Lecture #3: IoT concepts and applications

Cristian Hesselman, Elmer Lastdrager, Ramin Yazdani, and Etienne Khan

University of Twente | May 6, 2020

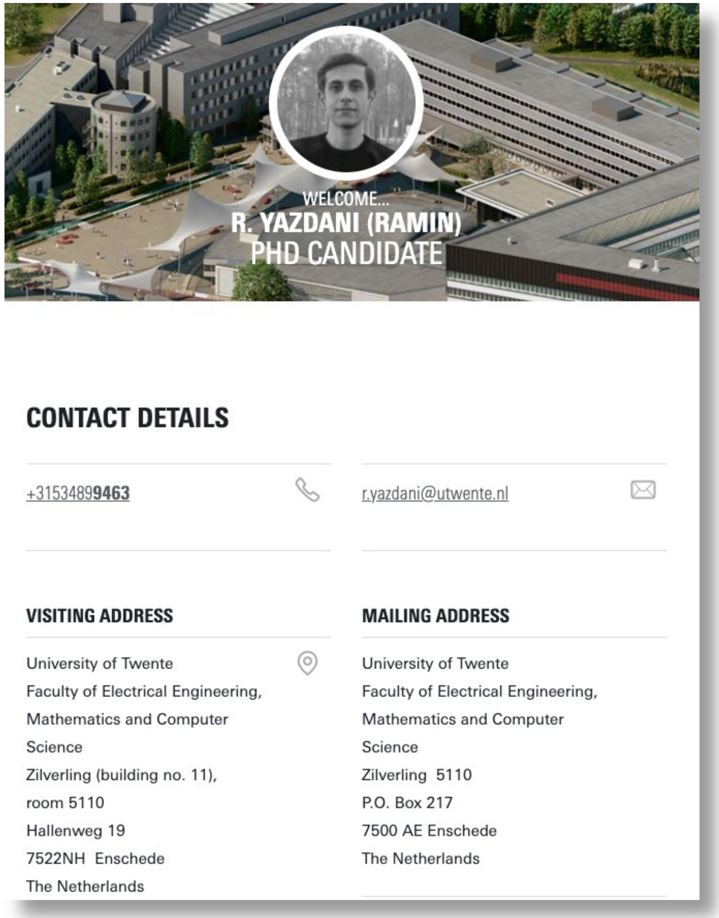
Paper summaries

- You must have handed in your two summaries **before 7AM on the day of the lecture**
- Each summary can be at most 250 words, at most 1 single-sided A4 page
- You can add figures, and graphs from the paper or add your own if you like (e.g., concept maps)
- You can use the summaries during the oral exam
- Submit through CANVAS
- You **cannot** complete SSI without submitting 12 paper summaries!

Devices for lab assignment

- Pick them up at Ramin’s office
  - IoT device if you don’t have any at home
  - Optional SPIN device

- Please contact Ramin beforehand!



WELCOME...
R. YAZDANI (RAMIN)
PHD CANDIDATE

CONTACT DETAILS

+31534899463 ☎

r.yazdani@utwente.nl ✉

VISITING ADDRESS

University of Twente
Faculty of Electrical Engineering,
Mathematics and Computer
Science
Zilverling (building no. 11),
room 5110
Hallenweg 19
7522NH Enschede
The Netherlands

MAILING ADDRESS

University of Twente
Faculty of Electrical Engineering,
Mathematics and Computer
Science
Zilverling 5110
P.O. Box 217
7500 AE Enschede
The Netherlands

Interactive lectures

- Objective: enable you to learn from each other and further increase your understanding of the papers, contributes to preparing yourself for the oral exam

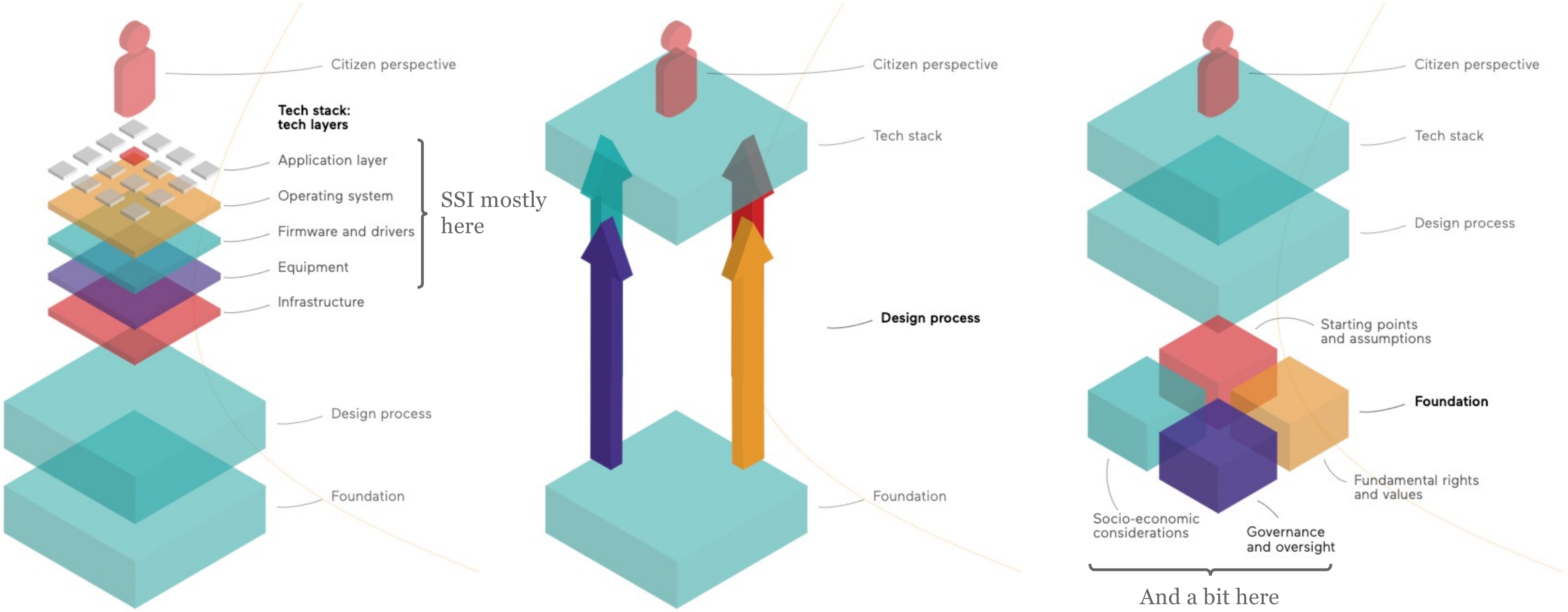
- Interactive format
  - Teachers summarize two papers per lecture
  - Multiple-choice questions (not graded) and discussion
  - We ask at least one of you to share their thoughts on each paper (pros, cons, surprises)
  - Enables you to learn from each other, so mandatory to participate

- A 7th “re-sit” lecture in case you miss a lecture (optional for everybody else), same format

Today’s objective

- “Setting the scene”: after the lecture, you will be able to discuss the interplay between the DNS and the IoT and discuss the IoT’s safety, legal, and regulatory implications
- Not very technical, but important for the more technical papers later in the course
- [WEIS] ties into guest lecture #2 (IoT security through standardization and regulation)
- Contributes to SSI learning goal #1: “Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF”

Motivation for this lecture: IoT is more than tech



SSI mostly here

And a bit here

“In the public stack, we view the ‘user’ as a citizen in a democratic society – not as a consumer in a business model or a subject of a state.”

Source: https://publicstack.net/layers/

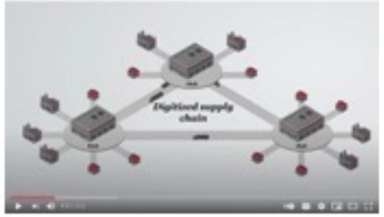
Today’s papers

[DNSIoT] C. Hesselman, M. Kaeo, L. Chapin, kc claffy, M. Seiden, D. McPherson, D. Piscitello, A. McConachie, T. April, J. Latour, and R. Rasmussen, “The DNS in IoT: Opportunities, Risks, and Challenges”, IEEE Internet Computing, Vol. 24, No. 4, July-Aug 2020

[WEIS] E. Leverett, R. Clayton, and R. Anderson, “Standardisation and Certification of the Internet of Things’”, 16th Annual Workshop on the Economics of Information Security (WEIS2017), USA, June 2017

“The DNS in IoT: Opportunities, Risks, and Challenges”, IEEE Internet Computing, Vol. 24, No. 4, July-Aug 2020

Internet of Things (IoT)



What is the IoT?

- 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

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

[ISOC] K. Rose, S. Eldridge, L. Chapin, “The Internet of Things: An Overview – Understanding the Issues and Challenges of a More Connected World”, ISOC Whitepaper, October 2015

Discussion

What is the key characteristic of the IoT for you and why?

A. Interaction with the physical world

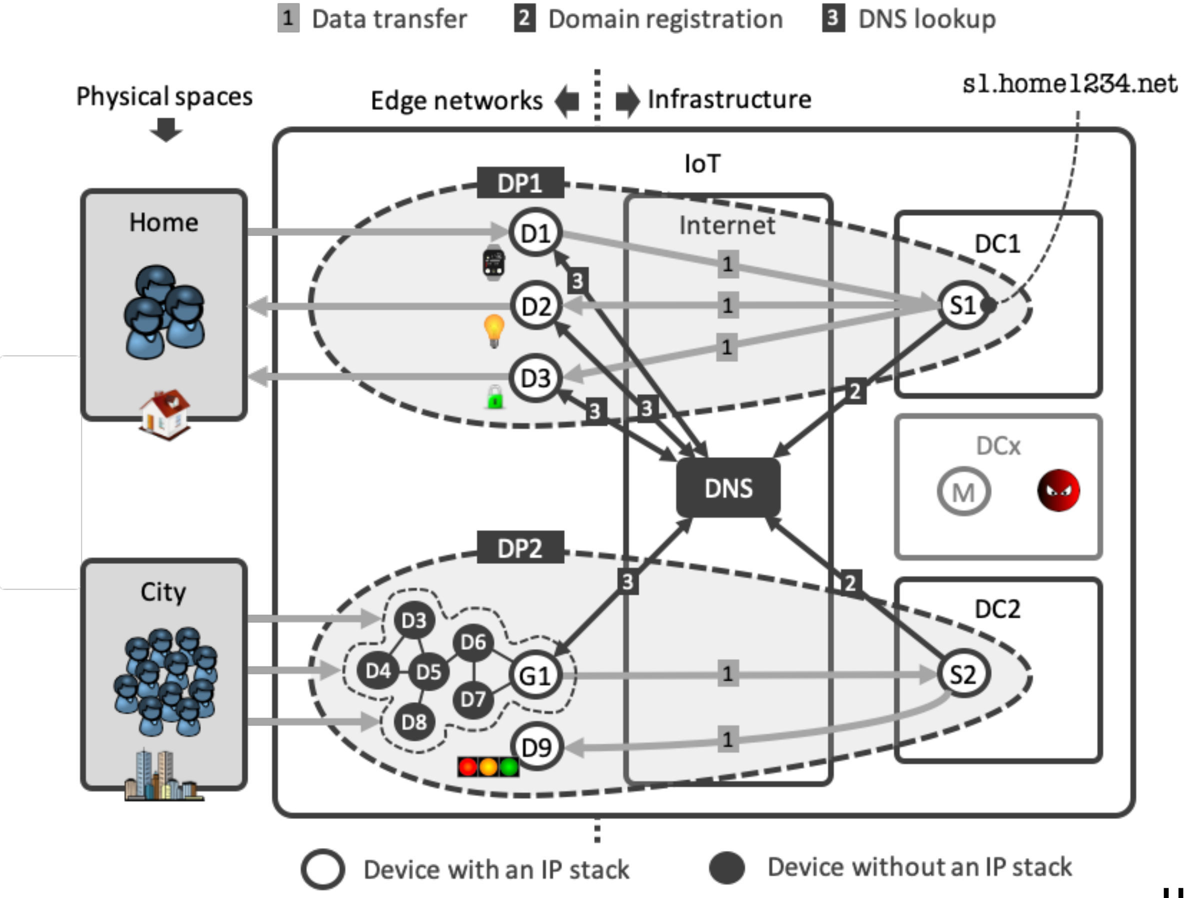
B. Connected devices

C. Massive scale

D. Unattended operation

E. Other

IoT deployments and the Domain Name System (DNS)



DNS high-level operation

M. Müller, “Making DNSSEC Future Proof”, Ph.D. thesis, University of Twente, 2021 (under review)

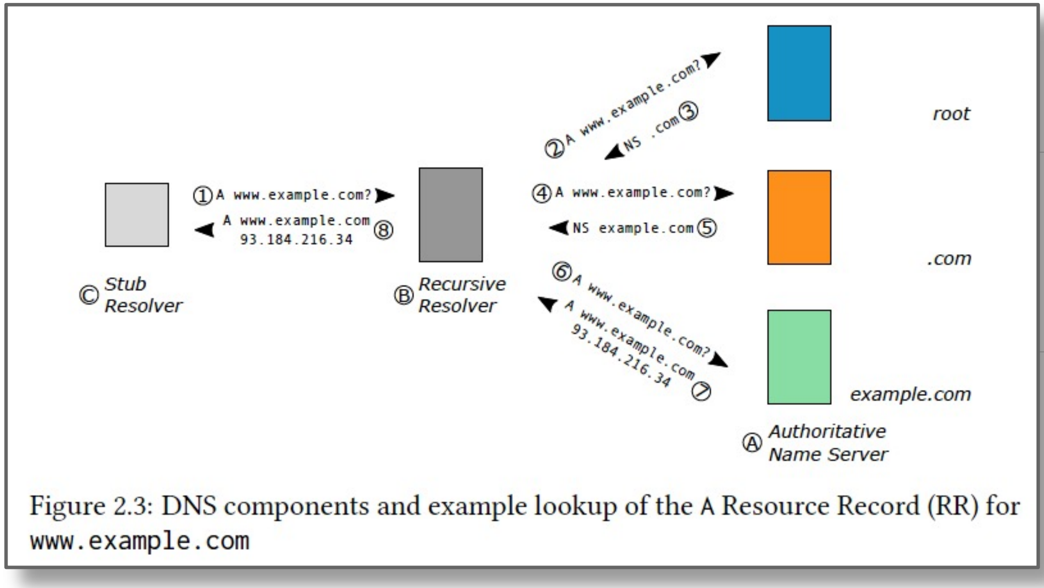
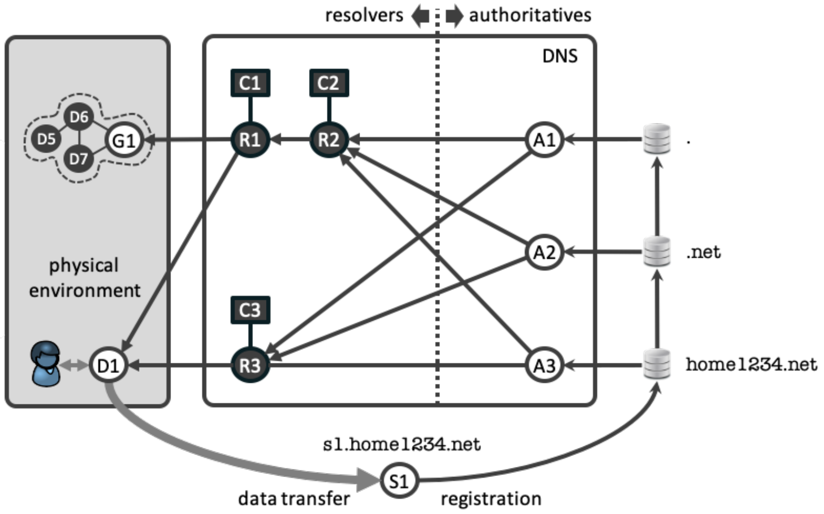
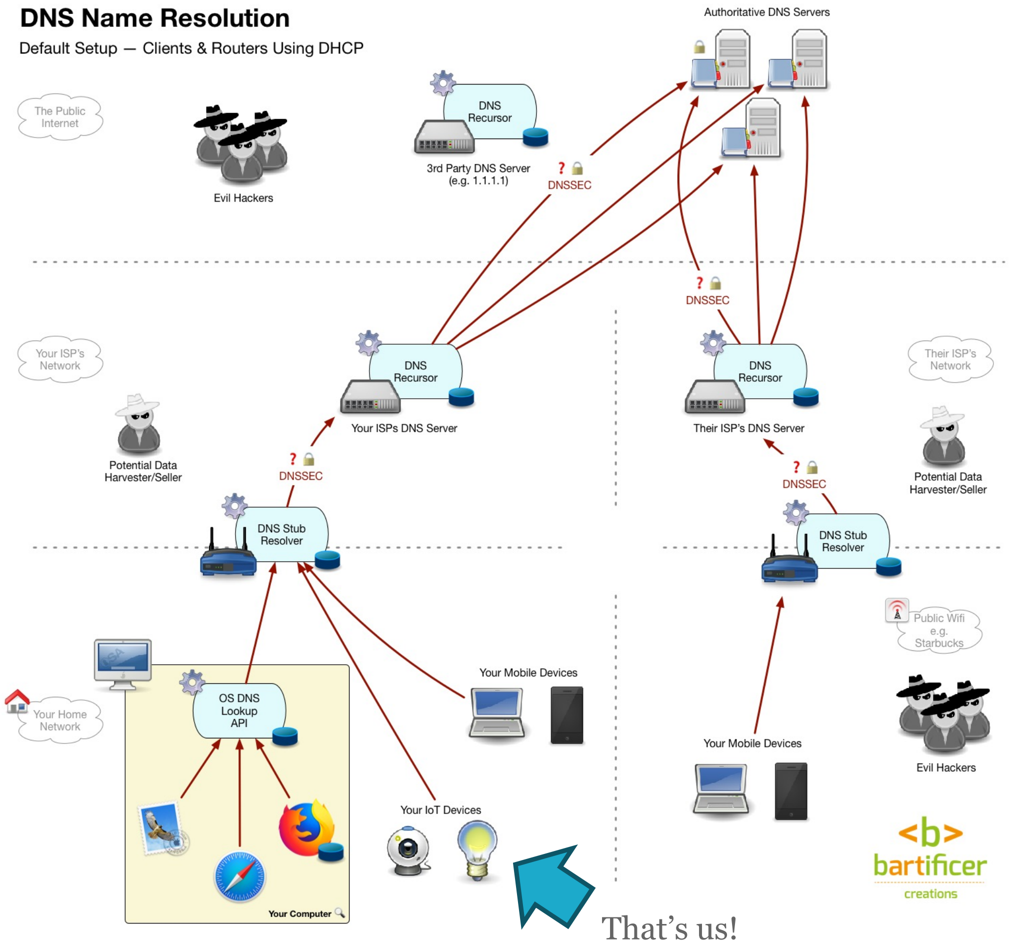


Figure 2.3: DNS components and example lookup of the A Resource Record (RR) for www.example.com



UNIVERSITY OF TWENTE. SIDN LABS

DNS ecosystem



That's us!

Source: https://www.podfeet.com/blog/which-dns-resolver-should-i-use/

DNS quiz

What’s the purpose of DNS caches?

A. Lower DNS response times

B. Increase DNS scalability

C. Enable operators to analyze DNS queries

D. Increase demand for computer memory

Overview

Help meet IoT's new safety and transparency requirements

Opportunities	
O1	Using DoH/DoT to encrypt DNS queries
O2	Using DNSSEC to detect malicious redirects of IoT devices
O3	DNS protocols to double-check the authenticity of IoT services
O4	Protecting IoT devices against domain registration hijacks
O5	Using DNS datasets to increase IoT transparency

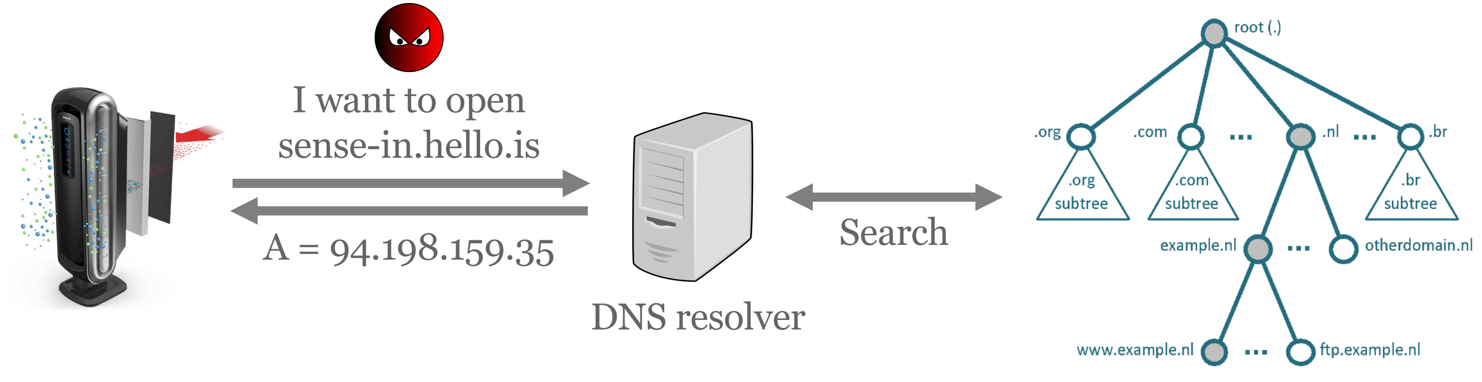
Protect the SSR of the DNS against insecure IoT devices

Risks	
R1	DNS unfriendly programming at IoT scale
R2	Increased size and complexity of IoT botnets targeting the DNS
R3	Increased DDoS amplification through open DNS resolvers

Technologies and systems that need to be developed

Challenges	
C1	Developing a DNS security and transparency library for IoT devices
C2	Training IoT and DNS professionals
C3	Developing a system to share information on IoT botnets
C4	Proactive and flexible mitigation of IoT-powered DDoS traffic
C5	Developing a system to measure how the IoT uses the DNS

O1: DNS-over-HTTPS (or another secure transport)

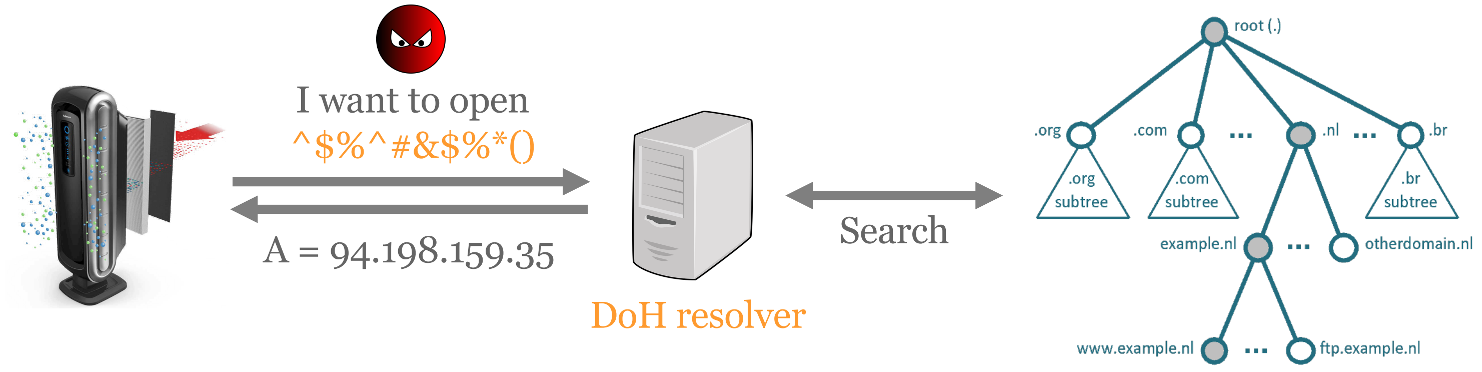


I want to open sense-in.hello.is

A = 94.198.159.35

DNS resolver

Search



I want to open ^$%^#&$%*()

A = 94.198.159.35

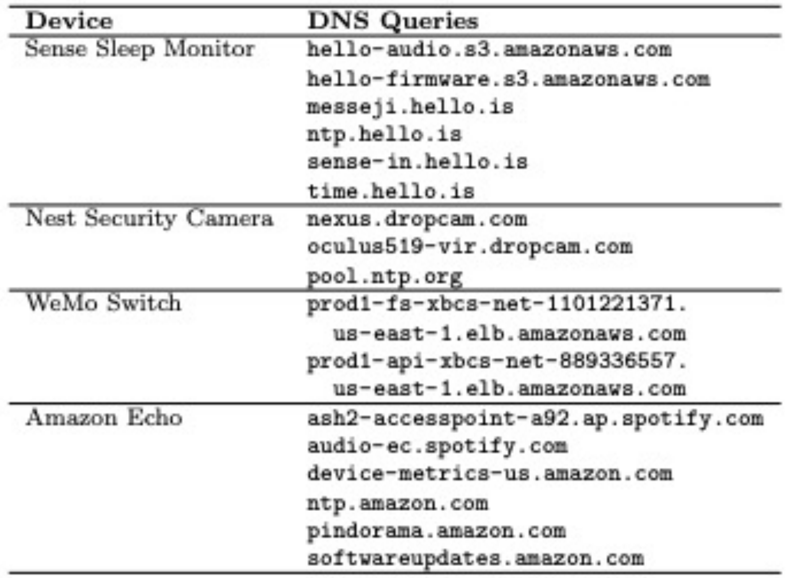
DoH resolver

Search

DoH reduces risk of IoT users being profiled

- Profiling based on the DNS queries that a user's IoT devices send
- Protects privacy: more difficult to figure out what devices people are using
- Protects safety: more difficult to figure out which devices are vulnerable
- Downside: risks in centralized resolver settings (e.g., Google Public DNS, Cloudflare)

N. Apthorpe, D. Reisman, N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic", Workshop on Data and Algorithmic Transparency (DAT '16), New York University Law School, November 2016



Device	DNS Queries
Sense Sleep Monitor	hello-audio.s3.amazonaws.com hello-firmware.s3.amazonaws.com messeji.hello.is ntp.hello.is sense-in.hello.is time.hello.is
Nest Security Camera	nexus.dropcam.com oculus519-vir.dropcam.com pool.ntp.org
WeMo Switch	prod1-fs-xbcs-net-1101221371.us-east-1.elb.amazonaws.com prod1-api-xbcs-net-889336557.us-east-1.elb.amazonaws.com
Amazon Echo	ash2-accesspoint-a92.ap.spotify.com audio-ec.spotify.com device-metrics-us.amazon.com ntp.amazon.com pindorama.amazon.com softwareupdates.amazon.com

Figure 1: DNS queries made by tested IoT devices during a representative packet capture. Many queries can be easily mapped to a specific device or manufacturer.

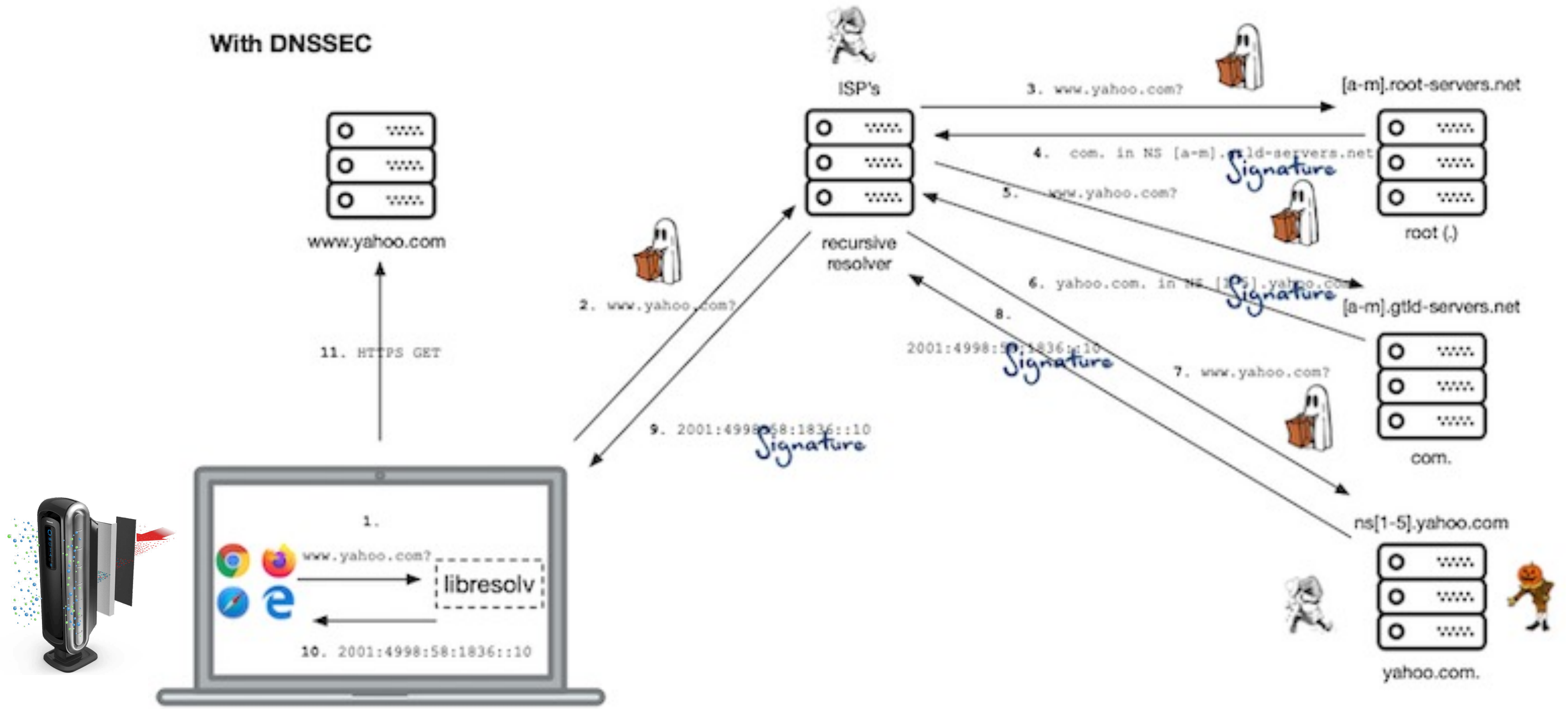
DoH quiz

With DoH it’s impossible for an adversary to identify the service your IoT device is connecting to

A. True

B. False

O2: Signing DNS responses with DNSSEC



Source: https://www.netmeister.org/blog/doh-dot-dnssec.html

DNSSEC reduces risk of IoT device being redirected

- Unauthorized redirects through manipulation of DNS responses

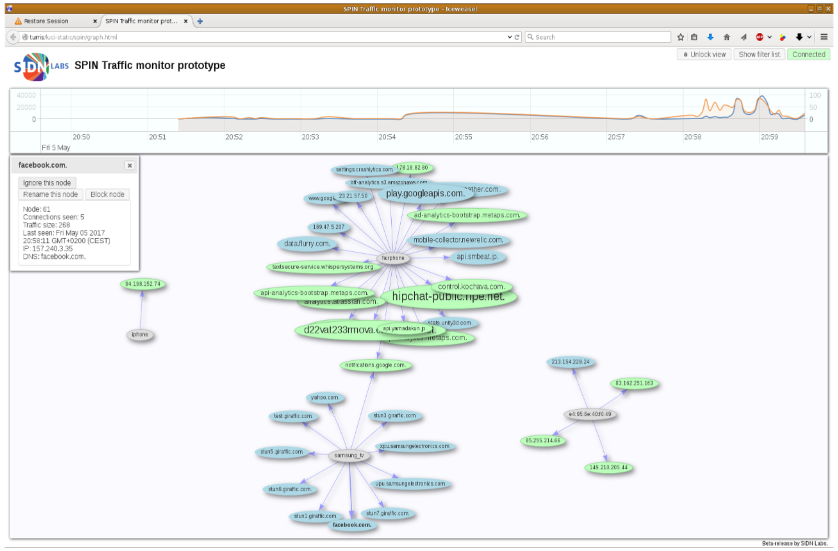
- DNSSEC reduces privacy risk: sharing intimate sensor data with rogue service

- DNSSEC reduces safety risk: lowers probability of IoT device receiving malicious instructions (cf. air purifier)

- Most secure setup: signature validation on IoT devices

O3: DNS queries

[IMC] 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



Node: 61
Connections seen: 5
Traffic size: 268
Last seen: Fri May 05 2017
20:58:11 GMT+0200 (CEST)
IP: 157.240.3.35
DNS: facebook.com.

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

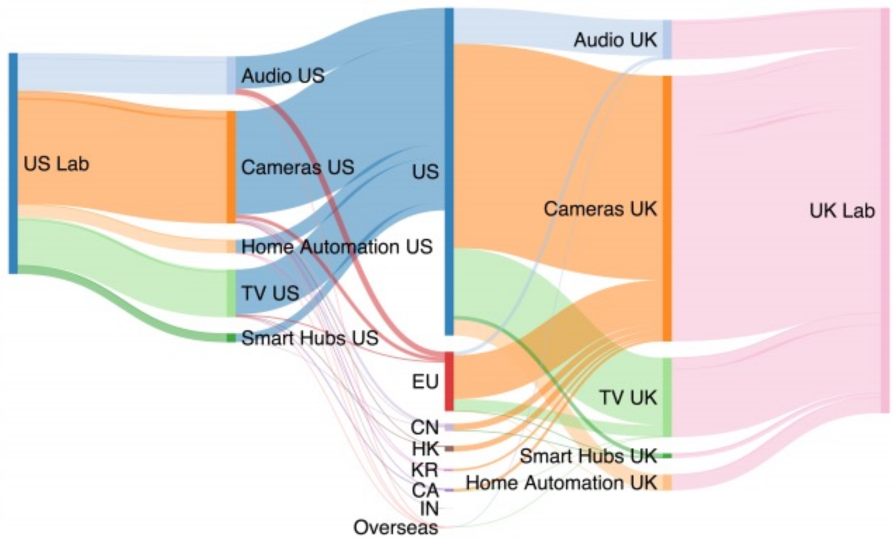
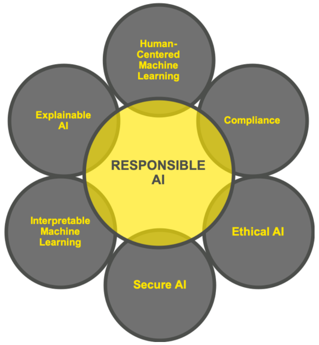


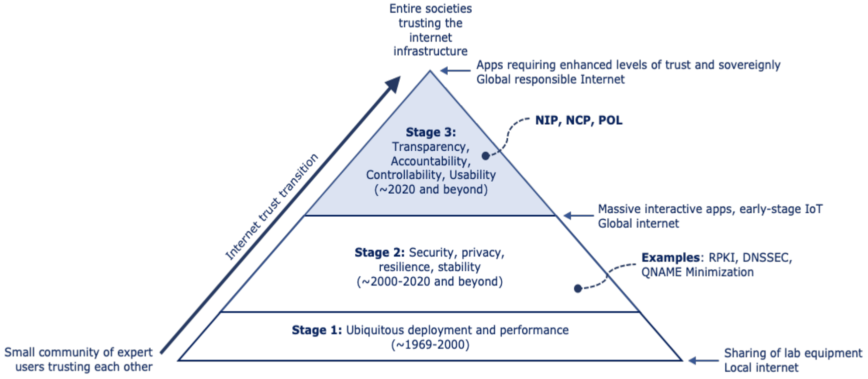
Figure 2: Volume of network traffic between the US (left) and UK (right) labs to the top 7 destination regions (center), grouped by category (middle left and right). Most traffic terminates the US, even for the UK lab; many devices send traffic to countries outside of their testbed’s privacy jurisdiction.

DNS query data to make the IoT more transparent

- Measure IoT device's DNS queries
- Requires intuitive visualization for users
- Also, what sensor data are devices sharing?
- Perhaps a topic for future regulation
- Part of larger discussion on data autonomy ➡

GAIA-X


Human-Centered Machine Learning
Explainable AI
Compliance
RESPONSIBLE AI
Interpretable Machine Learning
Ethical AI
Secure AI



Entire societies trusting the internet infrastructure

Apps requiring enhanced levels of trust and sovereignly
Global responsible Internet

Stage 3: Transparency, Accountability, Controllability, Usability (~2020 and beyond)

NIP, NCP, POL

Massive interactive apps, early-stage IoT
Global internet

Stage 2: Security, privacy, resilience, stability (~2000-2020 and beyond)

Examples: RPKI, DNSSEC, QNAME Minimization

Stage 1: Ubiquitous deployment and performance (~1969-2000)

Internet trust transition

Small community of expert users trusting each other

Sharing of lab equipment
Local internet

UNIVERSITY OF TWENTE.

SIDN LABS

Transparency discussion

How would you make the IoT more transparent?

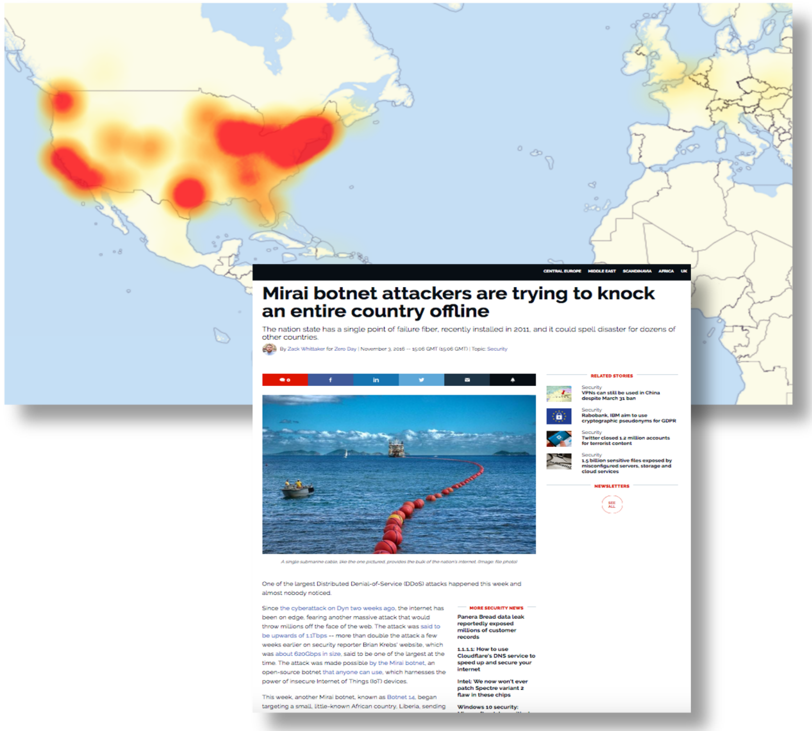
R1: DNS-unfriendly programming at IoT scale

- TuneIn app example: 700 iPhones generating random queries www.<random-string>.com
- In the stone age (2012), but still: imagine millions of unsupported devices exhibiting that kind of behavior after a software update
- High-level APIs abstract DNS away from developers

TUNE IN 2 TUNE OUT

R2: 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 (now around 3 million)



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

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:

Botnet discussion

What do you think will make IoT botnets more difficult to eradicate than a traditional one?

C1-C3: Challenges for the DNS and IoT industries

- Develop an open-source DNS security and transparency library for IoT devices
  - Such as DNSSEC validation, DoH/DoT support
  - User control over DNS security settings and services used

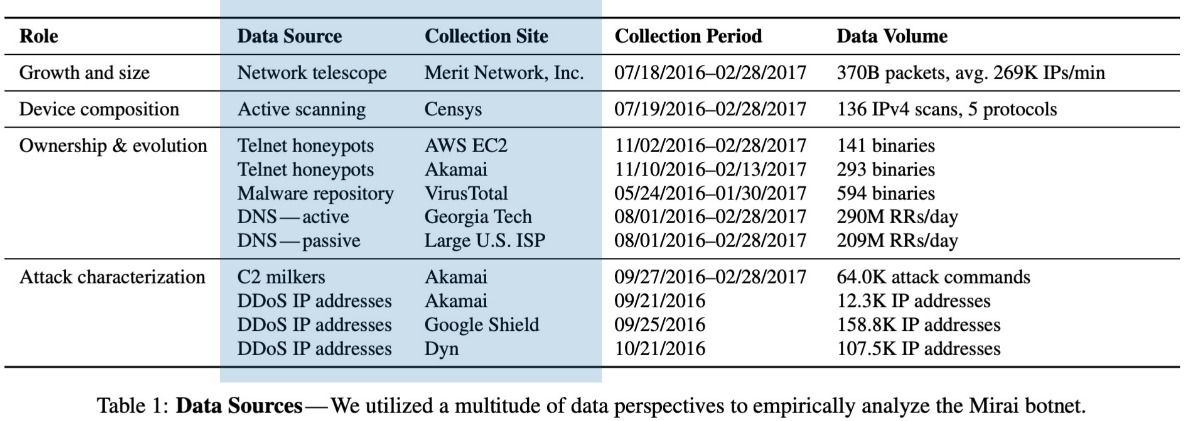
- Develop a system to proactively detect IoT botnets
  - Share DDoS “fingerprints”, countermeasures, and other botnet characteristics across operators
  - **Collaborative** DDoS detection and learning

- **Collaboratively** handle IoT-powered DDoS attacks
  - DDoS mitigation broker to flexibly share mitigation capacity
  - Security systems in edge networks, such as home routers

Why collaborative?

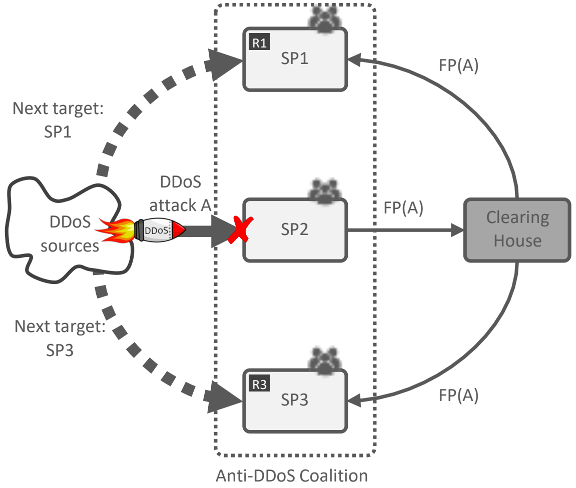
[Mirai] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet", in: 26th USENIX Security Symposium, 2017

- Collaborative incident analysis
- Mirai IoT botnet
- 11 sources, 9 organizations/sites



Role	Data Source	Collection Site	Collection Period	Data Volume
Growth and size	Network telescope	Merit Network, Inc.	07/18/2016–02/28/2017	370B packets, avg. 269K IPs/min
Device composition	Active scanning	Censys	07/19/2016–02/28/2017	136 IPv4 scans, 5 protocols
Ownership & evolution	Telnet honeypots Telnet honeypots Malware repository DNS — active DNS — passive	AWS EC2 Akamai VirusTotal Georgia Tech Large U.S. ISP	11/02/2016–02/28/2017 11/10/2016–02/13/2017 05/24/2016–01/30/2017 08/01/2016–02/28/2017 08/01/2016–02/28/2017	141 binaries 293 binaries 594 binaries 290M RRs/day 209M RRs/day
Attack characterization	C2 milkers DDoS IP addresses DDoS IP addresses DDoS IP addresses	Akamai Akamai Google Shield Dyn	09/27/2016–02/28/2017 09/21/2016 09/25/2016 10/21/2016	64.0K attack commands 12.3K IP addresses 158.8K IP addresses 107.5K IP addresses

Table 1: **Data Sources** — We utilized a multitude of data perspectives to empirically analyze the Mirai botnet.



- Collaborative mitigation of (IoT-powered) DDoS attacks
- Fingerprinting of DDoS attacks
- Sharing fingerprints and mitigation rules
- More detail: antiddoscoalition.nl

UNIVERSITY OF TWENTE.

SIDN LABS

Discussion

What challenges do you foresee in IoT security? For example, where in the network?

Key takeaways

- IoT enables smarter, safer, more sustainable society, but extraordinary safety and privacy risks

- The DNS is one of the core components of the Internet infrastructure for traditional applications and will also play a key role for the IoT

- Opportunities to help fulfilling the IoT's new safety and transparency requirements using the DNS' security functions, datasets, and ubiquitous nature

- Poorly developed and maintained IoT devices are a risk in terms of security and DNS usage

- Many challenges for the interaction between the IoT and the DNS, but starting points exist

Standardisation and Certification of the ‘Internet of Things’

Eireann Leverett, Richard Clayton, Ross Anderson

Pros and Cons of IoT

- The Good: Economic efficiency
- The Bad: Safety hazards
- The Ugly: Attacks

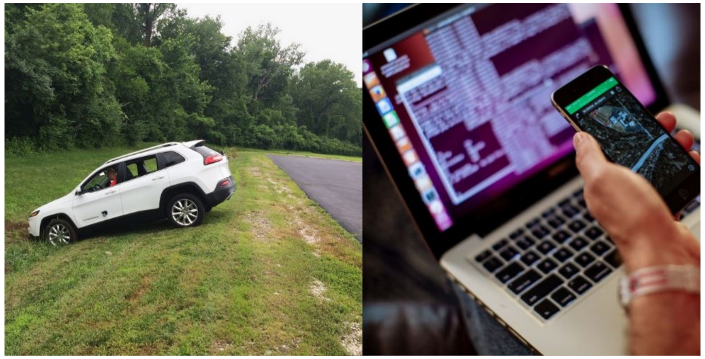
Shift from Safety to Security

- Having only safety in mind is not enough anymore and regulators need to consider security as well.

- These two are not fully separable contexts as in many languages they translate to the same word as well

Two Examples

The famous Jeep Hack



https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Florida Water Plant Hack

https://www.forbes.com/sites/leemathews/2021/02/15/florida-water-plant-hackers-exploited-old-software-and-poor-password-habits/

Core Question in the paper

What the EU's regulatory framework should look like a decade from now (2017).

- General: A powerful cross-domain regulator?
- Sectoral: Each sector with its own CyberSecurity cell?
- A mixture?
- sth else?

Discussion Question #1

What does the EU's regulatory framework look like at the moment?

A. General: A powerful cross-domain regulator?

B. Sectoral: Each sector with its own CyberSecurity cell?

C. Separate regulators for privacy, safety, consumer protection, …?

D. A mixture?

Goals (a Mixture of Safety and Privacy)

The goals and mission of a cybersecurity regulator may be a mix of the following:

1. Ascertaining, agreeing, and harmonising protection goals
2. Setting standards
3. Certifying standards achievement and enforcing compliance
4. Reducing vulnerabilities
5. Reducing compromises
6. Reducing system externalities

Quiz Question

What's an externality in the context of IoT security?

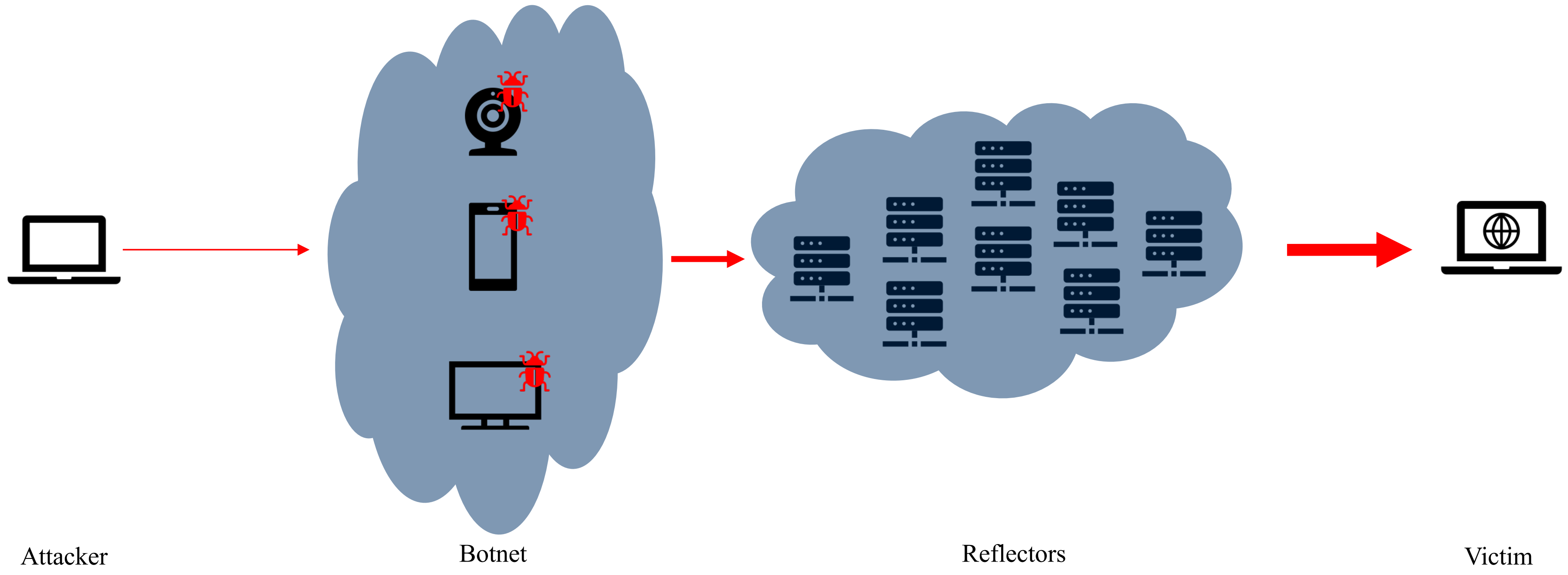
A. A human adversary in an IoT device's local operating environment

B. An external organization that regulates a specific IoT ecosystem (e.g., medical or automotive)

C. A sudden spike in RF bit error rate as a result of a solar flare

D. A device vendor not bearing the costs caused by an insecurity

An Example of Security Externality



An Example of Security Externality

- Three sources of externalities:
  - Botnet
  - Reflectors
  - Networks allowing spoofing

- Main cause: Lack of incentive to prevent it

History of the Safety Regulation

- Three industries discussed:
  - Road transport
  - Medical devices
  - Electrotechnical equipment

Road transport

- Inappropriate standards (developed due to political/commercial incentives) have reduced vehicle security (e.g., the Wassenaar Arrangement export controls that limited cryptographic key length).

- “It is more natural to embed security regulation in existing transport regulation rather than in a new general `security', `cyber' or `data protection' law.” [WEIS]

Healthcare

- Usability failures has been the main safety threat so far.

- A blame game between vendors and hospital network administrators

- “By not permitting notified bodies [NBs] and competent authorities [CAs] to study what happens after they grant approvals, the EU has failed to collect the evidence that would be most useful to security and safety regulators and researchers alike.” [WEIS]

Energy Sector

- Has attracted one of the highest attack rates on critical infrastructure

- An example of what can go wrong: Operators were not allowed to bill customers for cybersecurity costs of critical assets

- Strict standards of energy sector versus conflicting/competeing standards of IT industry.

Generic Approaches

- **Liability:** The EU Product Liability Directive needs to be extended to include services
- **Transparency:** Breach disclosure laws and coordinated vulnerability disclosure
- **Data protection:**
  - Consent or anonymize rule doesn't scale for IoT big data
  - Globalization
- **Attack and vulnerability testing:**
  - Conflict of interest for penetration testing (increases production costs)
  - Vulnerabilities after integration (rather than in a single product)
- **Economics of Security standards:** To reduce the costs of attacks on various stakeholders

Discussion Question #2

Who should investigate the IoT incidents?

A. Vendors
B. Regional authorities
C. A mix of stakeholders

Proposal of the Paper

- Creation of a European Safety and Security Engineering Agency

- Missions:
  - support the European Commission's policy work
  - support sectoral regulators in the EU institutions and at the Member State level
  - develop cross-sectoral policy and standards
  - act as a clearing house for data
  - work to promote best practice and harmonization
  - act as a counterweight to the national security authorities

Discussion Question #3

Which sector currently implements a practice closer to the goals of the IoT regulation?

A. Transport

B. Healthcare

C. Energy

D. Other (give an example)

Key takeaways

- Security and safety regulation of IoT devices are not separable concepts.

- IoT expands over a wide range of products for which a single solution might not always be the optimal one.

- IoT regulation is about standardizing a moving target

Lecture feedback

1. To what extent do you think you'll be able to discuss the interplay between the DNS and the IoT? (A = 🟢, B = 🟠, C = 🔴)

2. To what extent do you think you'll be able to discuss the IoT's safety, legal, and regulatory implications? (A = 🟢, B = 🟠, C = 🔴)

3. Open question: what are your main lesson learned of the papers and this lecture?

Volg ons

.nl SIDN.nl

@SIDN

in SIDN

Q&A

Next lecture: **Wed May 12, 11:00-12:45**

Cristian Hesselman Director of SIDN Labs	+31 6 25 07 87 33 c.e.w.hesselman@utwente.nl @hesselma
Elmer Lastdrager Research Engineer	+31 6 12 47 84 88 elmer.lastdrager@sidn.nl @ElmerLastdrager

UNIVERSITY OF TWENTE.

SIDN LABS