The Internet of Things and the DNS

Jacques Latour / SSAC

ICANN65 | June 2019

Introduction

Security and Stability Advisory Committee (SSAC)

Who We Are

- 39 Members
- Appointed by the ICANN Board

What We Do

Role: Advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

What is Our Expertise

- Addressing and Routing
- DNS & DNSSEC
- Registry & Registrar Operations
- ISP & Network Operations
- DNS Abuse & Cybercrime
- Internationalization
- ICANN Policy and Operations

How We Advise

105 Publications since 2002

Agenda

1. Introductions
2. IoT and the DNS
3. Opportunities for the DNS
4. Risks to the DNS posed by IoT
5. Challenges for the DNS and IoT Industries
6. Q & A

SAC105: The DNS and the Internet of Things

- SAC105: The DNS and the Internet of Things: Opportunities, Risks, and Challenges, published June 3rd, 2019
- A different kind of SSAC report:
  - **No recommendations** to the ICANN Board
  - A tutorial-style discussion intended to trigger and **facilitate dialogue** in the broader ICANN community
  - More **forward looking** than operational in nature
  - Partly within SSAC and ICANN's remit, but also goes beyond it
- Many aspects of our discussion are not new, except as they consider new challenges from IoT

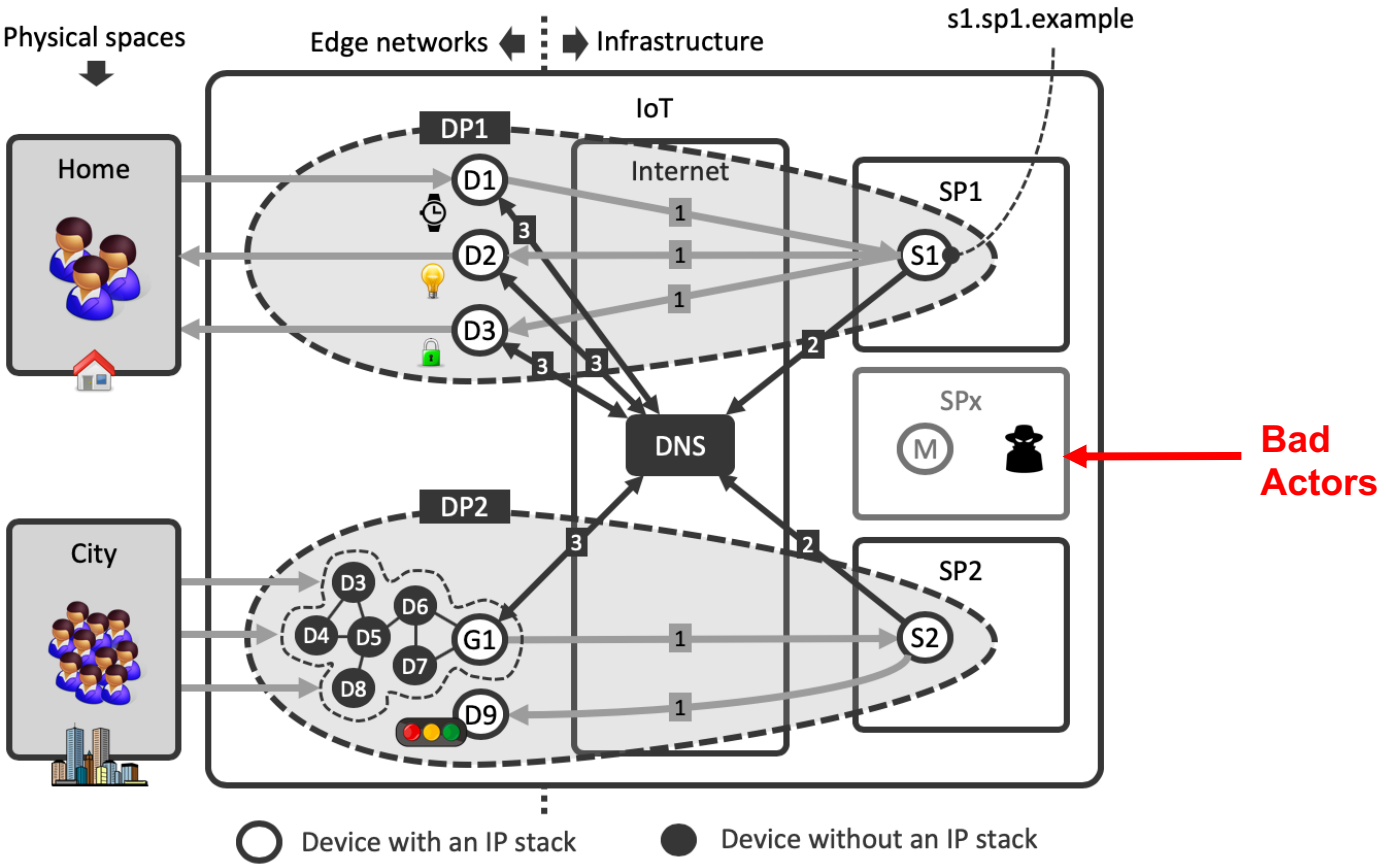
The Internet of Things (IoT)

- Internet application that extends “network connectivity and computing capability to objects, devices, sensors, and items **not ordinarily considered to be computers**” (ISOC, 2015)
- Examples: smart homes, smart cities, self-organizing dynamic networks of drones and robots
- Differences with “traditional” applications
  - IoT continually senses, interprets, and acts upon physical world
  - Often without user awareness or involvement (passive interaction)
  - Pervasive 20-30 billion devices operating “in the background” of people’s daily lives
  - Widely heterogeneous devices (hardware, operating systems, network connection)
  - Longer lifetimes (perhaps decades) and unattended operation

IoT and the DNS

- Remote services (cloud services) assist devices in performing their task (e.g., combining and analysing data from multiple sensors)
- Measurement studies show that IoT devices use the DNS to locate remote services (e.g., sleep trackers, light switches)
- **Opportunity:** DNS helps fulfilling IoT's more stringent security, stability, and transparency requirements stemming from seamless interaction with physical world
- **Risk:** IoT stresses the DNS, accidentally (e.g., large number of devices coming online simultaneously after a power outage) or on purpose (IoT-powered DDoS attack)
- **Challenge:** DNS and IoT industries can seize opportunities and address risks

Role of the DNS for the IoT



Opportunities: DNS helps protect the Real World

- DoH and DoT (**resolver verification** and transport encryption)
  - Avoid IoT devices being redirected to malicious resolvers
  - Reduce information devices reveal about themselves
  - Protect user privacy for devices with highly specific tasks
- DNSSEC (DNS response verification)
  - Avoid IoT devices being redirected to malicious services
- Multi-Factor Authentication (MFA) to protect against domain registration hijacks
  - May affect large installed base of IoT devices
  - Attackers might invest more because IoT services become high-value targets
- Visualize DNS queries to make IoT more transparent for users
  - Services and resolvers that IoT devices use
  - Enable users to control resolvers that IoT devices use

Risks to the DNS from the IoT

- DNS-unfriendly programming at IoT scale
  - TuneIn app example → random queries filled resolver cache of mobile operator
    - Only around 700 iPhones, took three weeks for the app to get updated
  - Effects depend on factors like device concentrations and TTLs
  - Unsupported devices that operate unattended for decades
- Larger and more complex DDoS attacks by IoT botnets (Mirai, Hajime)
  - IoT botnets currently around **400-600K bots** (Mirai, Hajime), may increase in the future
  - Set of IP addresses may change quickly
  - Higher propagation rates
    - Hajime exploited a 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 through open resolvers (on IoT devices)
  - 23-25 million open resolvers and amplification factors in the range 29-64

Challenges for DNS and IoT Industries (1 / 2)

- Developing a **DNS security library** for IoT devices
  - Such as DNSSEC validation, DoH/DoT support
  - User control over DNS security settings and insight into services that IoT devices use
  - Work on various IoT operating systems and CPU types
  - Example starting points: DNSSEC Trigger and Danish
- Training IoT and DNS professionals
  - IoT product managers: understand IoT botnets and open resolvers
  - IoT engineers: understand “DNS friendly” programming and security(e.g., DNSSEC)
  - DNS folks: understand IoT changes domain registration model and security
  - Example starting points: RFC4367 and “Hello DNS”

Challenges for DNS and IoT Industries (2 / 2)

- Deploying a cross-DNS operator system to share information on IoT botnets
  - Characteristics of DDoS attacks that DNS operators handle, “fingerprints”
  - Also filtering rules, bot concentrations across AS-es, botnet booters, etc.
  - Example starting points: DDoS-DB, IoT-Pot, Shadowserver’s Open Resolver Scanning Project
- More advanced mitigation of very large IoT-powered DDoS attacks
  - DDOS mitigation broker that enables DNS operators to flexibly share mitigation capacity (e.g., using DOTS signalling)
  - Security systems in edge networks, such as home routers (e.g., using SPIN and SHG)
- Develop a system to measure the evolution of the IoT
  - Device-to-domain name database (e.g., based on publicly available MUD specifications)
  - DNS operators provide coarse grained stats (e.g., counts, origin AS)

Conclusions and Future Work

- The IoT is an emerging distributed Internet application expected to further ease our daily lives and make our society safer and more sustainable
- Might make the role of DNS even more important
  - IoT devices autonomously and seamlessly interact with our physical world through billions of connected sensors and actuators
- SAC105: The DNS and the Internet of Things: Opportunities, Risks, and Challenges
  - Tutorial-style overview of the DNS and the IoT as two co-evolving and interacting ecosystems in terms of opportunities, risks, and challenges
  - https://www.icann.org/en/system/files/files/sac-105-en.pdf
- SSAC wishes to continue discussing our report with the ICANN community
- We welcome your feedback!

Q&A

Thank you