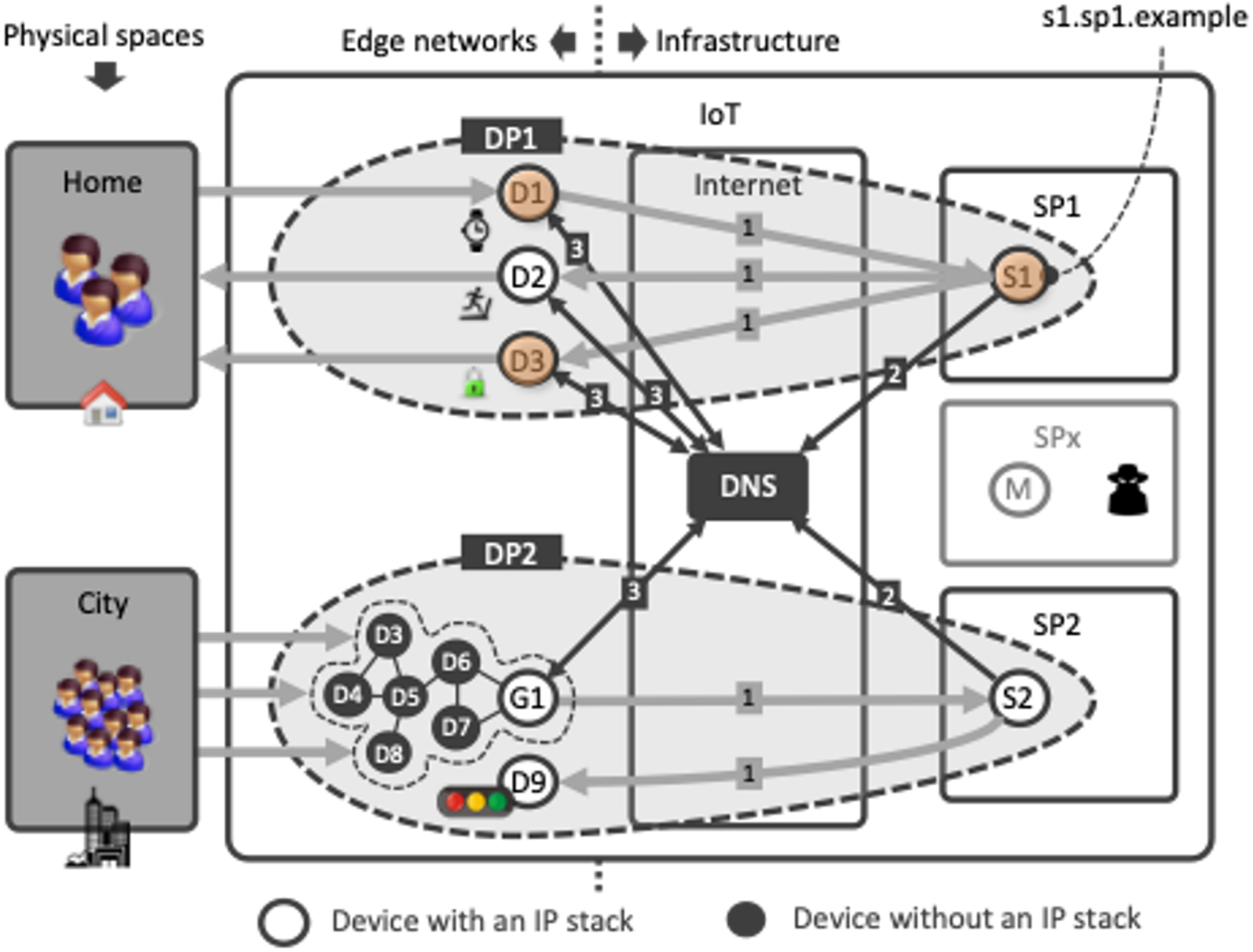


Smart energy grids

Smart homes and cities

Sources: [ISOC15], [SAC105]

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



Sources: [SAC105]

DNS opportunities: increase IoT privacy, safety, and transparency

- Reduce risk of users being profiled
  - Based on their IoT devices' DNS queries
  - Privacy risk: what devices are you using?
  - Safety risk: which of your devices are vulnerable?
  - Solution: encrypt DNS requests (DoH/DoT)

- Reduce risk of IoT device being redirected
  - IoT devices connecting to remote malicious service
  - Privacy risk: sharing intimate data
  - Safety: service might be able to instruct IoT device
  - Solution 1: validate integrity of DNS responses (DNSSEC)
  - Solution 2: MFA registrar services

- More insight into services and resolvers
  - Measure IoT device's DNS queries
  - Intuitive visualization for users

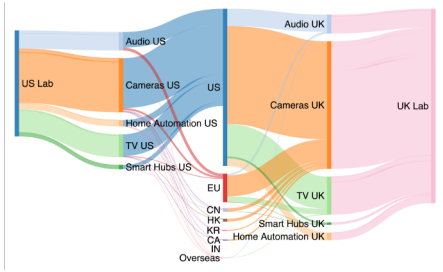
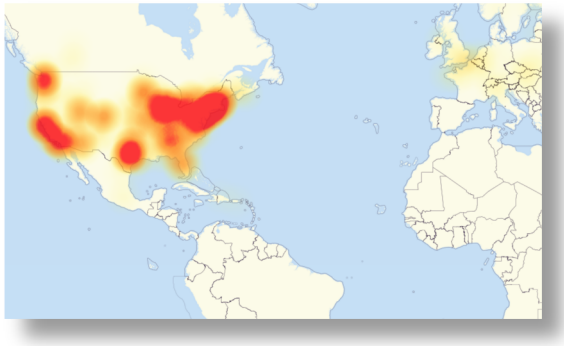


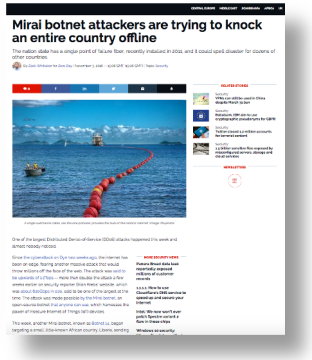
Figure from [Ren19]

Risks to the DNS from the IoT: influx of traffic from IoT devices

- DNS-unfriendly programming at IoT scale
  - TuneIn app example: 700 iPhones generating random queries
  - Imagine millions of unsupported devices that operate unattended for decades

- Larger and more complex DDoS attacks by IoT botnets
  - IoT botnets of 400-600K bots (Mirai, Hajime), may increase
  - Higher propagation rates (e.g., +50K bots in 24 hours)
  - Vulnerabilities difficult to fix, botnet infections unnoticed
  - DDoS amplification: 23-25 million open resolvers





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

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 experts: understand IoT botnets, open resolvers, "DNS friendly" programming and security (e.g., DNSSEC)
  - DNS experts: 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

SIDN LABS

Experts Panel - Sharing perspectives

Eliot Lear
(Cisco)

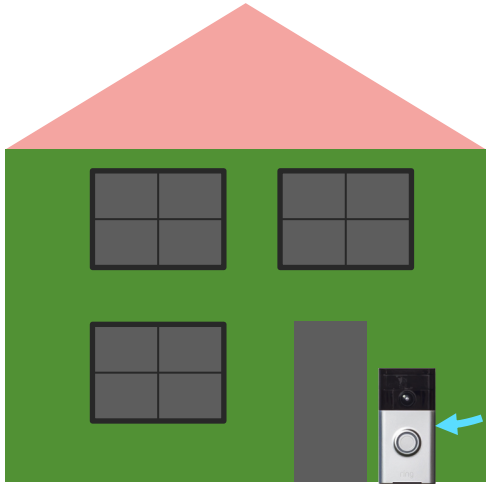
Lise Fuhr
(ETNO)

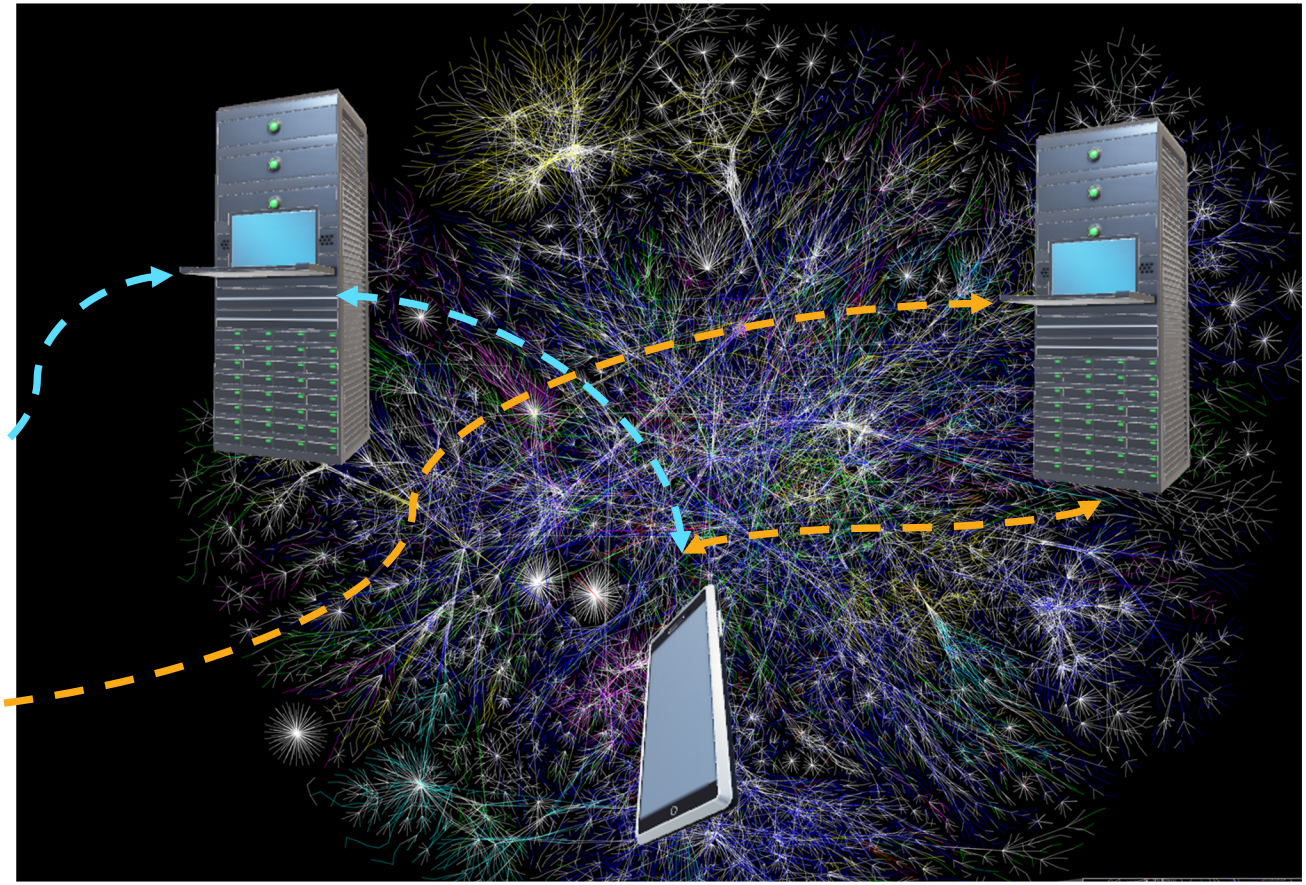
Cristian Hesselman
(.nl & SSAC)

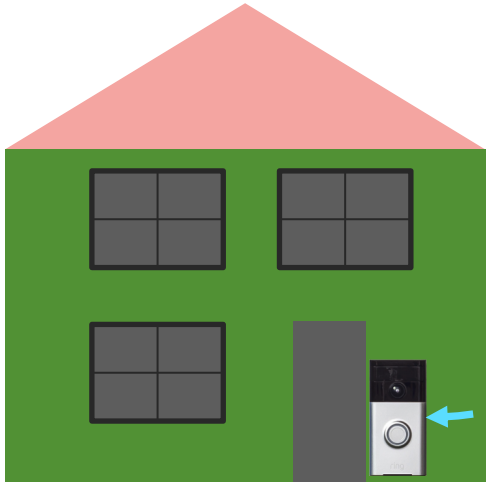
The IoT: The Story of an Oven

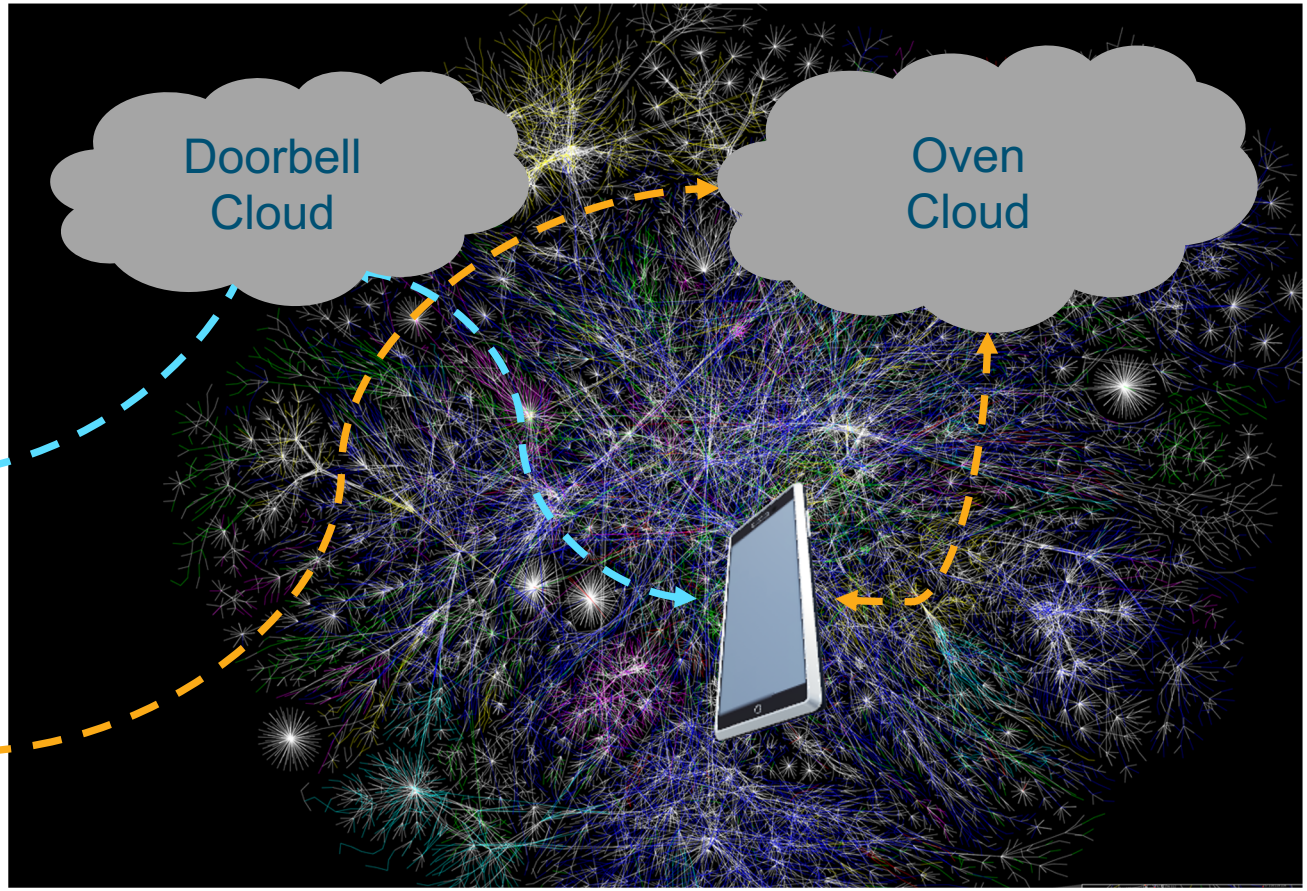
Eliot Lear (Cisco)

ICANN68
Tue Jun 23, 2020
Virtual Meeting







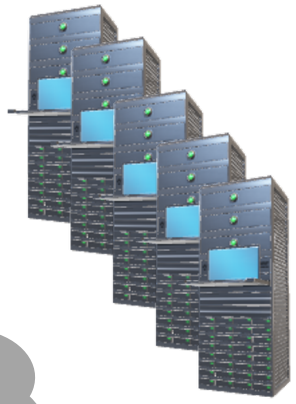


How to get to only oven cloud connector?
DNS + firewall

ovencloud.example.com?

ovencloud.example.com = 10.1.2.3

Oven Cloud



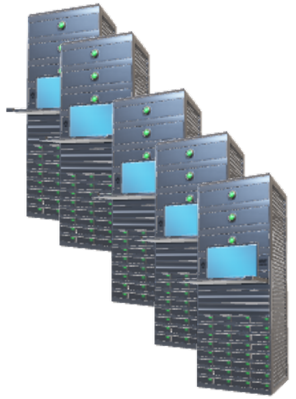
10.1.2.3

Linksys icon courtesy Evan-Amos - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=16128630

How to get to only oven cloud connector?
DNS + a firewall

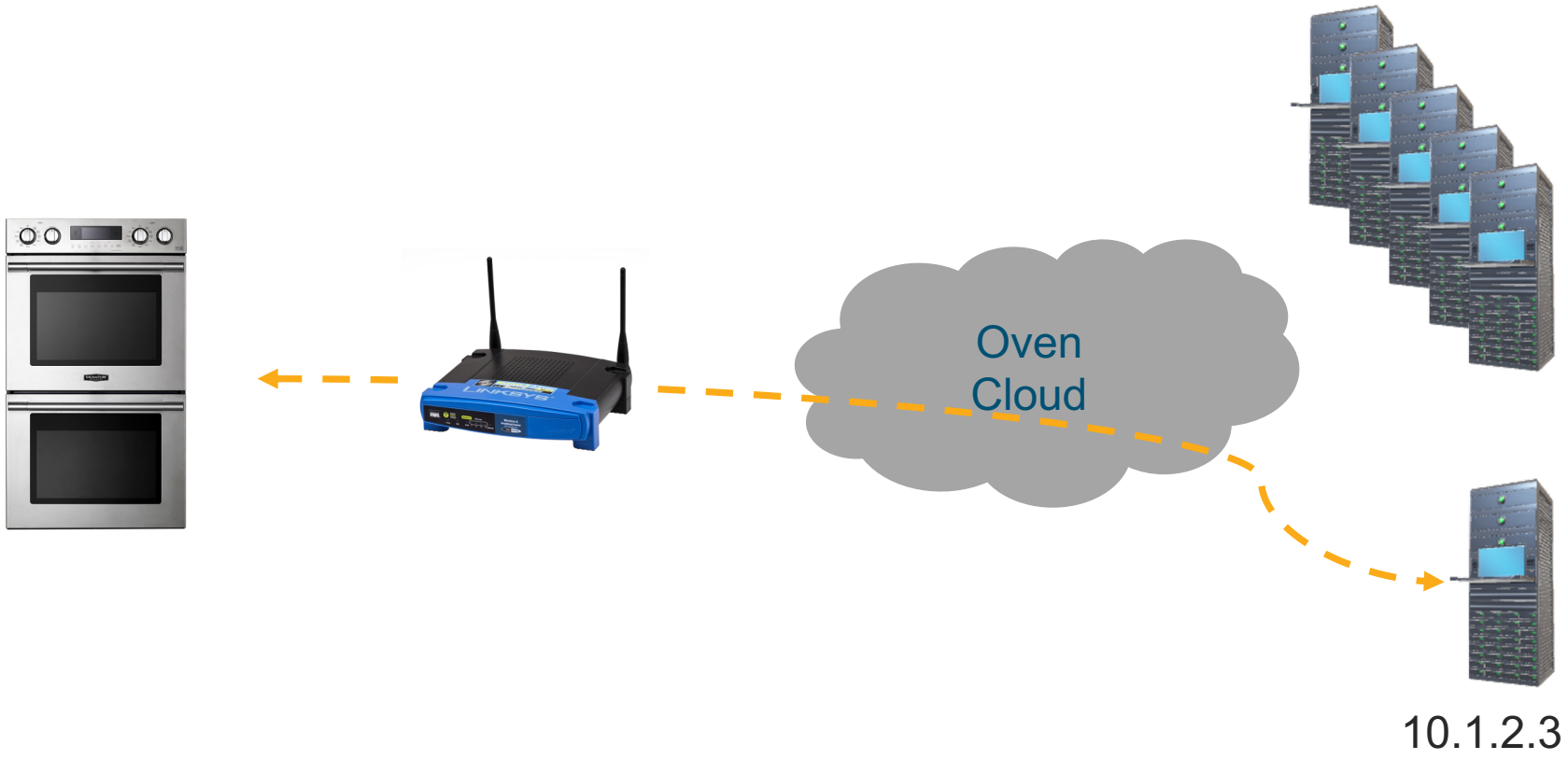
Permit
10.1.2.3

Oven
Cloud



10.1.2.3

How to get to only oven cloud connector?
DNS + a firewall



Different devices means different cloud endpoints

Oven Cloud

10.1.2.3

Doorbell Cloud

10.11.12.13

Oven doesn't need to talk to doorbell

IoT and DNS encryption

- OK to encrypt
- **IOT devices MUST** use deployment DNS if they want network protection (and they should)
- Observe the binding between DNS and the router as a protection point
- Rules distribution can take place using standard methods like Manufacturer Usage Descriptions (RFC 8520)

DNS abuse and IoT: opportunities, risks and challenges

Lise Fuhr, Director-General, ETNO

ICANN68 Policy Forum

THINK DIGITAL – REFORM – PROSPER

etno

Presentation outline

1. The Internet of Things and 5G
2. 5G new network opportunities
3. Addressing concerns around 5G and DNS
4. Where from here? A telco perspective

The Internet of Things will rely on next generation connectivity: 5G

- 5G will enable the rapid growth of the IoT: the number of mobile IoT connections in Europe is set to grow from 140 million in 2018 to nearly 740 million by 2026 (cf. ETNO State of Digital Communications, Jan 2020)

- NB-IoT (Narrow Band) and eMTC enhancements

- 5G IoT: non-IP infrastructures, legacy (cellular) M2M infrastructures already support services which can be labelled as “IoT”

- ***Telcos [5G] IoT does not grow in a vacuum: it’s part of a broader service portfolio and DNS and IP in general can act as a ‘federator’***

The inheritance of 5G & mobile DNS

In the mobile industry's world, in general 5 = 4 +1(!)

- A number of 5G networks will be building on 4G (including Operations/Business Support System) – aka non standalone 5G
- Therefore use of DNS/domain names in these mobile core networks is not prevalent
- Exception for "VoLTE" wherever that applies
- use of DNS/domain names for
  - interdomain is limited (IPX/GRX…) – and mostly derived from legacy IDs
  - mobile Internet access is nonspecific (to mobile)

What 5G may change…

The core network is now intended to be “IP native”

Virtualised hardware-independent environments become the norm

And it’s hard to operate/manage networks solely with IP(v6) addresses… - DNS is just as useful for 5G as it was for previous generations; IPv6 makes it more relevant from an operational perspective

Inter-domain will also be “IP native”…

Including Voice interconnect should gradually move to IP

Inter-domain

Interdomain Virtualised Network Function is largely unchartered territory for mobile networks

How would that use of domain name materialise?

Essentially transparent for users

- Core network/interconnect/IoT: mostly for technical purposes

Largely implementation specific

- 5G will not be a significant source of new second level registrations
- But explicit/implicit use of domain names is prevalent in 3GPP 23.5** specs – not all of which will be resolved on DNS (and few on public DNS – nothing 5G specific here…)

5G will bring many benefits to the network

- **Core network level**: virtual network functions – enabling of Industry 4.0, IoT: LTE-M (Machine Type Communication) or NB-IOT (NarrowBand)
- **Security**: network slicing
- **Using Artificial Intelligence**: development of artificial intelligence for network optimization

What are the challenges and how can we mitigate them?

- Network slicing and the fragmentation of the Internet?
- Domain names and collision avoidance
  - public domain names on private infrastructures (infrastructure domain names used for 5G networks are part of the Internet name system – although they may be resolved on non-public DNS infrastructures – cf. use of 3gppnetworks.org domain names by 3/4/5G networks)
- DNS Security Extensions (DNSSec)
  - Distinguish mobile Internet (unspecific and transparent) and DNS for mobile networks (mostly standard-free and up to the operators)
- Denial-of-Service (DoS) attacks and Botnet
  - There is an encryption trend and if the ISPs are to monitor the DNS-client we need to be able to see the DNS-traffic

Where from here? A telco perspective

- Still many open questions “From Standards to Operations”
- Infrastructure is expensive – IoT business case is still not strong, and more investment is needed
  - with cellular IoT today/early 5G, operators tend to sell “always-on connectivity & monitoring”, less frequently devices or advanced services.
  - But mobile Internet access remains untouched and IoT over 5G networks remains open to third party innovation
- What impact will the covid-19 crisis have on this?
  - Stronger focus on the need for digitalization
  - Stronger focus on security
  - Less travelling? More remote monitoring?

The DNS and the IoT @.nl

Cristian Hesselman (SIDN)

ICANN68
Tue Jun 23, 2020
Virtual Meeting

.nl = the Netherlands' ccTLD

- Registry operator: *Stichting Internet Domeinregistratie Nederland* (SIDN)

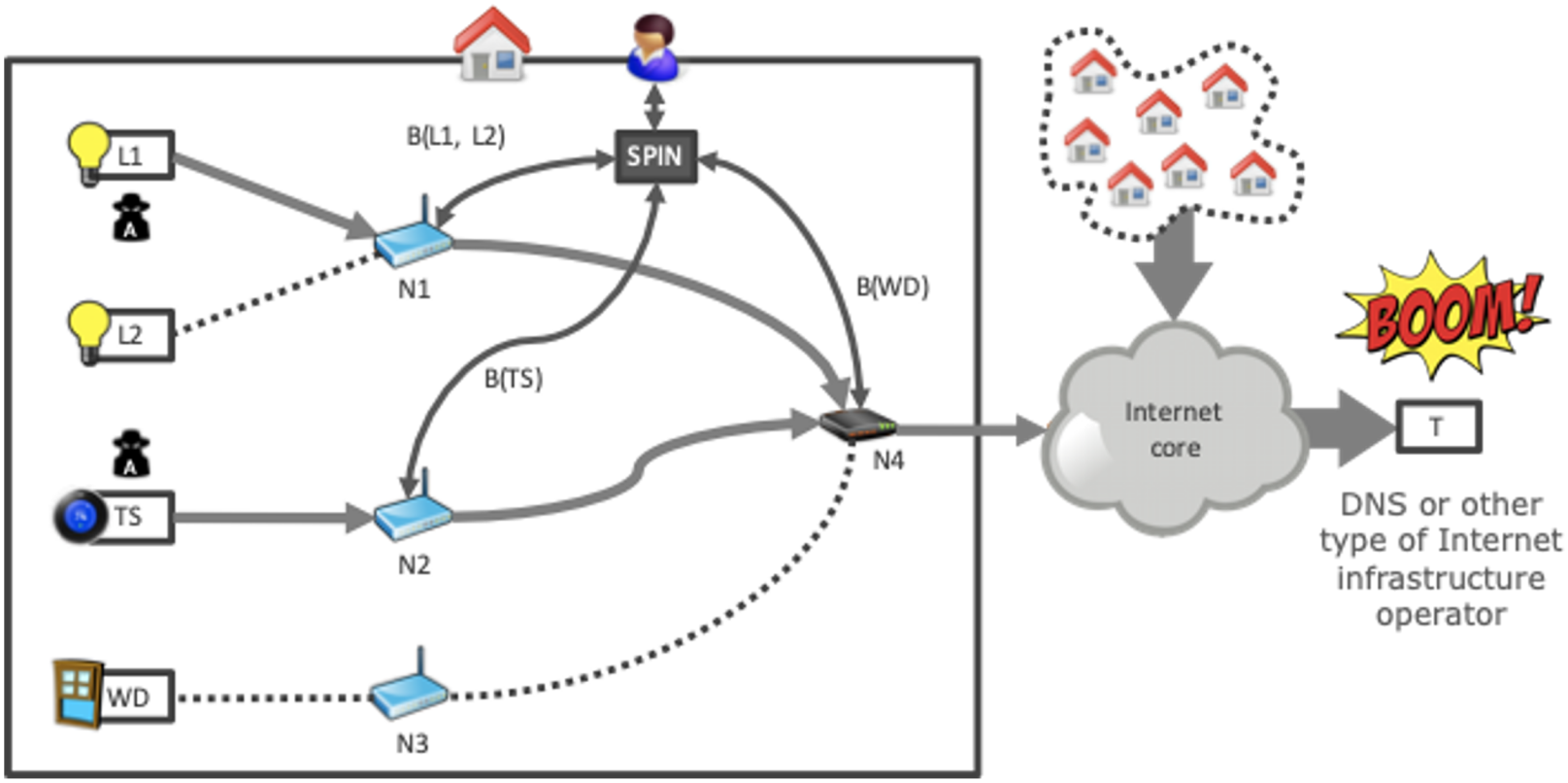
- Critical infrastructure services
  - Registration of all .nl domain names
  - Manage fault-tolerant and global DNS infrastructure

- Increase the value of the Internet in NL and elsewhere
  - Enable safe and novel use of the Internet
  - Improve the security and resilience of the Internet itself

.nl = the Netherlands
17M inhabitants
6.0M domain names
3.3M DNSSEC-signed
1.3B DNS queries/day

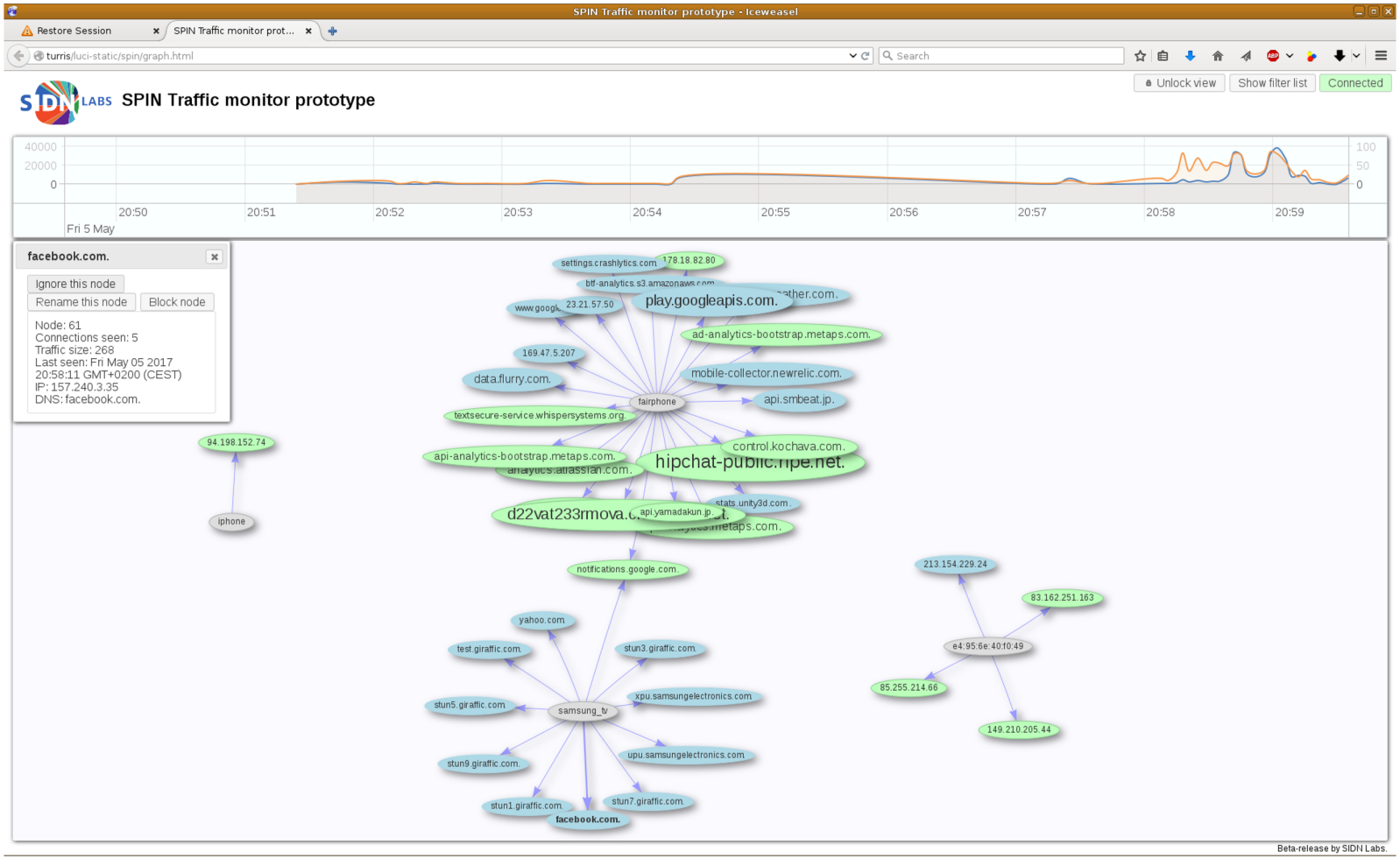
SIDN LABS

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

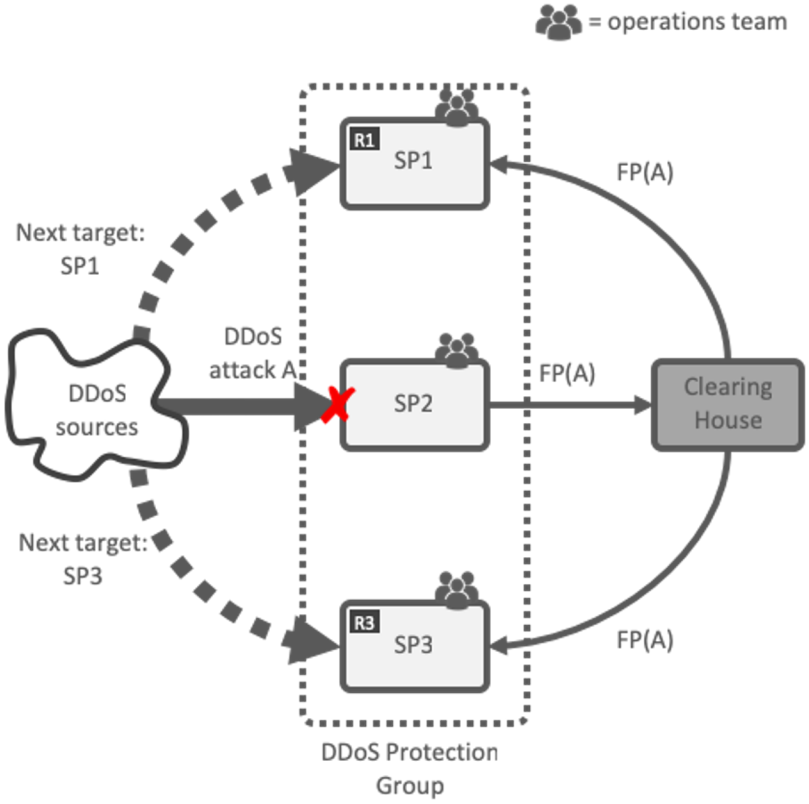
SPIN DNS traffic monitor for IoT users



spin.sidnlabs.nl | github.com/sidn/spin

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]



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.

Reviewing the Presentations

Philippe Fouquart
(ISPCP)

Rafik Dammak
(NCUC)

KC Claffy
(SSAC)

Housekeeping rules

https://cdn.emojidex.com/emoji/seal/female_police_officer.png

- ★ **Please type your questions in Q&A pod.**
- ★ Text written in the chat will not be read aloud.
- ★ Chat sessions are archived.
- ★ Moderator and remote participation manager will manage the queue.
- ★ This meeting is governed under ICANN's Expected Standard of Behavior.

http://www.icann.org/en/news/in-focus/accountability/expected-standards

Q&A

Eliot Lear
(Cisco)

Lise Fuhr
(ETNO)

Cristian Hesselman
(.nl & SSAC)

Philippe Fouquart
(ISPCP)

Rafik Dammak
(NCUC)

KC Claffy
(SSAC)


ICANN
VIRTUAL POLICY FORUM
68
Thank you!
23 June 2020

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

[Hajime19] 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

[DDoS19] “Increasing the Netherlands’ DDoS resilience together”, March 2020, https://www.nomoreddos.org/en/increasing-the-netherlands-ddos-resilience-together/

[Ren19] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, “Information Exposure from Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach”, Internet Measurement Conference (IMC2019), Amsterdam, Netherlands, Oct 2019

Further Reading (continued)

- National Institute of Standards and Technology (NIST) Trustworthy Networks of Things https://www.nist.gov/programs-projects/trustworthy-networks-things
- NIST Mitigating IoT-Based DDoS https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos
- NIST Security for IoT Sensor Networks https://www.nccoe.nist.gov/projects/building-blocks/iot-sensor-security
- NIST Consumer Home IoT Product Security https://www.nccoe.nist.gov/projects/building-blocks/consumer-home-iot
- NIST IoT Device Cybersecurity Capability Core Baseline https://www.nist.gov/publications/iot-device-cybersecurity-capability-core-baseline
- Foundational Cybersecurity Activities for IoT Device Manufacturers https://www.nist.gov/publications/foundational-cybersecurity-activities-iot-device-manufacturers
- NIST Smart Cities and Communities Framework Series https://www.nist.gov/el/cyber-physical-systems/smart-americaglobal-cities/nist-smart-cities-and-communities-framework
- NIST Global City Teams Challenge https://www.nist.gov/el/cyber-physical-systems/smart-americaglobal-cities/global-city-teams-challenge