Lecture #2: IoT and Internet Core Protocols

Antonia Affinito, Etienne Khan, Ting-Han Chen, and Cristian Hesselman

University of Twente | Wed May 8, 2024

UNIVERSITY OF TWENTE.

SIDN LABS

Your teachers today

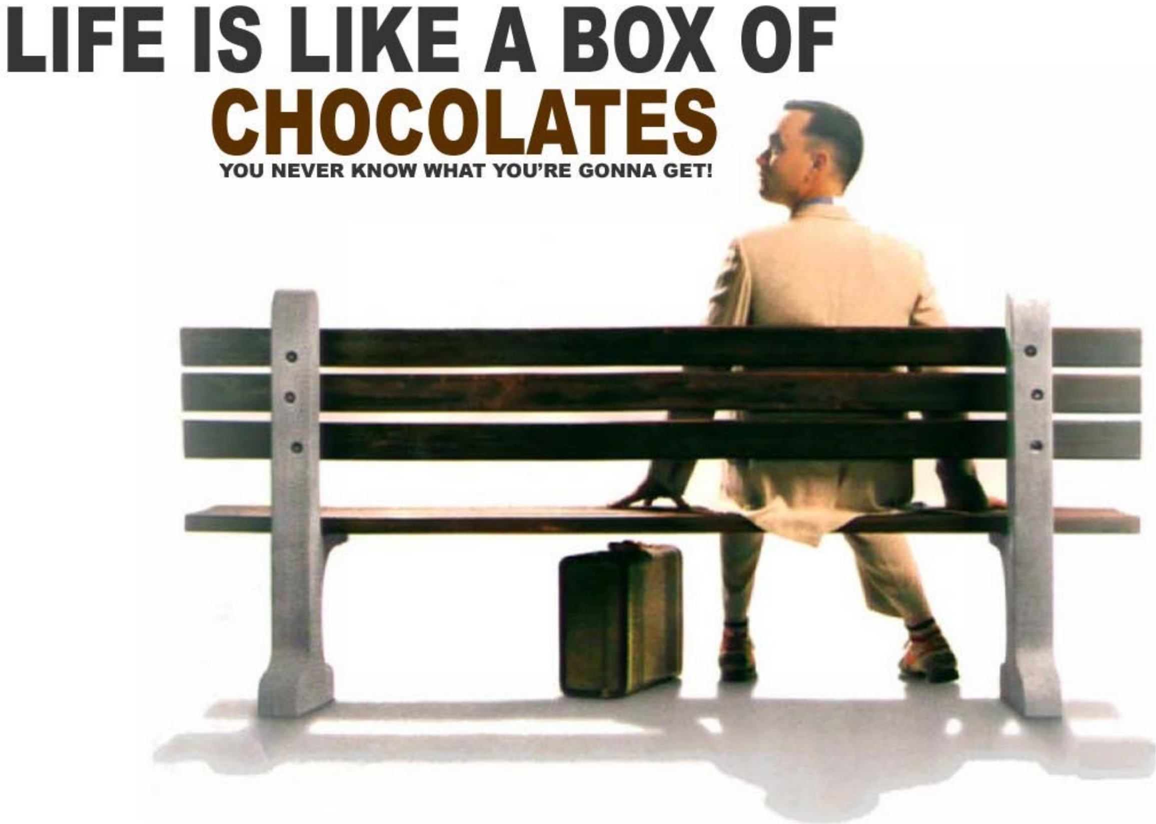
Ting-Han Chen

- Ph.D. candidate in the DACS group
- Objective: aim for IoT vulnerability and disclosure notification
- Motivation: we deserve a secure IoT surrounded daily life and friendly connections between people making IoT better

Cristian Hesselman

- Professor in the DACS group, director of SIDN Labs
- Objective: increase the security of the Internet infrastructure
- Motivation: enable future generations to solve the challenges of their time using an Internet infrastructure they can trust

UNIVERSITY OF TWENTE. SIDN LABS


LIFE IS LIKE A BOX OF
CHOCOLATES
YOU NEVER KNOW WHAT YOU'RE GONNA GET!

The Internet of Things is like a …

Today's agenda

- Admin
- Introduction to today's lecture
- Paper on the DNS in IoT
- Paper on IPv6 scanning
- Initial round of feedback

Admin

Interactive lectures

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

- Interactive format
  - Teachers summarize two papers per lecture
  - Multiple-choice and open questions (not graded) and discussion
  - Enables you to learn from each other

- Summaries are mandatory!

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!

Schedule

Lecture	Date	Contents
R1	May 1	Course introduction
R2	**May 8**	**IoT and Internet Core Protocols**
G1	May 14	How the core of the Internet works **(recorded)** ⚠
R3	May 15	IoT Edge Security Systems
	May 22	No lecture (as several of your teachers will be in Dresden :)
R4	May 29	IoT Botnet Measurements 1
R5	Jun 5	IoT Botnet Measurements 2
R6	Jun 12	IoT Security in Non-Carpeted Areas
R7	Jun 19	IoT Device Security
	Jun 26	No lecture (so you can study for the exam :)
G2	TBD	TBD

Important dates

- Two summaries per lecture: **before every lecture at 7 AM CEST**
- Lab report (PDF) and required files: **Wed Jun 19, 9 AM CEST**
- Written exam: **Wed July 3** (timeslot may change, we'll keep you posted)
- Lab groups of 3 people: **Fri May 10, EOB**
- Alle summaries and lab reports to be submitted through CANVAS

Grading clarification

- Based on your feedback at the introduction lecture (thanks!)

- Grade = (score of written exam) × 50% + (score of the lab assignment) × 50%
  - Where both scores must be a 5.5 or higher. We added this constraint because we'd like folks to focus on both deliverables. This was less of an issue when we used an oral instead of a written exam (2018-2023), because oral exams are more difficult to "slack out of"
  - You MUST submit summaries for all 12 papers in time to pass SSI. The reason is that the summaries are essential for group learning and help you prepare for your written exam in an incremental way

- We updated the language on https://courses.sidnlabs.nl/ssi/

UNIVERSITY OF TWENTE. SIDN LABS

Introduction to today's lecture

From pipes to a lasagna

IVA
Kungl. IngenjörsVetenskaps Akademien

Traditional deployment in ”pipes” implies a tight control throughout the infrastructure

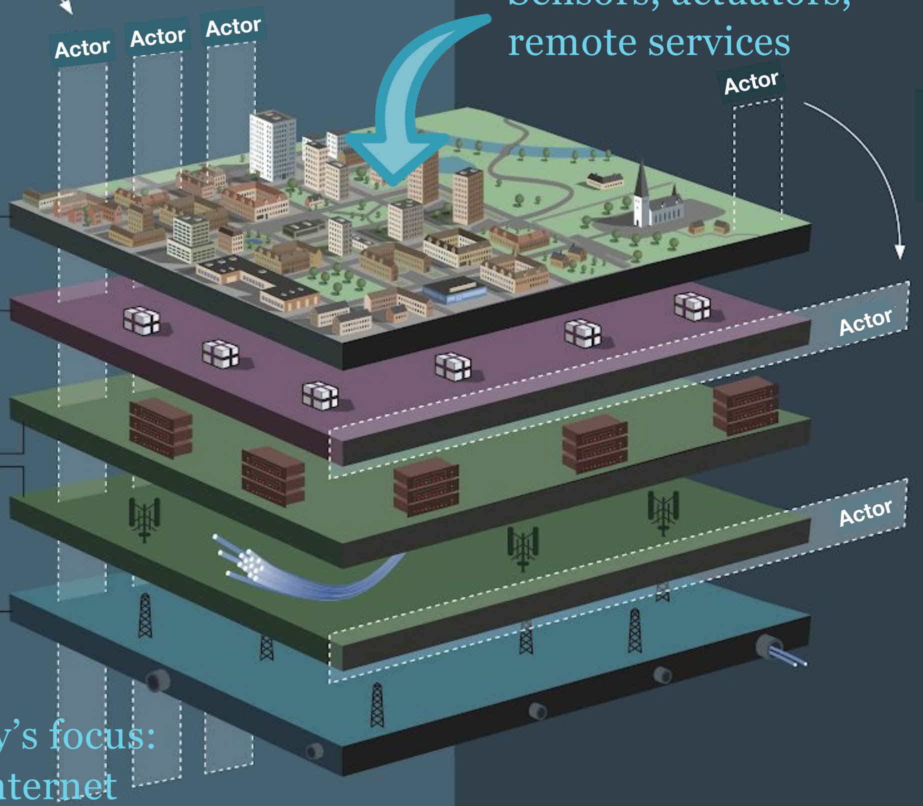
Services
Companies, public sector and others offer services like web, email and apps to companies, citizens and consumers.

Internet Access
Internet- and mobile operators give companies and consumers access to Internet.

Active infrastructure
Transmission providers ensure transport of data to internet- and mobile operators.

Passive inf… ucture
Ducts, fibre, … sts etc. Built by municipa… , private companies a… thers.

Sensors, actuators, remote services



Today's focus: the Internet

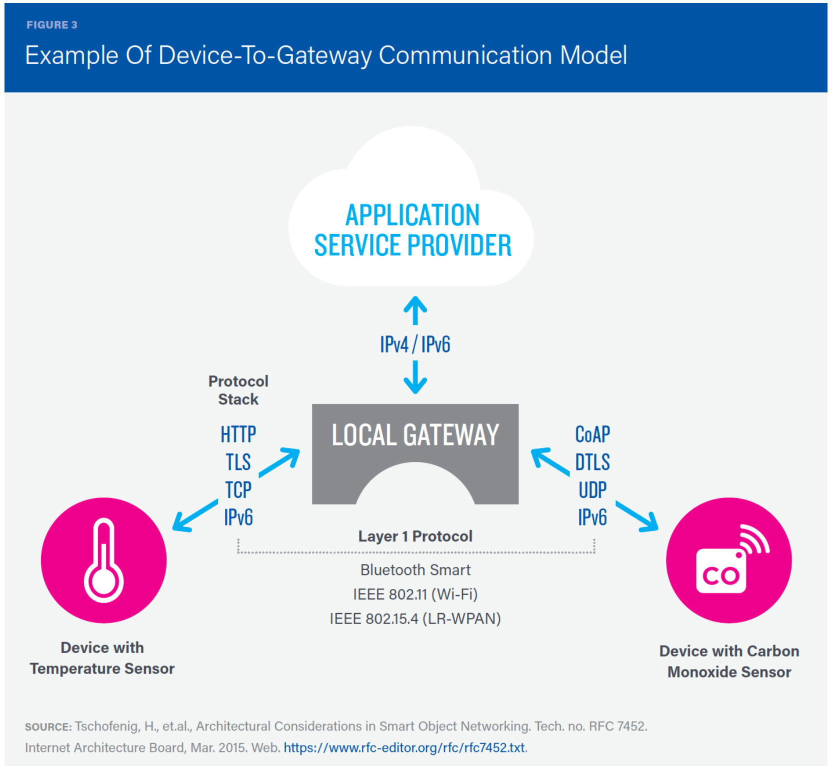
A continuous change towards a partial horizontal division of roles implies requirement for different control mechanisms throughout the architecture, between layers.

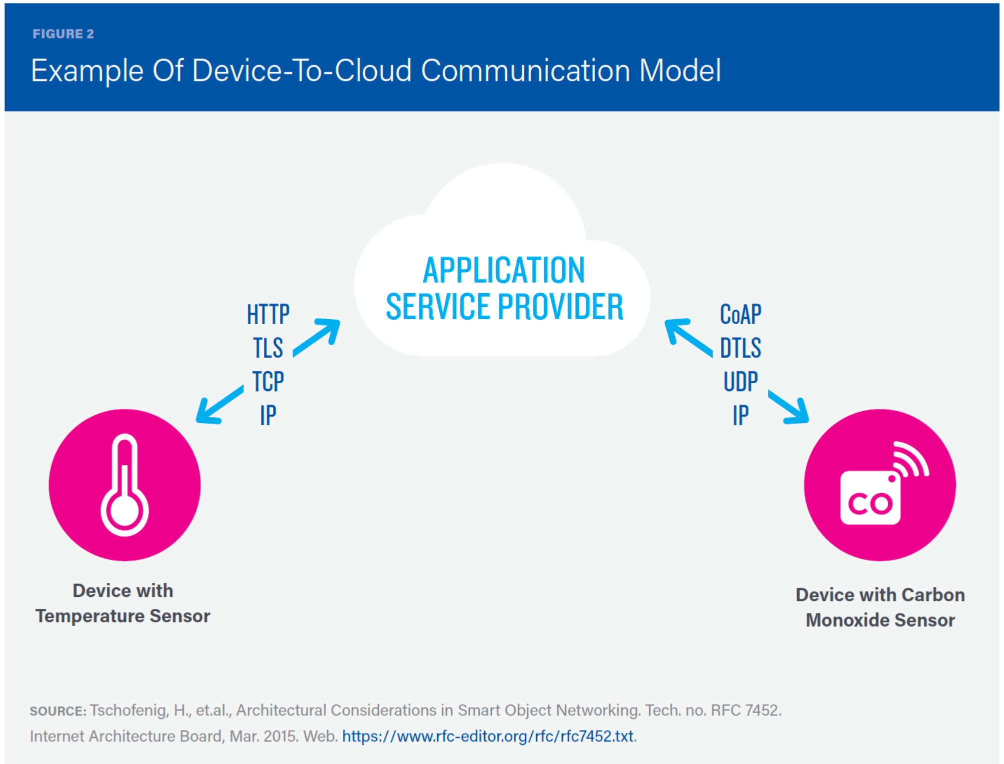
Pros:
- Simpler management of control
- Increased ability to innovate
- Standardization leads to replaceability of products and services

Cons:
- ”Markets” on different layers that do not work as efficient as possible
- Lack of control and planning
- Low skills regarding procurement
- Non-optimal risk management for the society as a whole

https://www.iva.se/det-iva-gor/projekt-och-program/digitalisering-for-okad-konkurrenskraft

Communication pattern





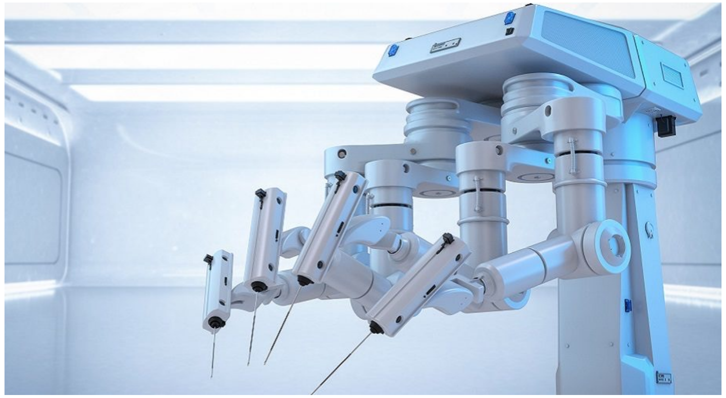
K. Rose, S. Eldridge, L. Chapin, "The Internet of Things: An Overview – Understanding the Issues and Challenges of a More Connected World", ISOC Whitepaper, October 2015

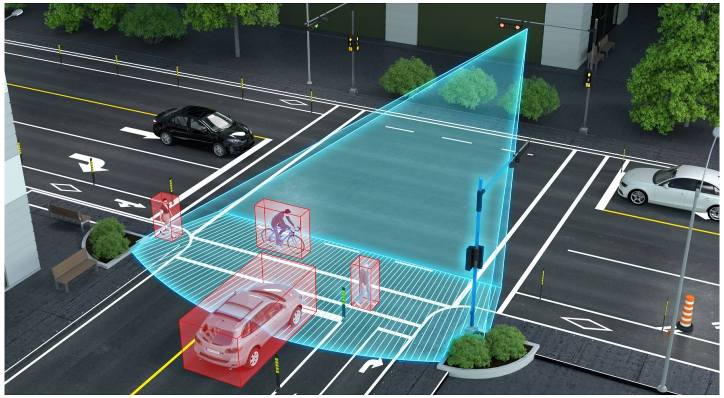
Motivation: IoT builds on the Internet today…

UNIVERSITY OF TWENTE.

SIDN LABS

And in the future

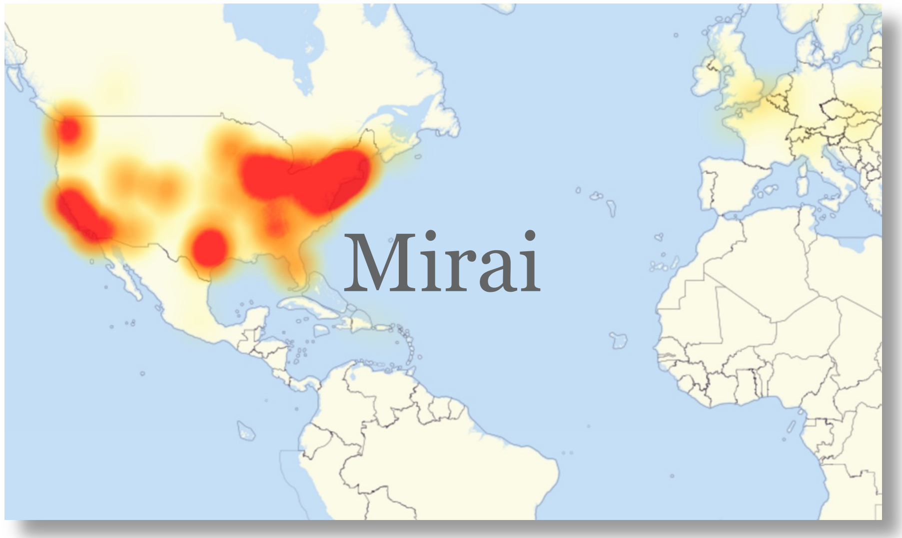


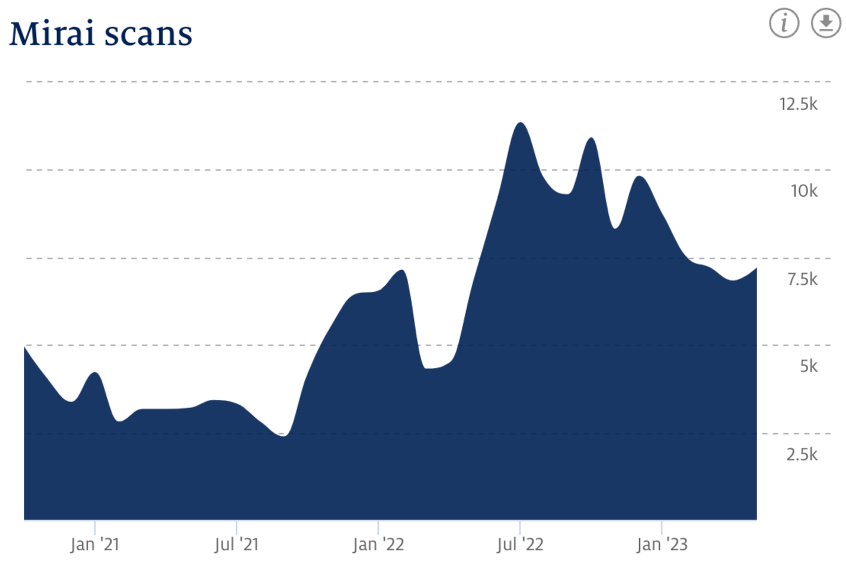


UNIVERSITY OF TWENTE.

SIDN LABS

But IoT can also impact the Internet





stats.sidnlabs.nl

UNIVERSITY OF TWENTE. SIDN LABS

So that's why we selected 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

[IPv6] P. Richter, O. Gasser, and A. Berger, "Illuminating large-scale IPv6 scanning in the internet", In Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22), New York, NY, USA, 410–418, 2022, https://doi.org/10.1145/3517745.3561452.

IPv6 challenges, such as detecting scans of IoT botnets [Mirai, Hajime]

Picture: https://blog.apnic.net/2015/09/30/ipv6-the-future-is-now-more-than-ever/

UNIVERSITY OF TWENTE. SIDN LABS

Today's learning objective

- After the lecture, you will be able to discuss the role of DNS for the IoT and the basic characteristics of the IPv6 address space and its challenges for scanning
- Limited technical depth, but important to "set the scene" for more technical papers on IoT security later in the course
- Contributes to SSI learning goal #1: "Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF"

“The DNS in IoT: Opportunities, Risks, and Challenges”

IEEE Internet Computing, July-Aug 2020

IoT Definition

No Browser. Widely Heterogeneous. Longevity. Background

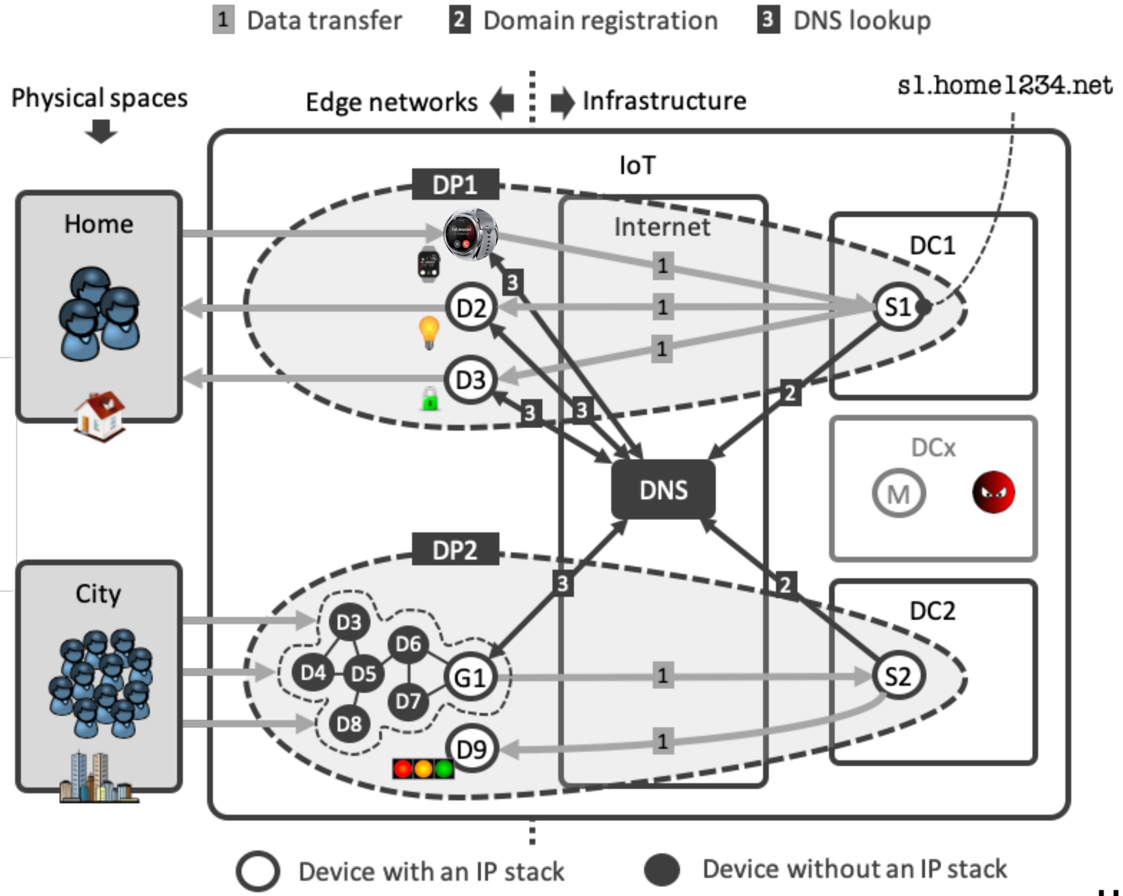
Let’s see what’s going on recently

Smart lamp with Emotion

Tablet for IoT control

Wristwatch with GPS/LTE

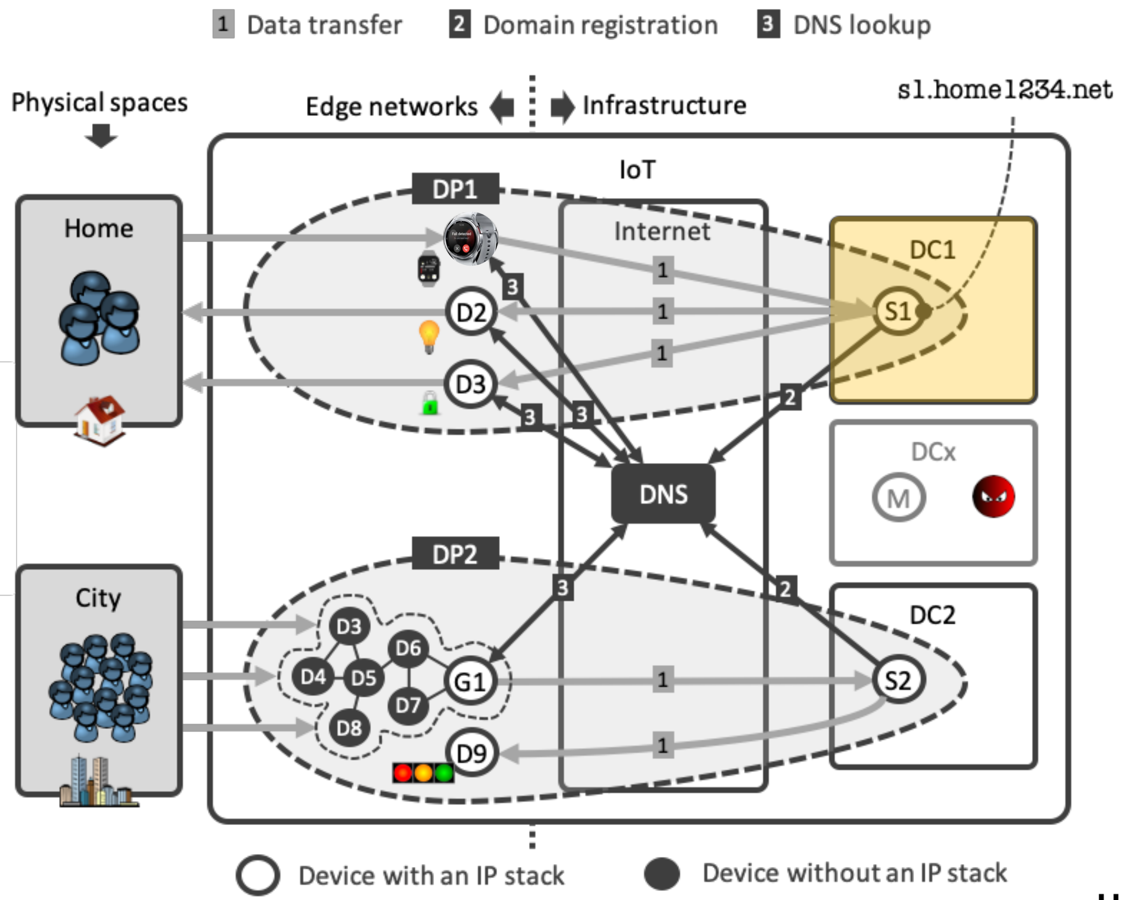
IoT deployments and the Domain Name System (DNS)



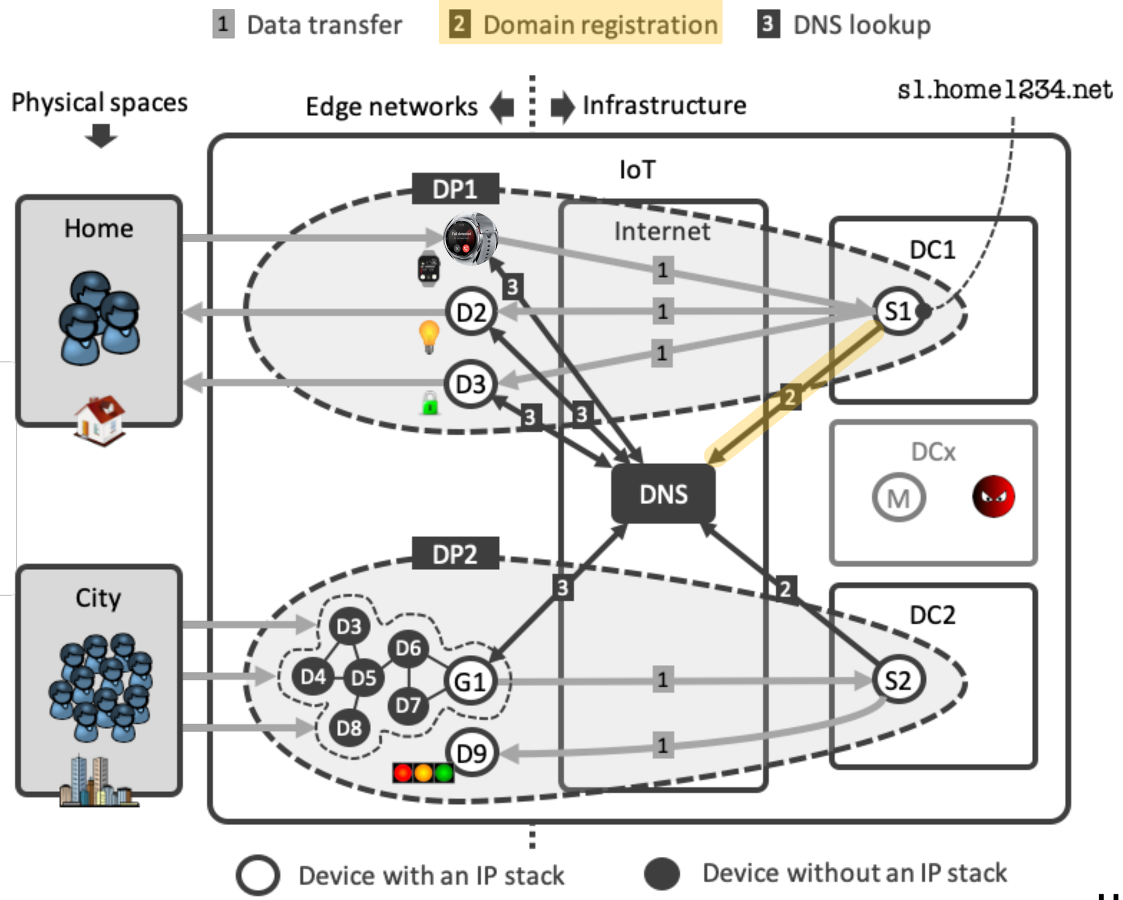
UNIVERSITY OF TWENTE.

SIDN LABS

IoT deployments and the Domain Name System (DNS)

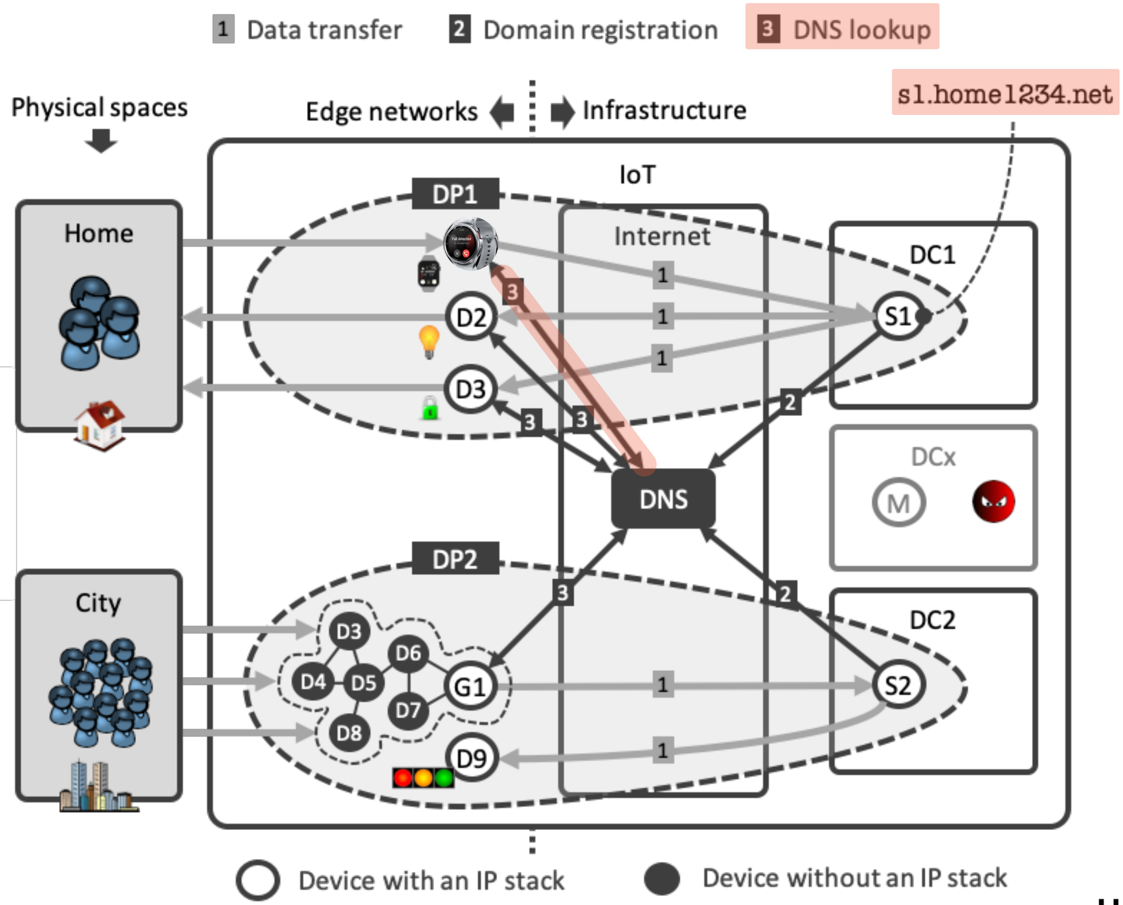


IoT deployments and the Domain Name System (DNS)

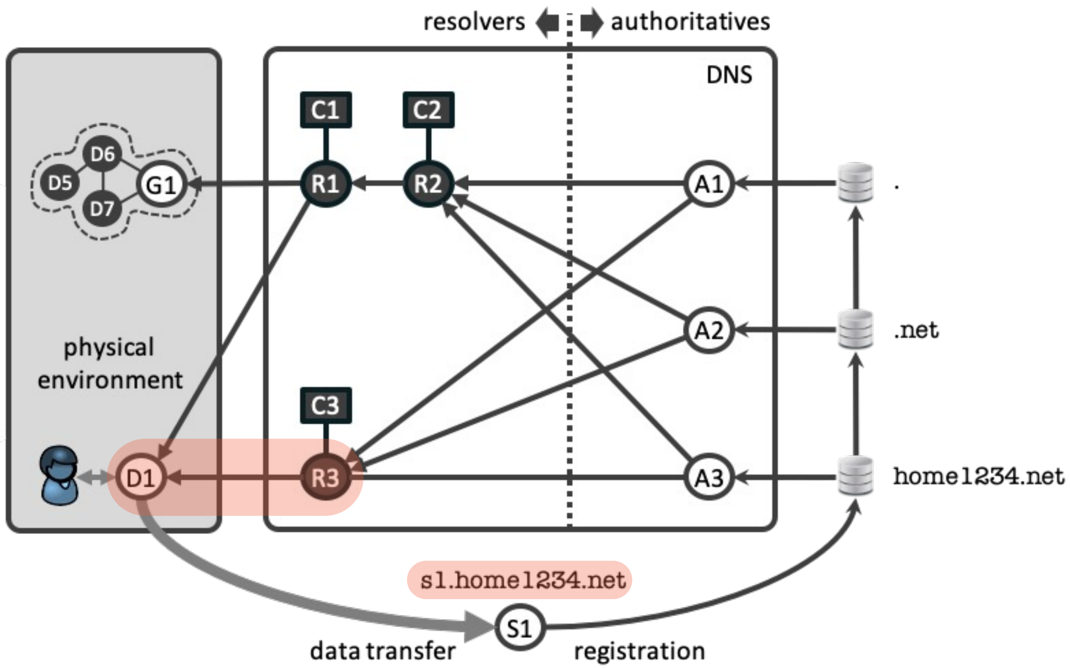


UNIVERSITY OF TWENTE. SIDN LABS

IoT deployments and the Domain Name System (DNS)

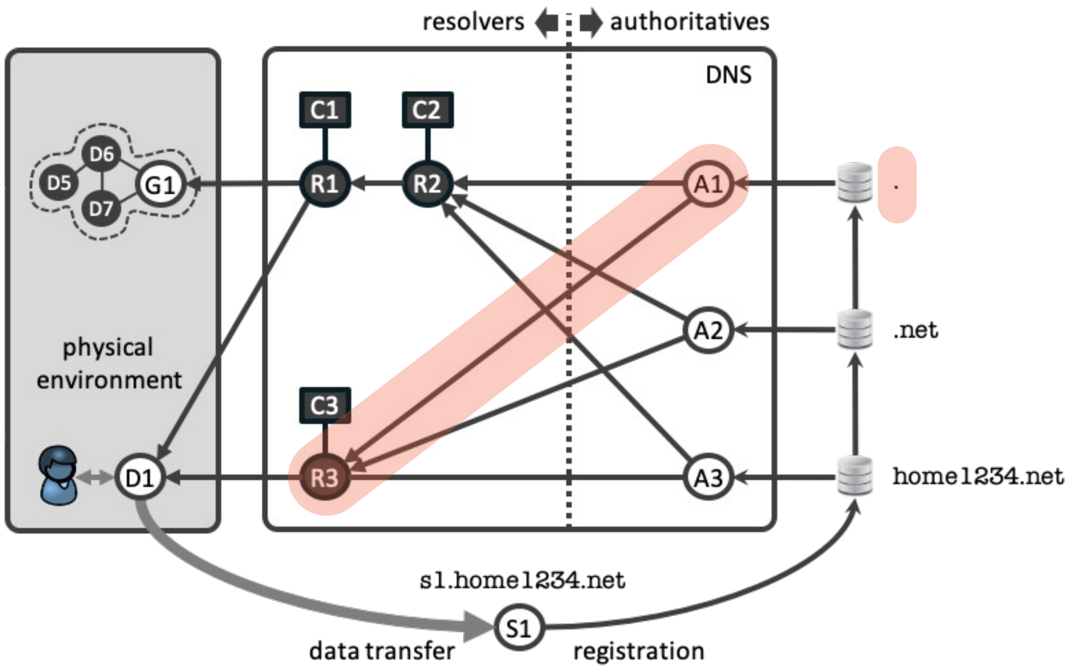


DNS high-level operation



O. van der Toorn, M. Mueller, S. Dickinson, C. Hesselman, A. Sperotto, and R. van Rijswijk-Deij, **"Addressing the Challenges of Modern DNS: A Comprehensive Tutorial"**, Elsevier Computer Science Review, 2022 (to appear)

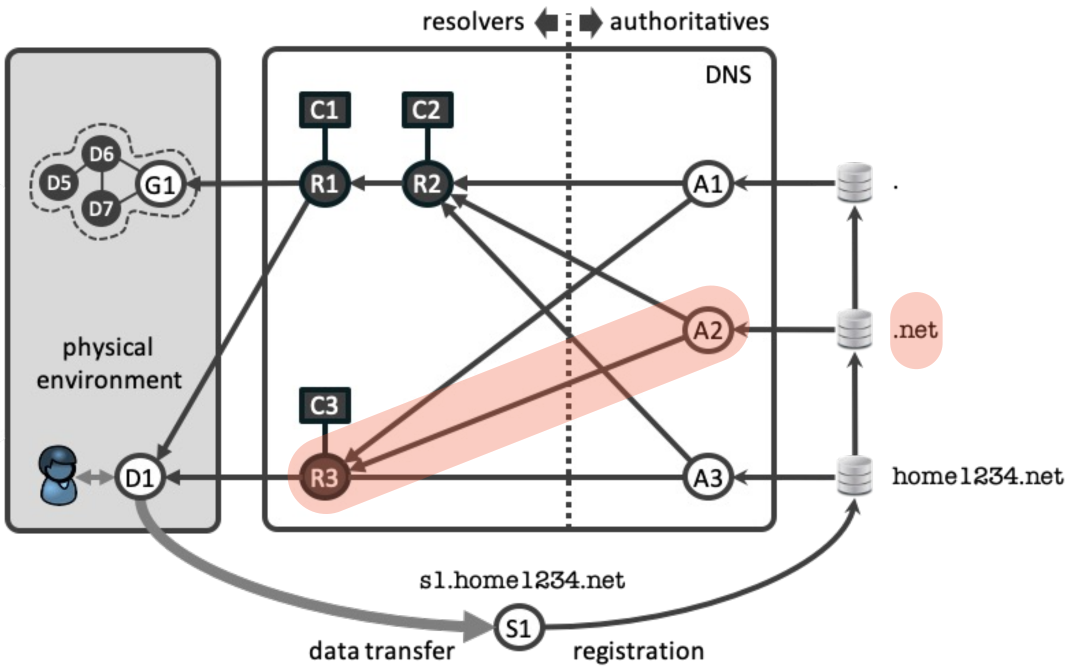
DNS high-level operation



DNS Root Server

O. van der Toorn, M. Mueller, S. Dickinson, C. Hesselman, A. Sperotto, and R. van Rijswijk-Deij, **"Addressing the Challenges of Modern DNS: A Comprehensive Tutorial"**, Elsevier Computer Science Review, 2022 (to appear)

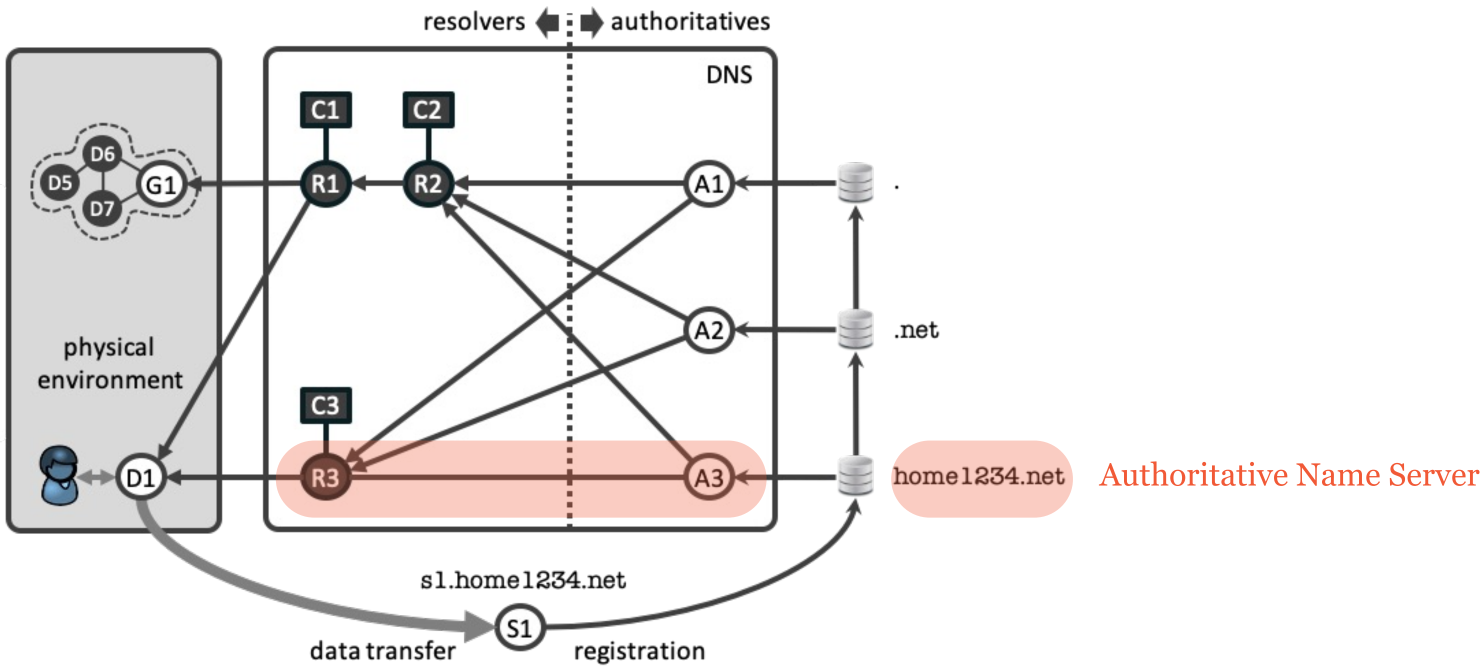
DNS high-level operation



TLD Name Server

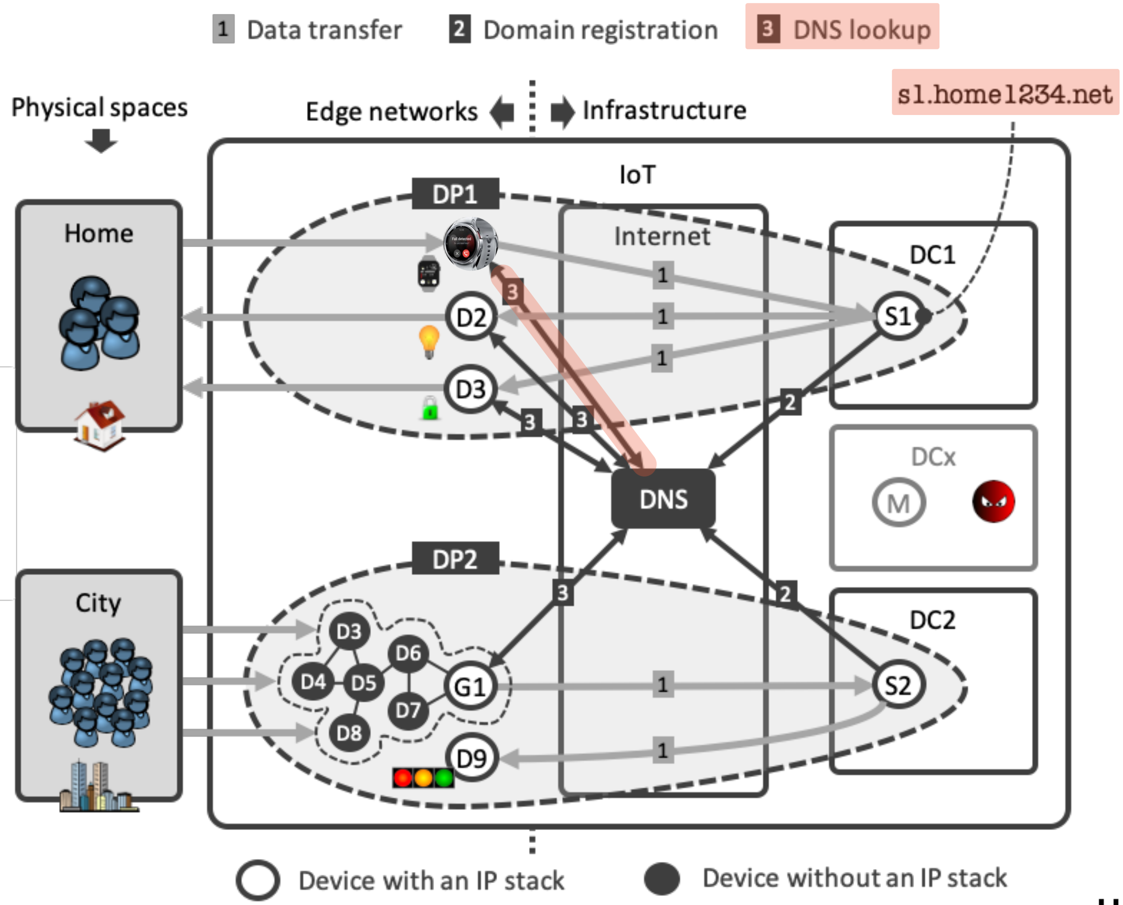
O. van der Toorn, M. Mueller, S. Dickinson, C. Hesselman, A. Sperotto, and R. van Rijswijk-Deij, **"Addressing the Challenges of Modern DNS: A Comprehensive Tutorial"**, Elsevier Computer Science Review, 2022 (to appear)

DNS high-level operation



O. van der Toorn, M. Mueller, S. Dickinson, C. Hesselman, A. Sperotto, and R. van Rijswijk-Deij, **"Addressing the Challenges of Modern DNS: A Comprehensive Tutorial"**, Elsevier Computer Science Review, 2022 (to appear)

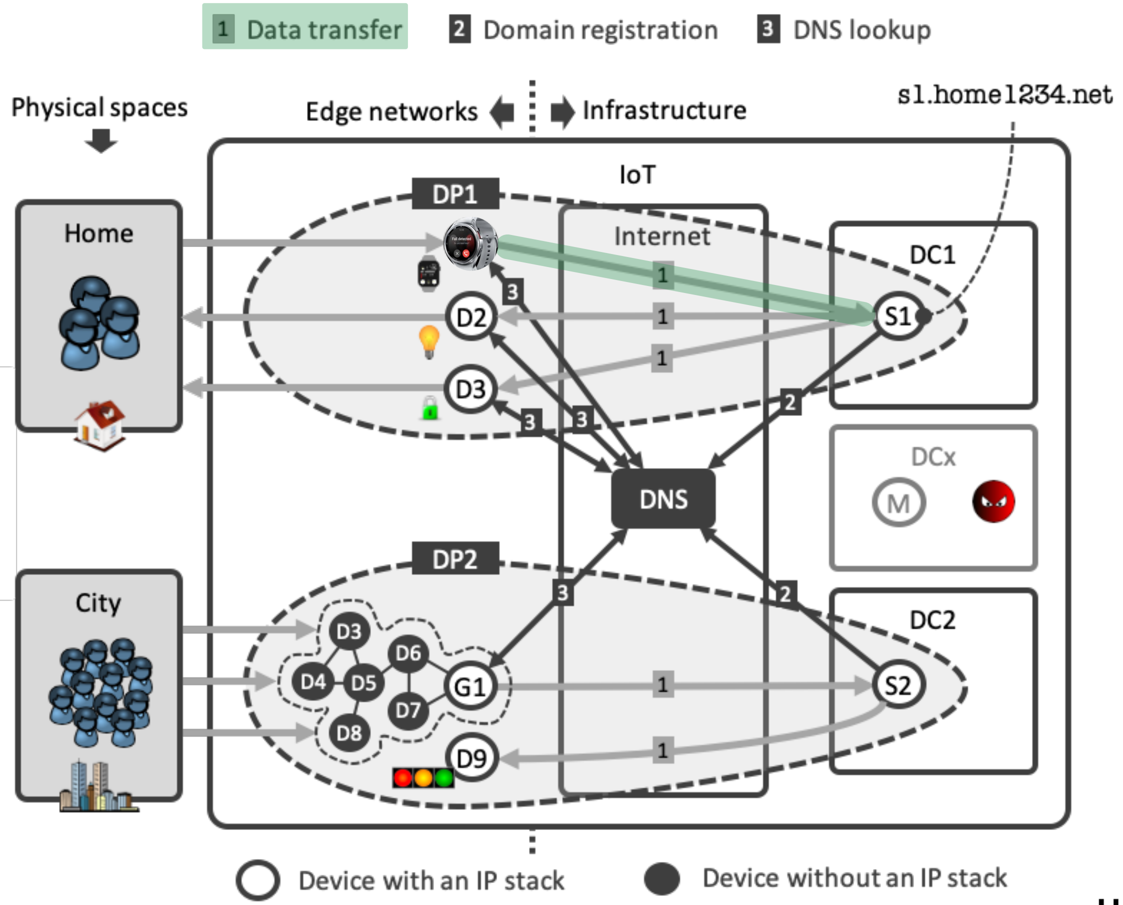
IoT deployments and the Domain Name System (DNS)



UNIVERSITY OF TWENTE.

SIDN LABS

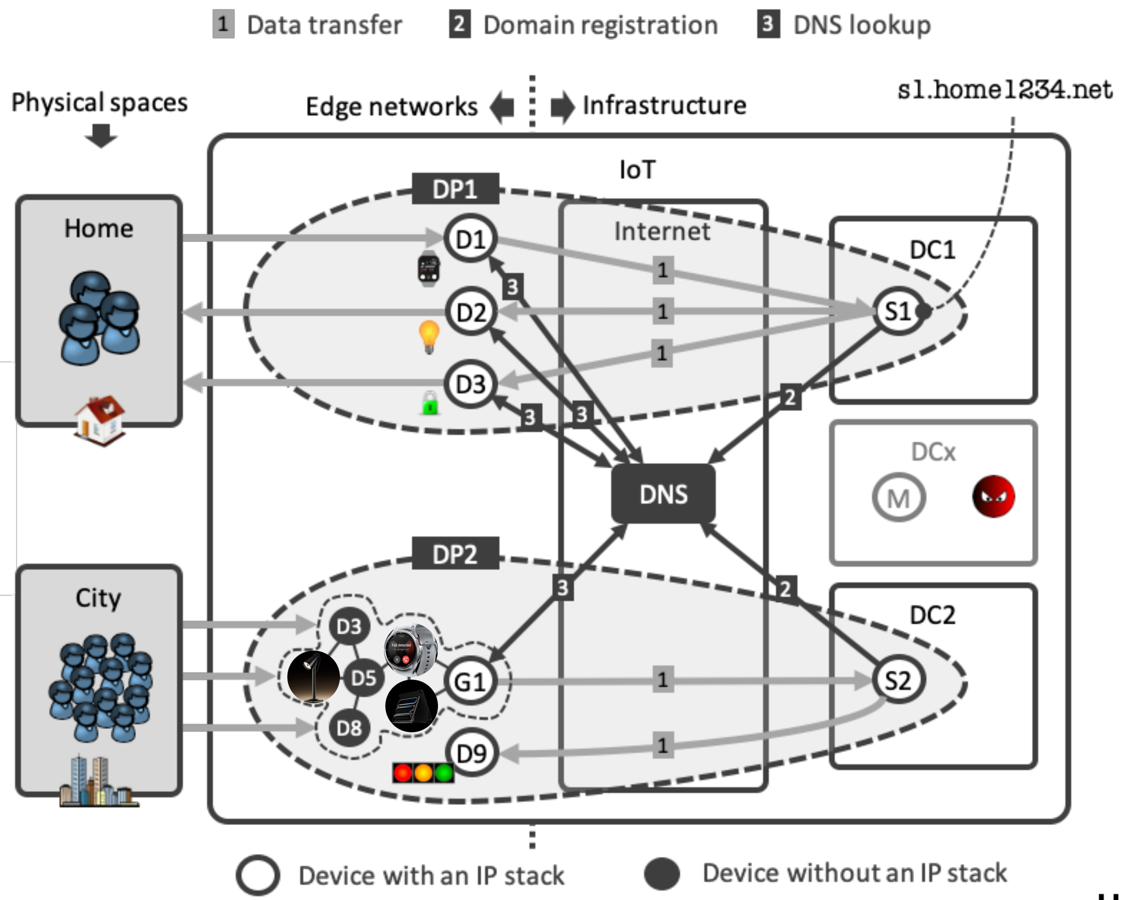
IoT deployments and the Domain Name System (DNS)



UNIVERSITY OF TWENTE.

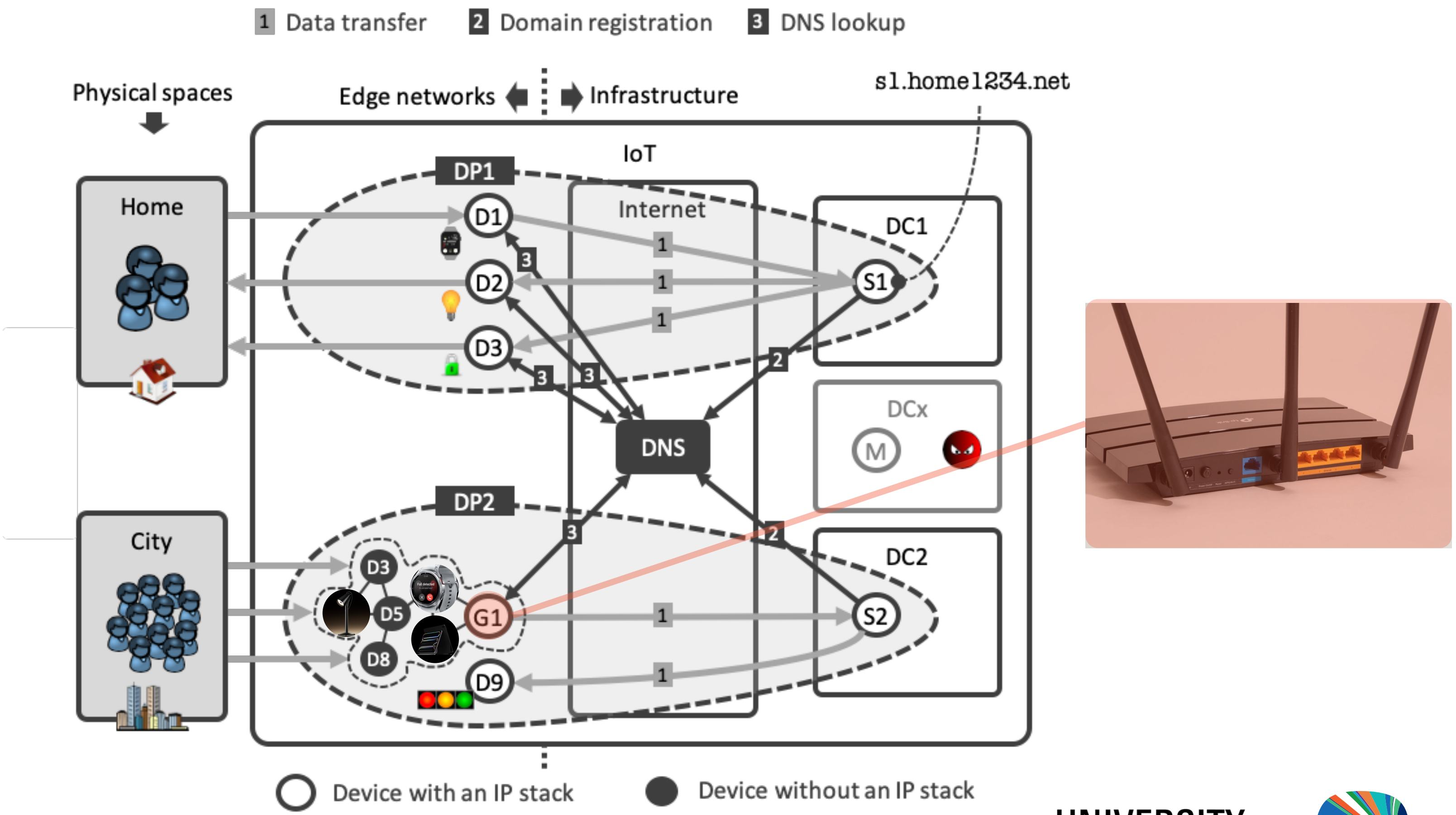
SIDN LABS

IoT deployments and the Domain Name System (DNS)



UNIVERSITY OF TWENTE. SIDN LABS

IoT deployments and the Domain Name System (DNS)



DNS Lookup Checked!

How about DNS caches?

Multiple-Choice Question:
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

DNS Lookup and DNS caches checked

Let's look at the Opportunities, Risks, and Challenges!

Overview

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

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

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

UNIVERSITY OF TWENTE. SIDN LABS

Overview

Opportunities

Help meet IoT's new safety and transparency requirements

O1 Using DoH/DoT to encrypt DNS queries

O2 Using DNSSEC to detect malicious redirects of IoT devices

O5 Using DNS datasets to increase IoT transparency

Risks

Protect the SSR of the DNS against insecure IoT devices

R1 DNS unfriendly programming at IoT scale

R2 Increased size and complexity of IoT botnets targeting the DNS

Challenges

Technologies and systems that need to be developed

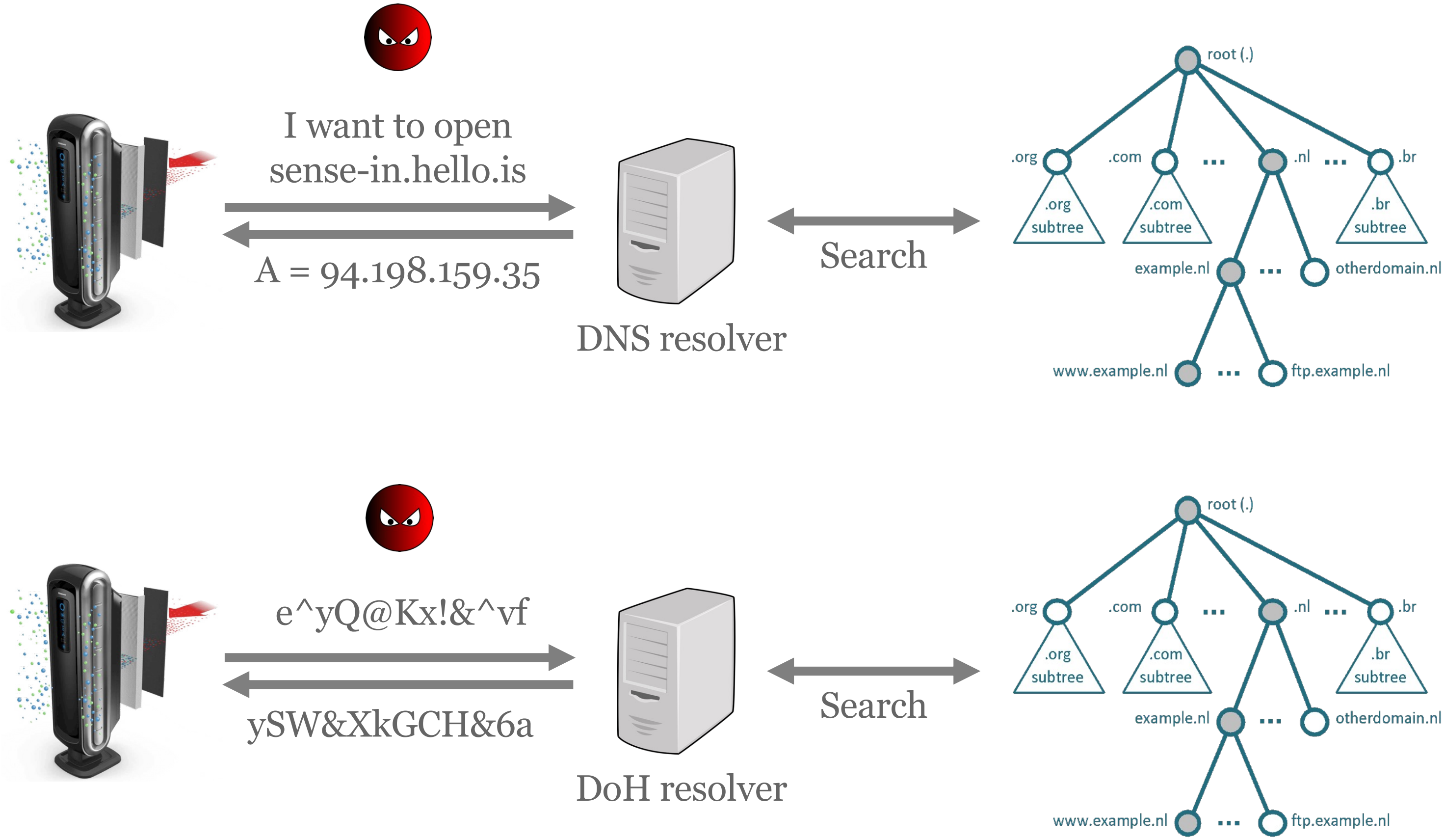
C1 Developing a DNS security and transparency library for IoT devices

C3 Developing a system to share information on IoT botnets

C4 Proactive and flexible mitigation of IoT-powered DDoS traffic

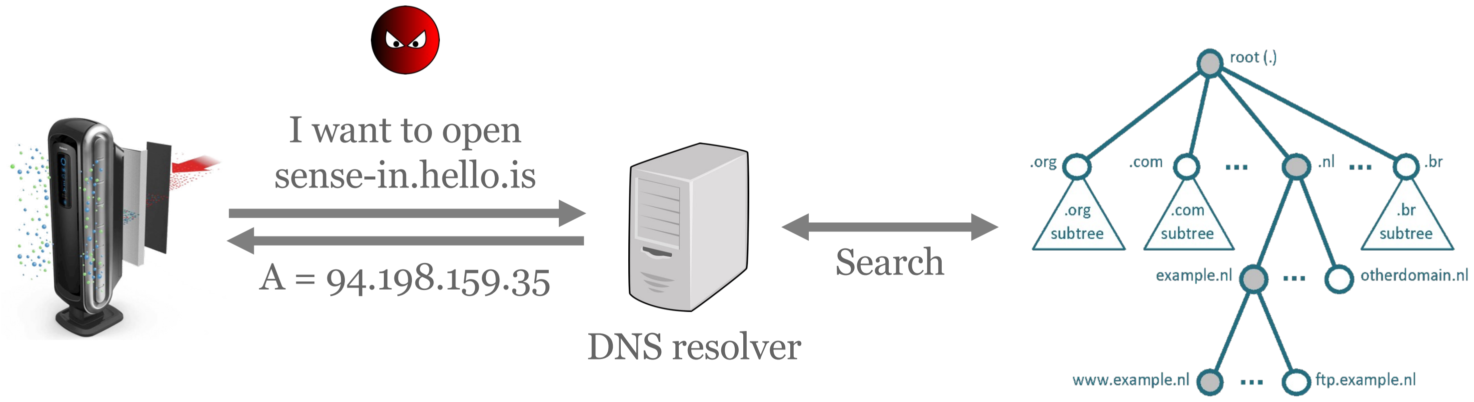
UNIVERSITY OF TWENTE. SIDN LABS

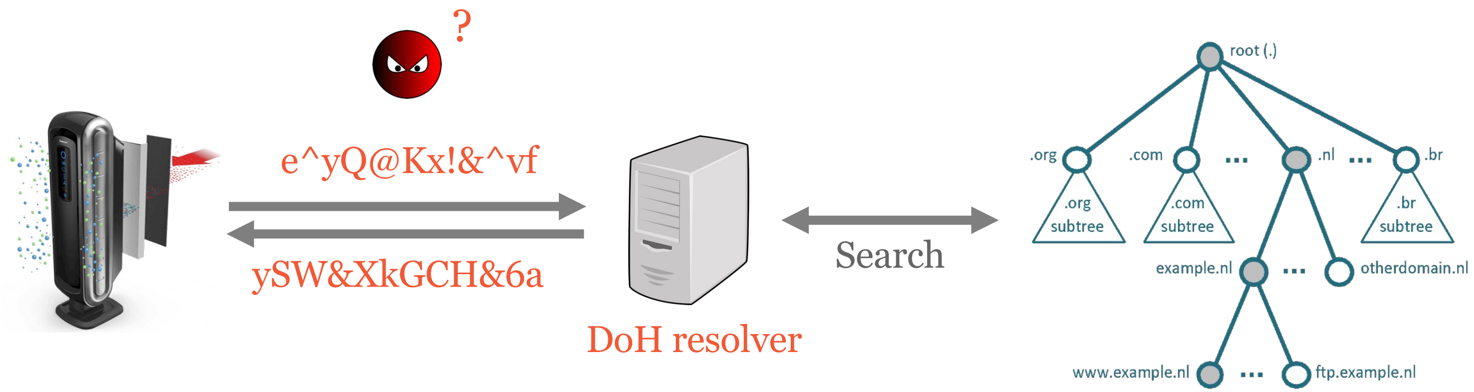
01 Using DoH/DoT to encrypt DNS queries



UNIVERSITY OF TWENTE. SIDN LABS

01 Using DNS-over-HTTPS to encrypt DNS queries





UNIVERSITY OF TWENTE.
SIDN LABS

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)

[Castle] 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

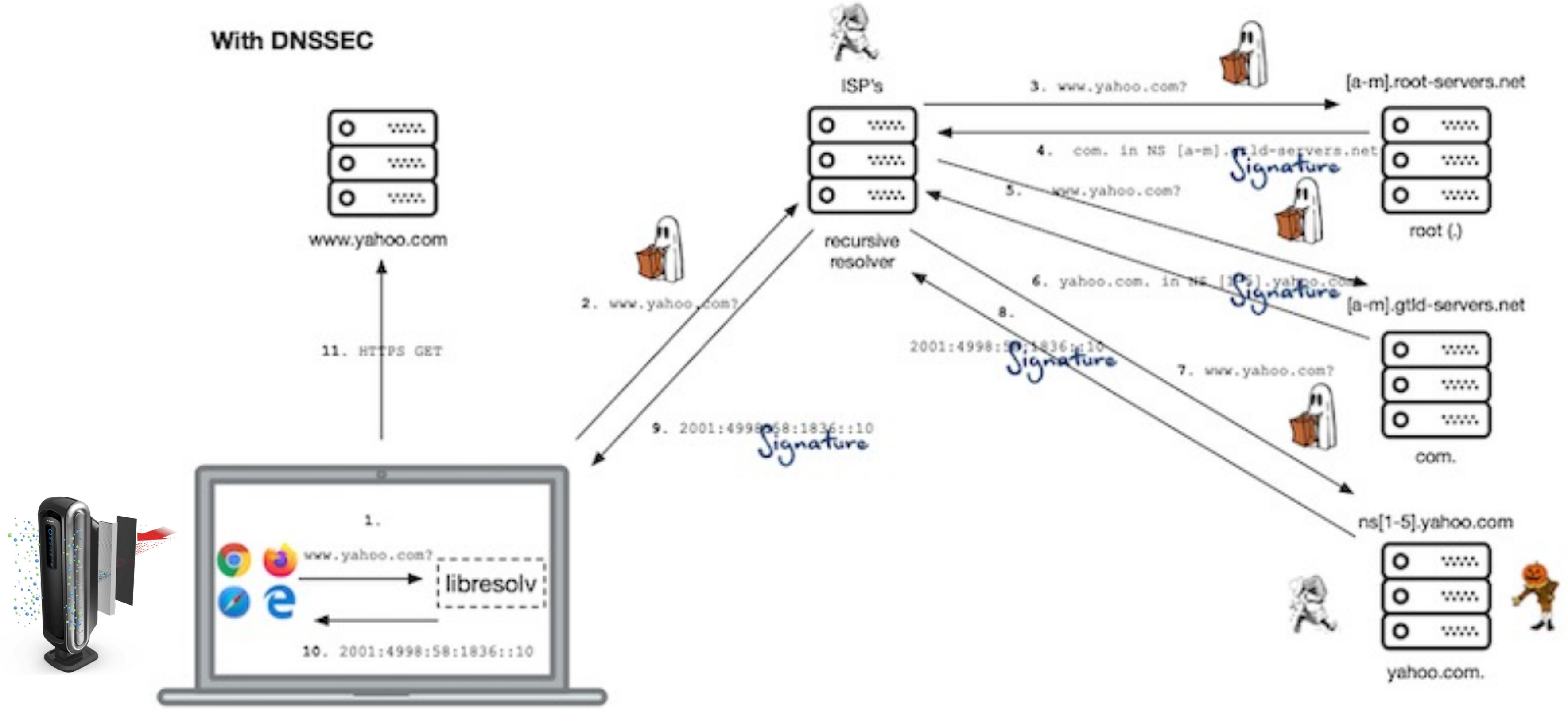
Device	DNS Queries
Sense Sleep Monitor	hello-audio.s3.amazonaws.com hello-firmware.s3.amazonaws.com messeji.hello.is ntp.hello.is sense-in.hello.is time.hello.is
Nest Security Camera	nexus.dropcam.com oculus519-vir.dropcam.com pool.ntp.org
WeMo Switch	prod1-fs-xbcs-net-1101221371.us-east-1.elb.amazonaws.com 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.

UNIVERSITY OF TWENTE.

SIDN LABS

O2 Signing DNS responses with DNSSEC



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

UNIVERSITY OF TWENTE. SIDN LABS

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

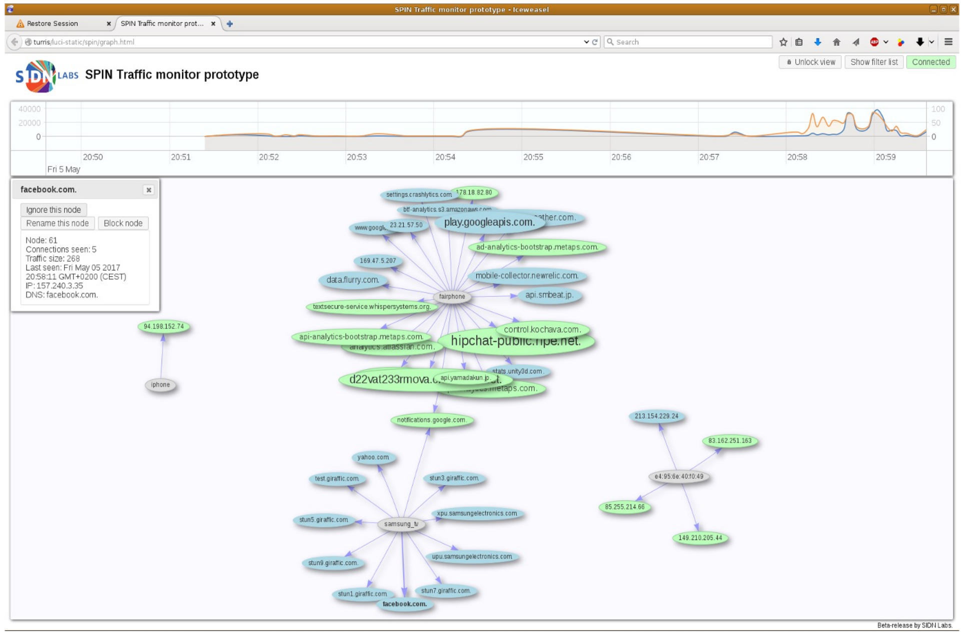
- DNSSEC reduces safety risk: lowers probability of IoT device receiving malicious instructions (cf. air purifier)

- Most secure setup: signature validation on IoT devices

If you were IT operators

Would you apply these? Is there still a concern?

O5 Using DNS datasets to increase IoT transparency



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

- 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

UNIVERSITY OF TWENTE. SIDN LABS

Open question:
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

- Actually, this does not apply to DNS alone. Unfriendly programming and Software update can cause trouble everywhere like large company

TUNE IN 2 TUNE OUT

UNIVERSITY OF TWENTE. SIDN LABS

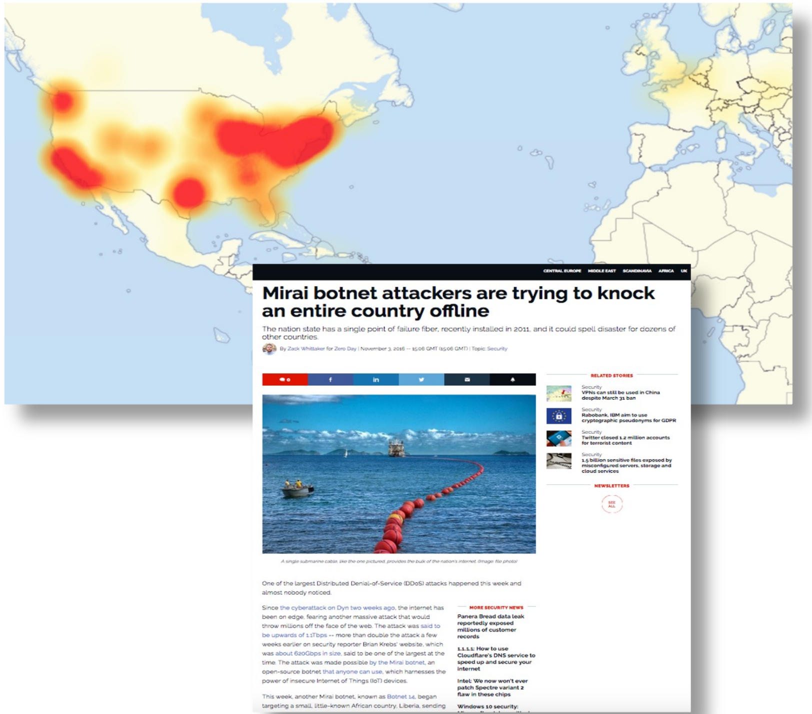
If you're the manager/engineer

What would you do to prevent this?

UNIVERSITY OF TWENTE. SIDN LABS

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)



UNIVERSITY OF TWENTE.

SIDN LABS

Open question:
What do you think will make IoT botnets more difficult to eradicate than a traditional ones?

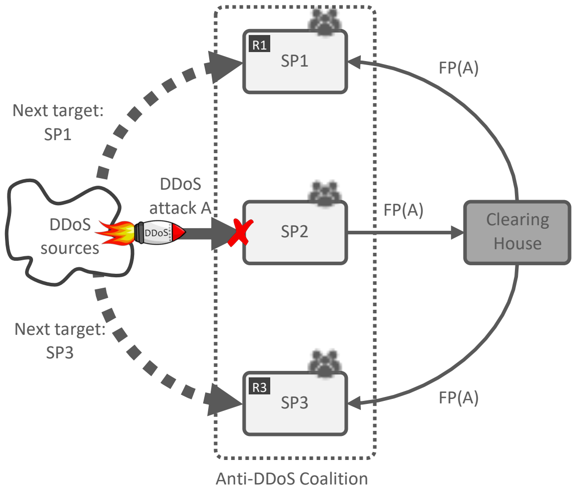
Why collaborative?

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

[Mirai]

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	AWS EC2	11/02/2016–02/28/2017	141 binaries
	Telnet honeypots	Akamai	11/10/2016–02/13/2017	293 binaries
	Malware repository	VirusTotal	05/24/2016–01/30/2017	594 binaries
	DNS — active	Georgia Tech	08/01/2016–02/28/2017	290M RRs/day
	DNS — passive	Large U.S. ISP	08/01/2016–02/28/2017	209M RRs/day
Attack characterization	C2 milkers	Akamai	09/27/2016–02/28/2017	64.0K attack commands
	DDoS IP addresses	Akamai	09/21/2016	12.3K IP addresses
	DDoS IP addresses	Google Shield	09/25/2016	158.8K IP addresses
	DDoS IP addresses	Dyn	10/21/2016	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 details: antiddoscoalition.nl

UNIVERSITY OF TWENTE. SIDN LABS

A platform for collaboration

Sounds good, but what are pros and cons?

UNIVERSITY OF TWENTE.

SIDN LABS

Do you think your device is safe?

What will you do after this lecture?

UNIVERSITY OF TWENTE.

SIDN LABS

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

Overview

Opportunities

Help meet IoT's new safety and transparency requirements

O1 Using DoH/DoT to encrypt DNS queries

O2 Using DNSSEC to detect malicious redirects of IoT devices

O5 Using DNS datasets to increase IoT transparency

Risks

Protect the SSR of the DNS against insecure IoT devices

R1 DNS unfriendly programming at IoT scale

R2 Increased size and complexity of IoT botnets targeting the DNS

Challenges

Technologies and systems that need to be developed

C1 Developing a DNS security and transparency library for IoT devices

C3 Developing a system to share information on IoT botnets

C4 Proactive and flexible mitigation of IoT-powered DDoS traffic

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

UNIVERSITY OF TWENTE. SIDN LABS

Open question:
What do you think is the most important challenge for IoT security?

“Illuminating Large-Scale IPv6 Scanning in the Internet”

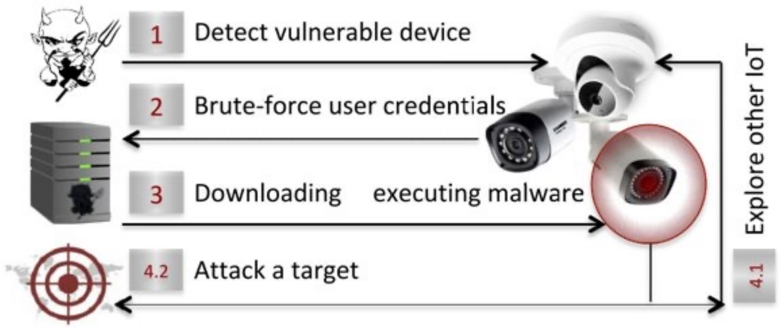
22nd ACM Internet Measurement Conference (IMC ’22), New York, USA, 2022

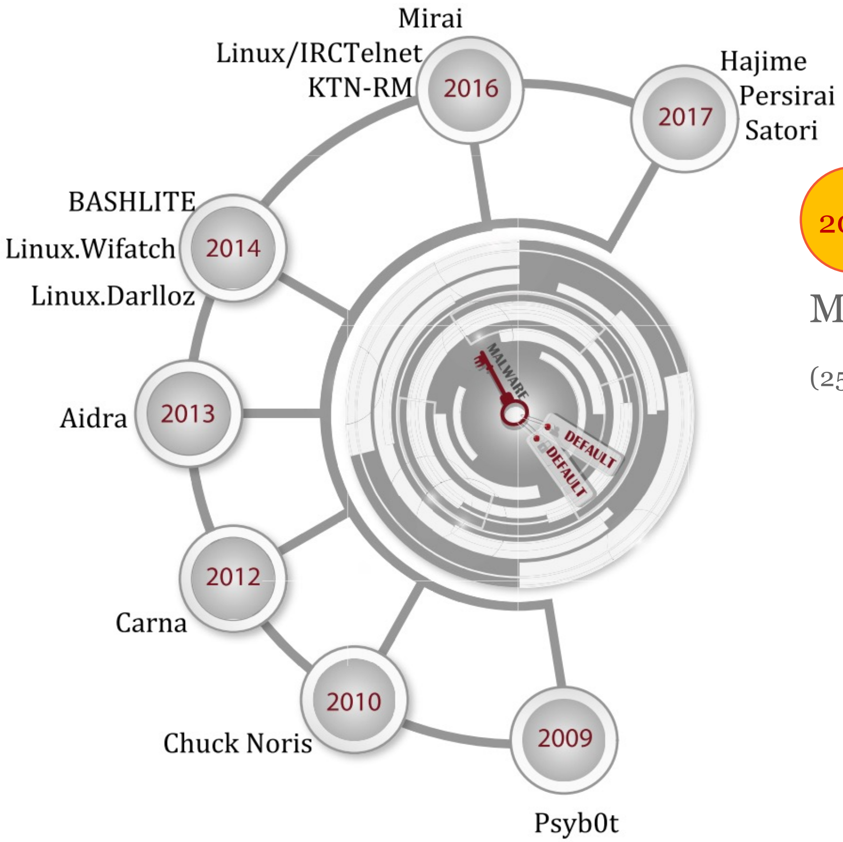
What struck you about the paper?

UNIVERSITY OF TWENTE.

SIDN LABS

One type of scanner: IoT botnets (currently only IPv4)





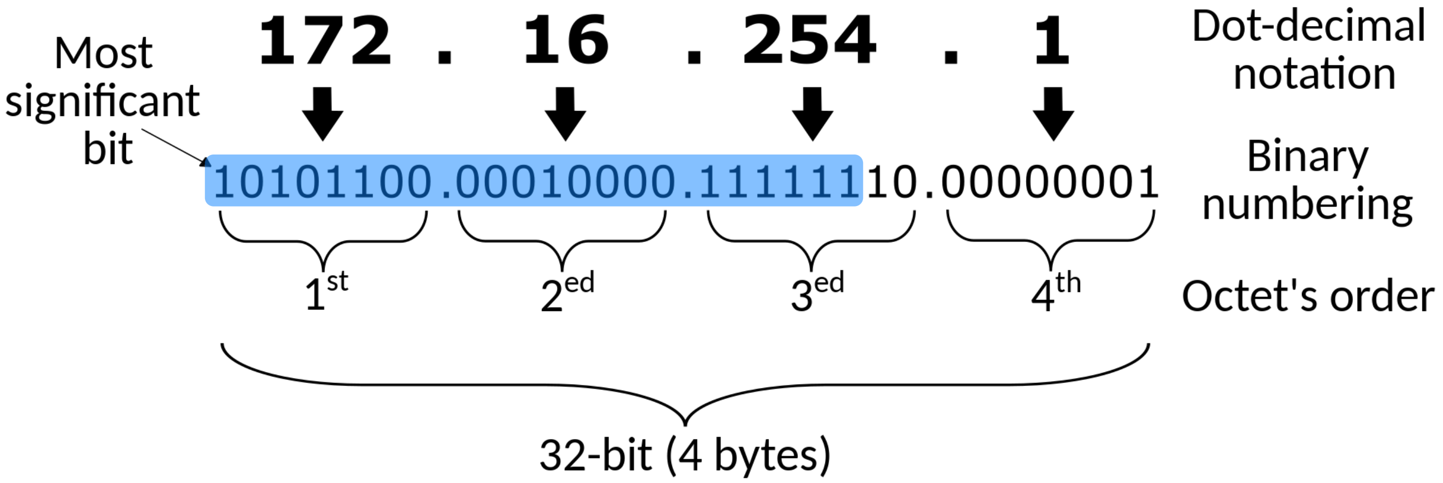
2021

Mēris

(250k infected MikroTik routers)

Figures from: Neshenko et al., "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations", IEEE Communications Surveys & Tutorials, Vol. 21, No. 3, Third Quarter 2019

IPv4 address space



/22

https://en.wikipedia.org/wiki/Internet_Protocol_version_4#Addressing

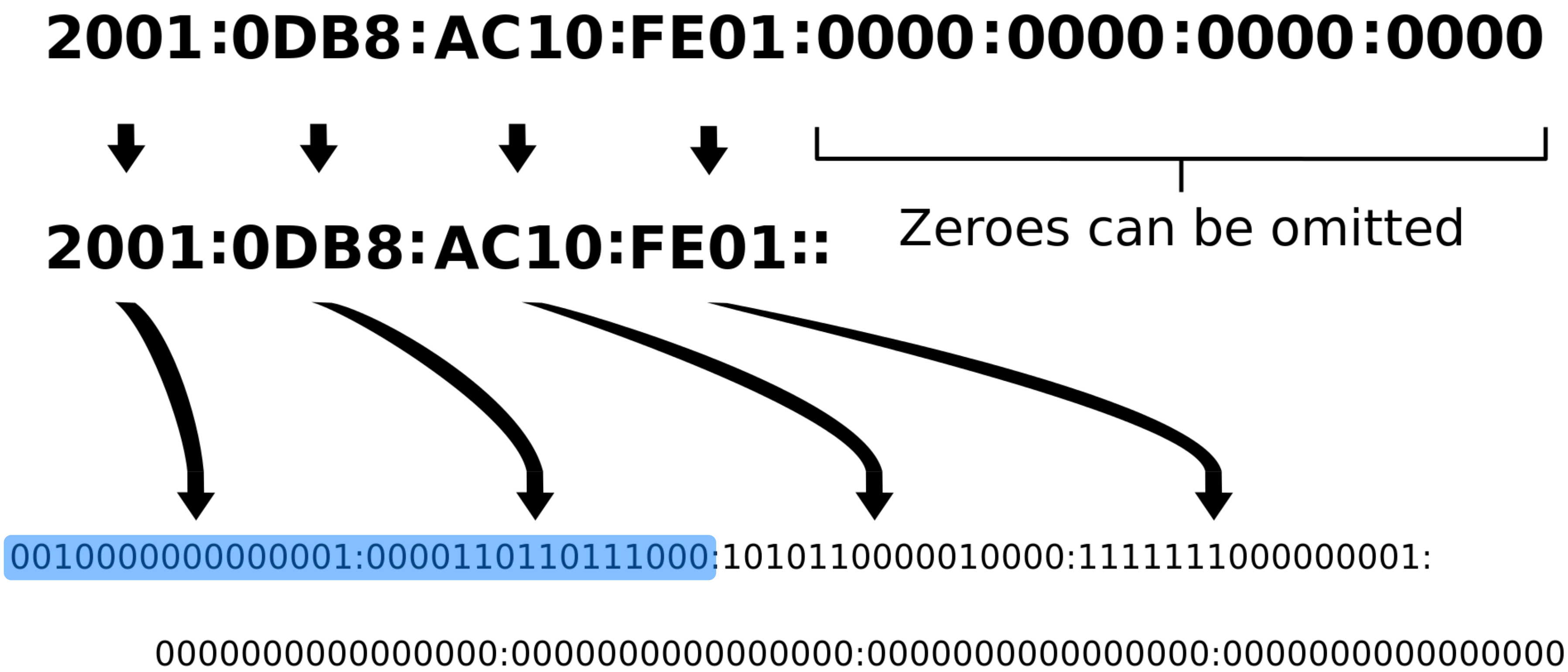
UNIVERSITY OF TWENTE. SIDN LABS

Quiz question #1

How long would it take to scan the **IPv4** address space on a typical desktop computer, approximately?

A. A week
B. A day
C. An hour
D. A minute

IPv6 address space



/32

https://en.wikipedia.org/wiki/IPv6_address

Challenge #1: scanning the IPv6 address space

- How long you recon it would approximately take to scan the the *full* IPv6 address space?
  - "Full" includes reserved IPv6 address ranges
  - For example, addresses for multicast, anycast, documentation

- Using the current rates of IPv4 scans, that would be some **$9*10^{24}$ years**
  - Full IPv4 scan currently takes about an hour
  - In one year, we can scan around $2^{32}*24*365$ IPv4 addresses
  - So, 2^{128} addresses would take $2^{128}/(2^{32}*24*365) = 9*10^{24}$ years

- Won't even work if we use all the estimated 20-30B IoT devices in the world simultaneously to conduct the scan!

Discussion question #1

- If you were a scan actor (e.g., an IoT botnet operator), what approach would you take to scan the vast IPv6 address space?

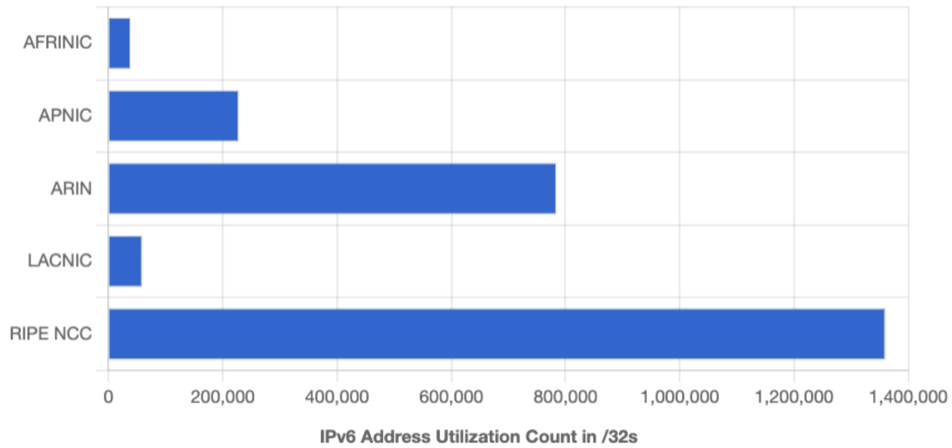
Approach #1: scan *allocated* address space only

- How long would that take?

- That will take "just" **$5,2*10^{21}$** years ☺
  - 2.473.315 /32s allocated in May 2024
  - $2.473.315*2^{96} \approx 1.96*10^{35}$ IPv6 addresses
  - $1.96*10^{35}/(2^{32}*24*365) = 5,21*10^{21}$ years

- How to further reduce our search space?

Source: https://www.iana.org/numbers/allocations/

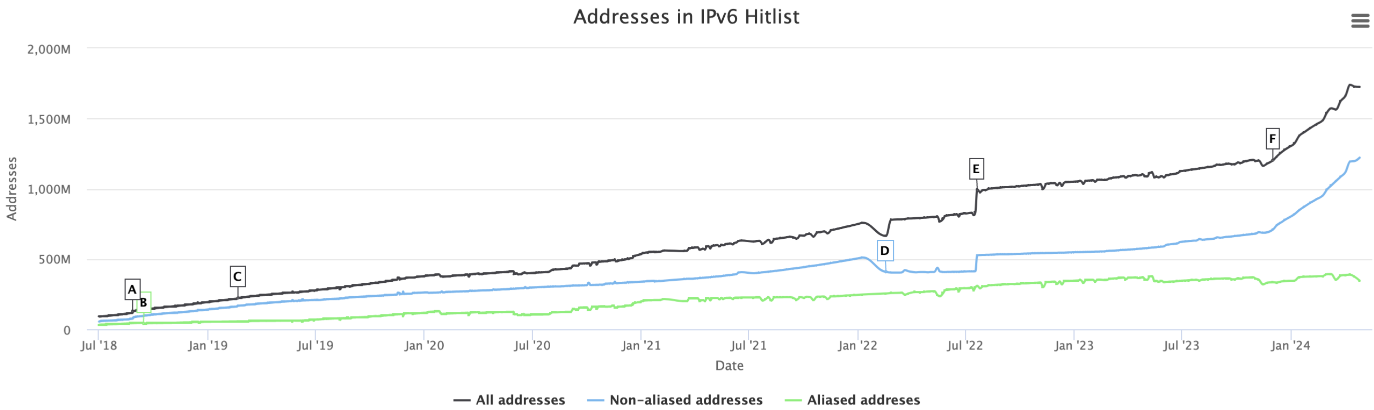


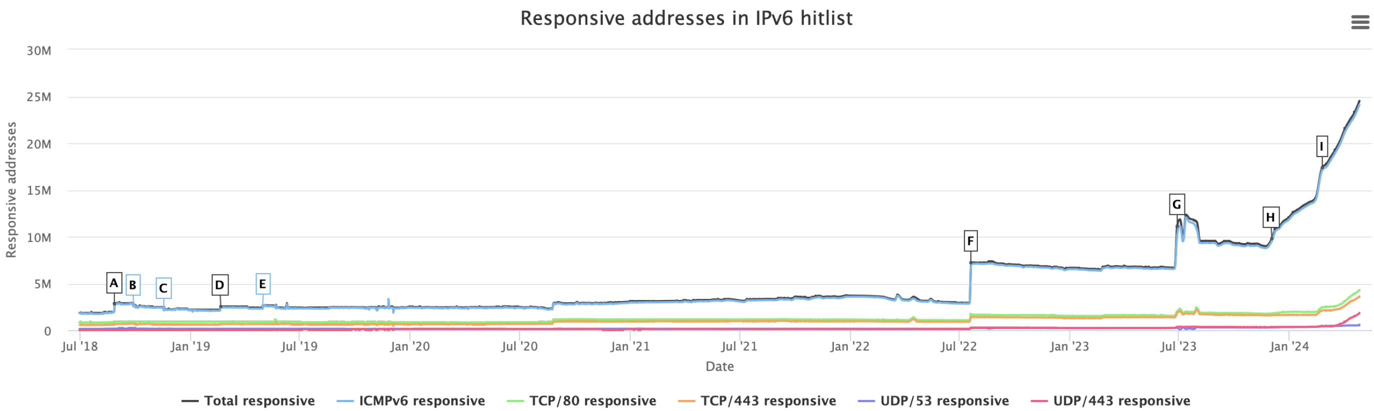
Approach #2: scan addresses …

Approach #2: scan addresses *in use*

- How would you create such an IPv6 hitlist?
- Investigate DNS entries: for 75% of /64 scan sources, all probed addresses are in the DNS
- Not-in-DNS targets: scan “nearby” addresses of IPs that are in the DNS (e.g., within a /124)
- Measurements of data flows to flag IPv6 addresses being used, such as at IXPs

Example IPv6 hitlist: https://ipv6hitlist.github.io/





UNIVERSITY OF TWENTE.

SIDN LABS

Additional reading on IPv6 scanning

O. Gasser et al., “Scanning the IPv6 Internet: Towards a Comprehensive Hitlist”, TMA 2016.

O. Gasser et al., “Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists”, IMC 2018.

J. Zirngibl et al., “Rusty Clusters? Dusting an IPv6 Research Foundation”, IMC 2022.

UNIVERSITY OF TWENTE.

SIDN LABS

Challenge #2: detecting IPv6 scanners

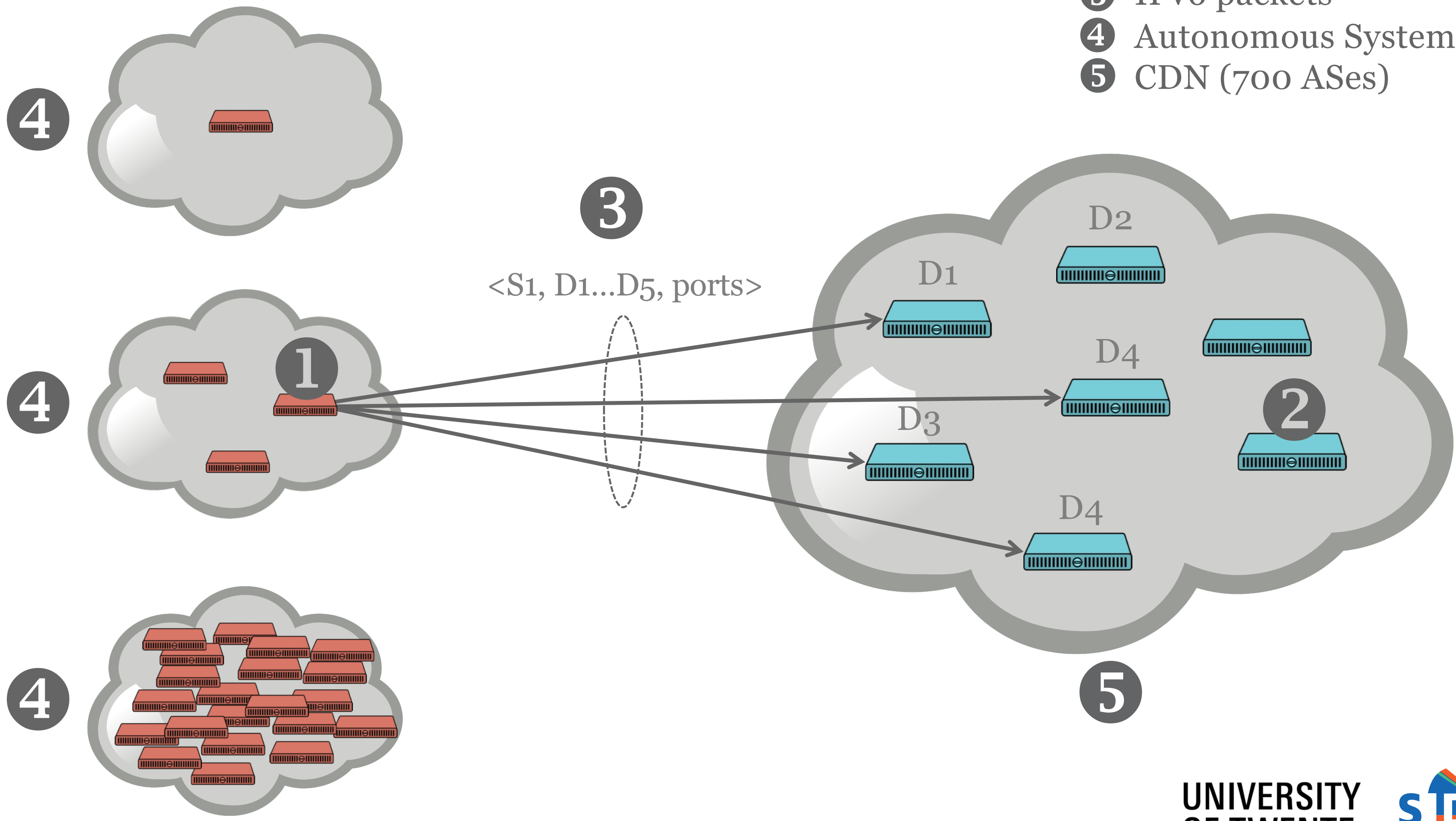
- What would that take?

- A sizable measurement infrastructure to attract “enough” traffic, such as the CDN in the paper

- A methodology to detect scan *actors*, which may use trillions of different IP addresses

Paper measurement setup

1. Scannning source
2. Server (320K)
3. IPv6 packets
4. Autonomous System (1 AS)
5. CDN (700 ASes)



UNIVERSITY OF TWENTE. SIDN LABS

What’s their methodology?

1. Collect IPv6 source addresses of scanners across the 320K servers of the CDN for 15 months

2. Create clusters of IPv6 addresses (scan sources)
   - Using well-known IPv6 prefixes
   - /48, /64, and /128

3. Apply scan detection methodology (e.g., 100+ destinations probed)

4. Lookup ownership of the /48s and /64s in the WHOIS databases at RIRs

UNIVERSITY OF TWENTE.

SIDN LABS

Scan detection methodology

- How does the paper detect IPv6 scanners?
- The authors leverage a CDN network of 320.000 nodes
- Single out "large-scale" scans: a source is a scan source if it contacts ≥100 destination IPs within the CDN, with a timeout of max 3.600 seconds
- Remove sources repeated failing connection attempts, which are those that hit the same destination IP more than 5 times in a single day
- Ports 80 and 443 not considered because of lots of legitimate use

Results from the paper: scan sources

Top 5 accounts for 92.8% of scan packets

Top 10 accounts for 99% of scan packets

rank	AS type	packets	scan sources /48s	/64s	/128s
#1	Datacenter (CN)	839M (39.2%)	1	1	1
#2	Datacenter (CN)	744M (34.8%)	1	1	5
#3	Cybersecurity (US)	275M (12.9%)	1	1	12
#4	Cloud (US/global)	78M (3.7%)	2	2	512
#5	Cloud (DE)	48M (2.3%)	3	59	59
#6	Cloud (US/global)	45M (2.1%)	10	15	205
#7	Cloud (US/global)	39M (1.8%)	9	9	123
#8	Cloud (CN)	30M (1.4%)	5	5	53
#9	Transit (global)	11M (0.5%)	1	2	956
#10	Cloud (CN)	10M (0.5%)	1	1	7
#11	Cloud (US/global)	4.7M (0.2%)	1	1	353
#12	Datacenter (CN)	3.1M (0.1%)	9	12	19
#13	ISP (VN)	2.5M (0.1%)	1	1	1
#14	Datacenter (CN)	1.6M (≤ 0.1%)	1	1	2
#15	Research (DE)	1.1M (≤ 0.1%)	1	1	1
#16	ISP (RU)	0.9M (≤ 0.1%)	1	1	2
#17	University (DE)	0.8M (≤ 0.1%)	1	1	2
#18	Cloud/Transit (DE)	0.6M (≤ 0.1%)	1,092	1,057	1,057
#19	ISP (RU)	0.6M (≤ 0.1%)	1	1	1
#20	University (DE)	0.5M (≤ 0.1%)	1	1	1

Scan sources mostly limited to datacenters and cloud providers, no networks that exclusively connect residential users

Results from the paper: target ports

- IPv6 scans currently scan a range of ports, like penetration testing
  - AS #1 targets some 444 different ports in the first half of 2021, and then only ports 22, 3389, 8080, and 8443 starting in May 2021.
  - AS #3: almost the entire port space, 45k ports.
  - AS #18: only scans port 22.

- Port selection characteristics can be used to attribute scans to entities

- (IPv4 scans typically target a single port)

- Which ports would you scan?

UNIVERSITY OF TWENTE. SIDN LABS

Discussion question #2

- What are design parameters for an IPv6 scanner detection algorithm?

- Detection vantage points: a large-scale CDN in the paper, but would there be others?

- Aggregation level
  - Too specific: can lead to missing scanning activities in part or entirely
  - Too coarse: conflating individual scan actors
  - In operational settings, the latter may lead to blocking legitimate sources

- Other design choices?

Key Takeaways

- Challenge #1: IPv6 scanning, which is more complicated than with IP4
- Challenge #2: infrastructure and methodology for detecting scan sources (e.g., aggregation level)
- Observations from the paper:
  - Large-scale IPv6 scans are relatively rare compared to IPv4
  - Scan actors mostly operate out of data centers, no residential ISPs
  - IPv6 scanners target a broad range of ports, in contrast to IPv4 scans
  - IPv6 scanning is presumably not yet originating from IoT botnets

Check your IPv6-readiness (and other protocols)

Internet.nl

IS YOUR INTERNET UP TO DATE?

Today's learning objective revisited

- After the lecture, you will be able to discuss the role of DNS for the IoT and the basic characteristics of the IPv6 address space and its challenges for scanning

- Limited technical depth, but important to "set the scene" for more technical papers later in the course (we'll point you to them)

- Contributes to SSI learning goal #1: "Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF"

UNIVERSITY OF TWENTE. SIDN LABS

What's your feedback on today's lecture?

UNIVERSITY OF TWENTE. SIDN LABS

Guest lecture:
Tue May 14, 08:45-10:30
Topic: how the core of the Internet works

Next regular lecture:
Wed May 15, 10:45-12:30
Topic: IoT edge security systems

Dr. Antonia Affinito | a.affinito@utwente.nl
Prof. Cristian Hesselman | c.e.w.hesselman@utwente.nl

UNIVERSITY OF TWENTE.

SIDN LABS