Lecture #4: IoT and Internet Core Protocols

Cristian Hesselman, Antonia Affinito, Savvas Kastanakis
Etienne Khan, Ting-Han Chen, and Pascal Huppert

University of Twente | May 16, 2025

UNIVERSITY OF TWENTE. SIDN LABS

Teaching team

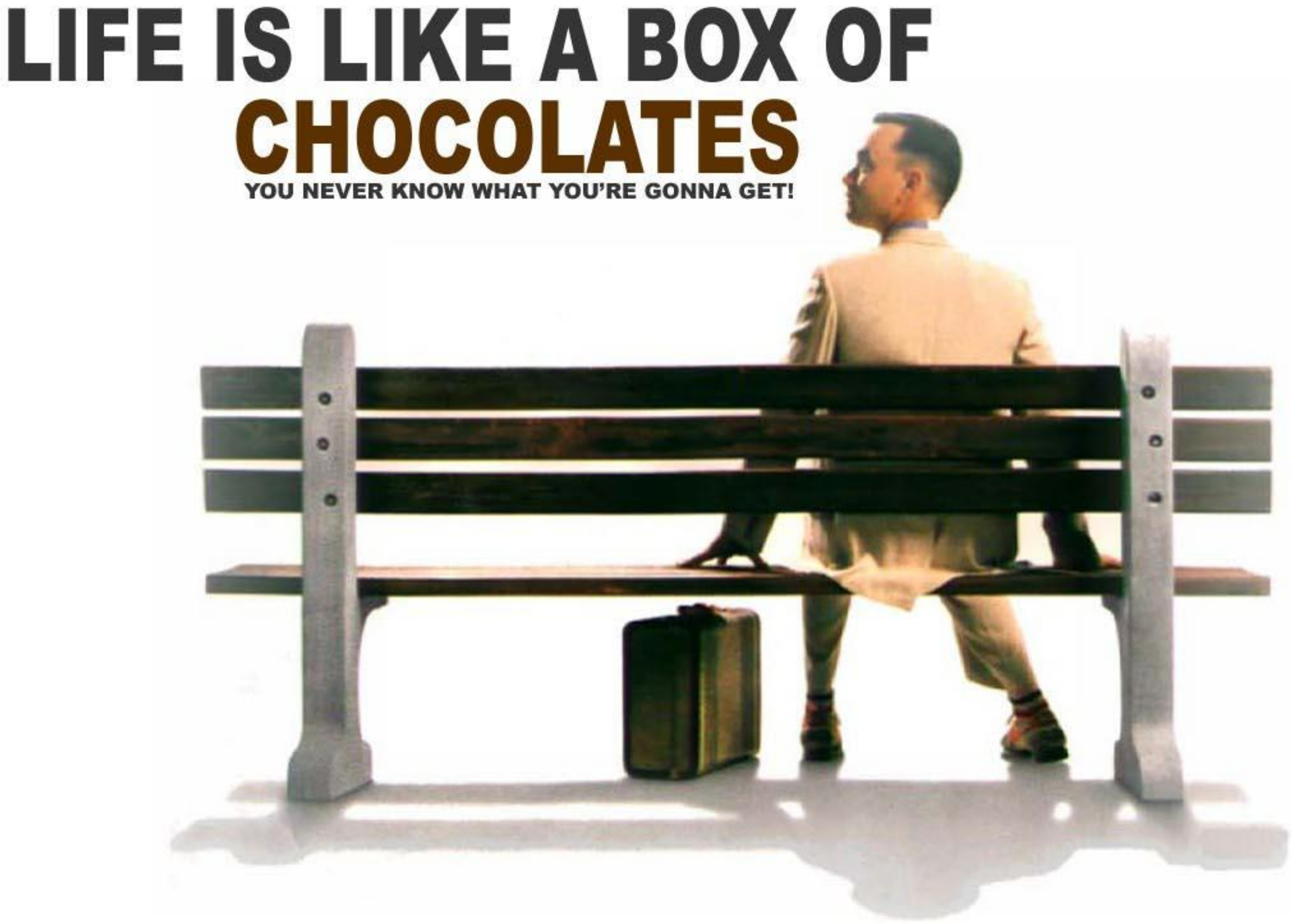
Etienne Khan

Ting-Han Chen

PhD Candidates at Design and Analysis of Communication Systems (DACS)

UNIVERSITY OF TWENTE.

SDN LABS


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

Schedule

Lecture	Date	Contents
R1	Apr 25	Course Introduction
G1	Apr 30	How the core of the Internet works (recorded)
R2	May 9	Principles of IoT Security
R3	**May 16**	**Internet Core Protocols**
R4	May 23	IoT Botnet Measurements
R5	May 27	IoTLS and Q&A Group Assignment
G2	Jun 6	Guest Lecture – PQC in IoT
R6	Jun 13	IoT Security Vulnerabilities
R7	Jun 20	IoT Forensic

Today's agenda

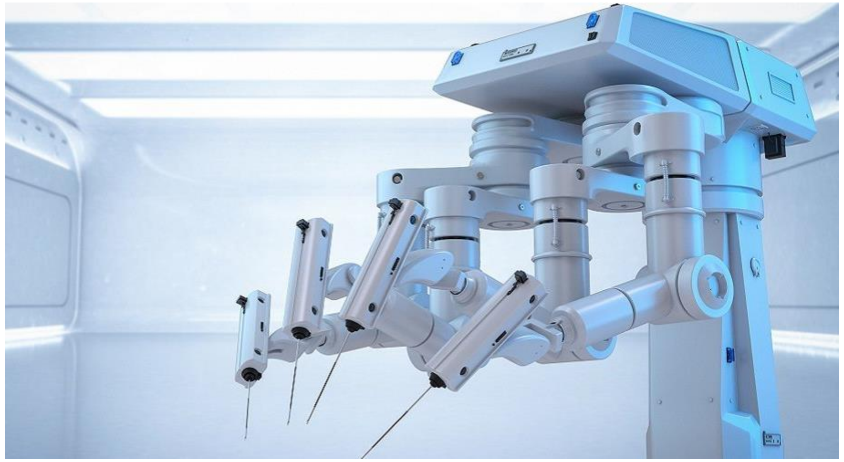
- Admin
- Introduction to today's lecture
- Paper on the DNS in IoT
- Paper on IPv6 port scanning
- Feedback

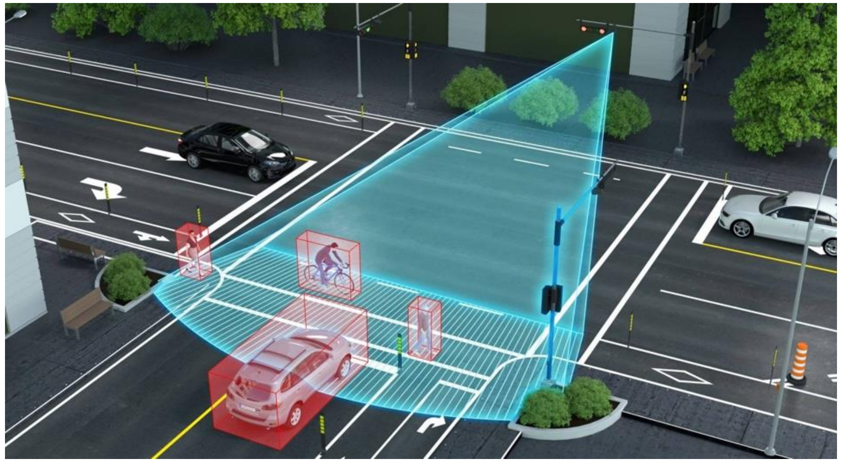
Introduction to today’s lecture

Motivation: IoT builds on the Internet today…

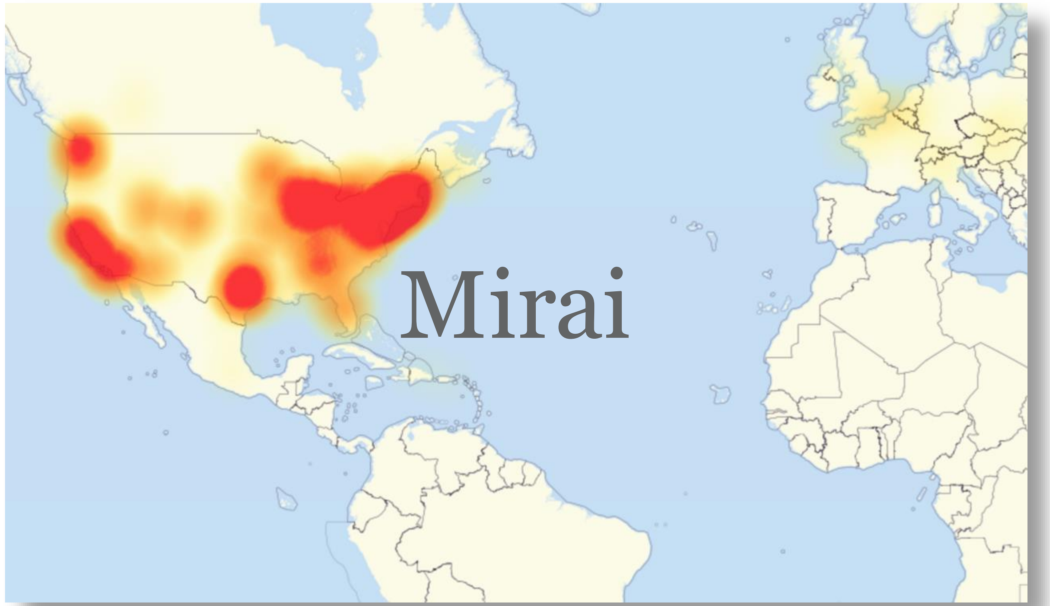
UNIVERSITY OF TWENTE. SDN LABS

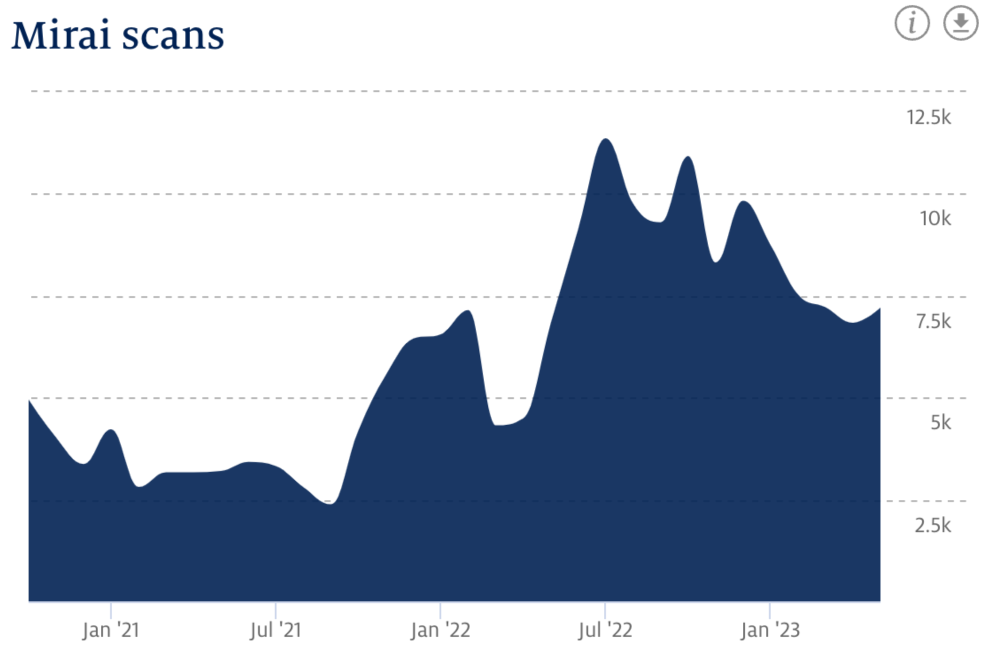
And in the future





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]

UNIVERSITY OF TWENTE.

SIDN LABS

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

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

UNIVERSITY OF TWENTE.

SIDN LABS

IoT Characteristics

No Browser. Widely Heterogeneous. Longevity. Background

Let’s see the recent IoT devices

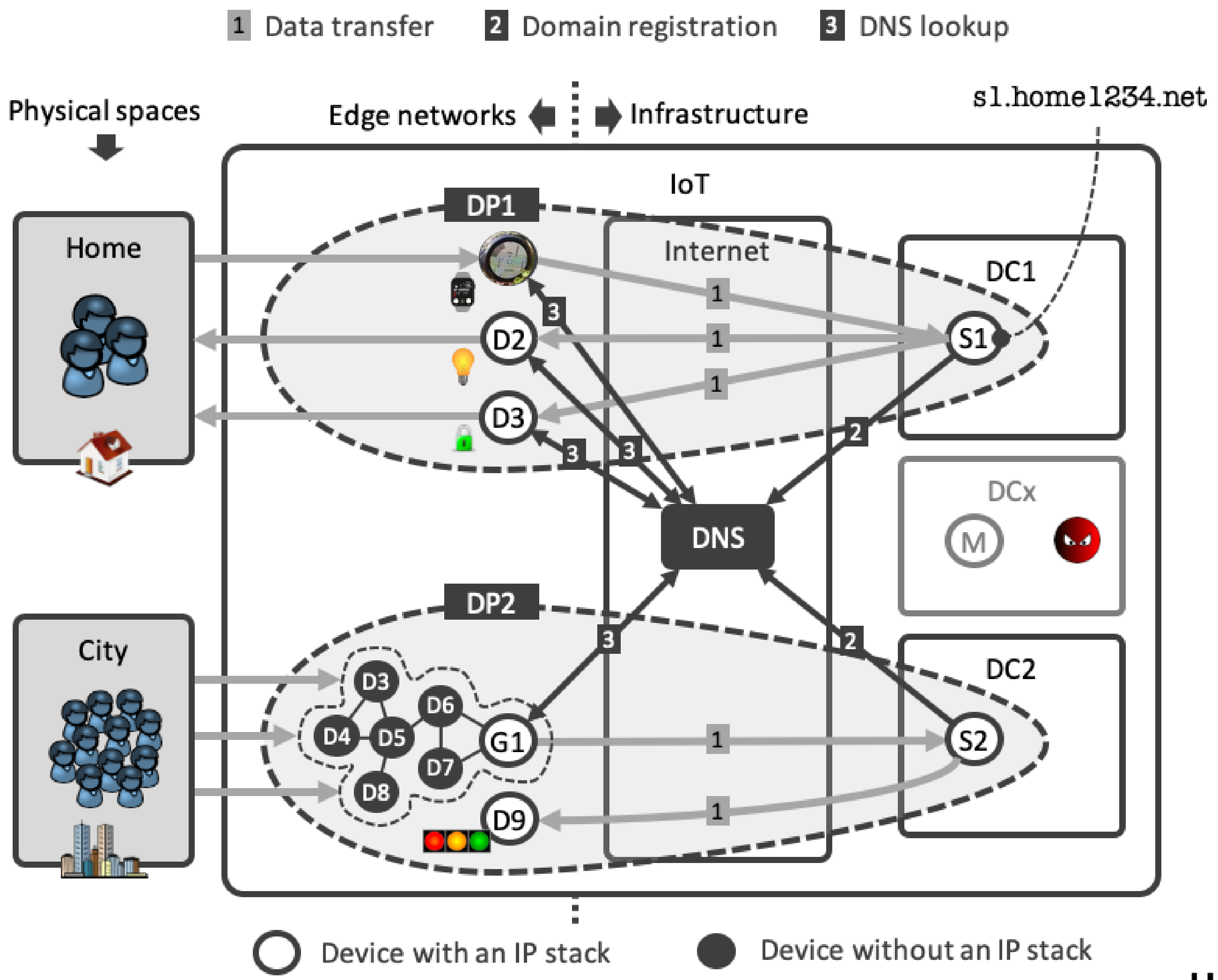
[Smart Lamp with Emotion]

[Mobile Pet Friend]

Wristwatch with GPS/LTE

UNIVERSITY OF TWENTE. SDN LABS

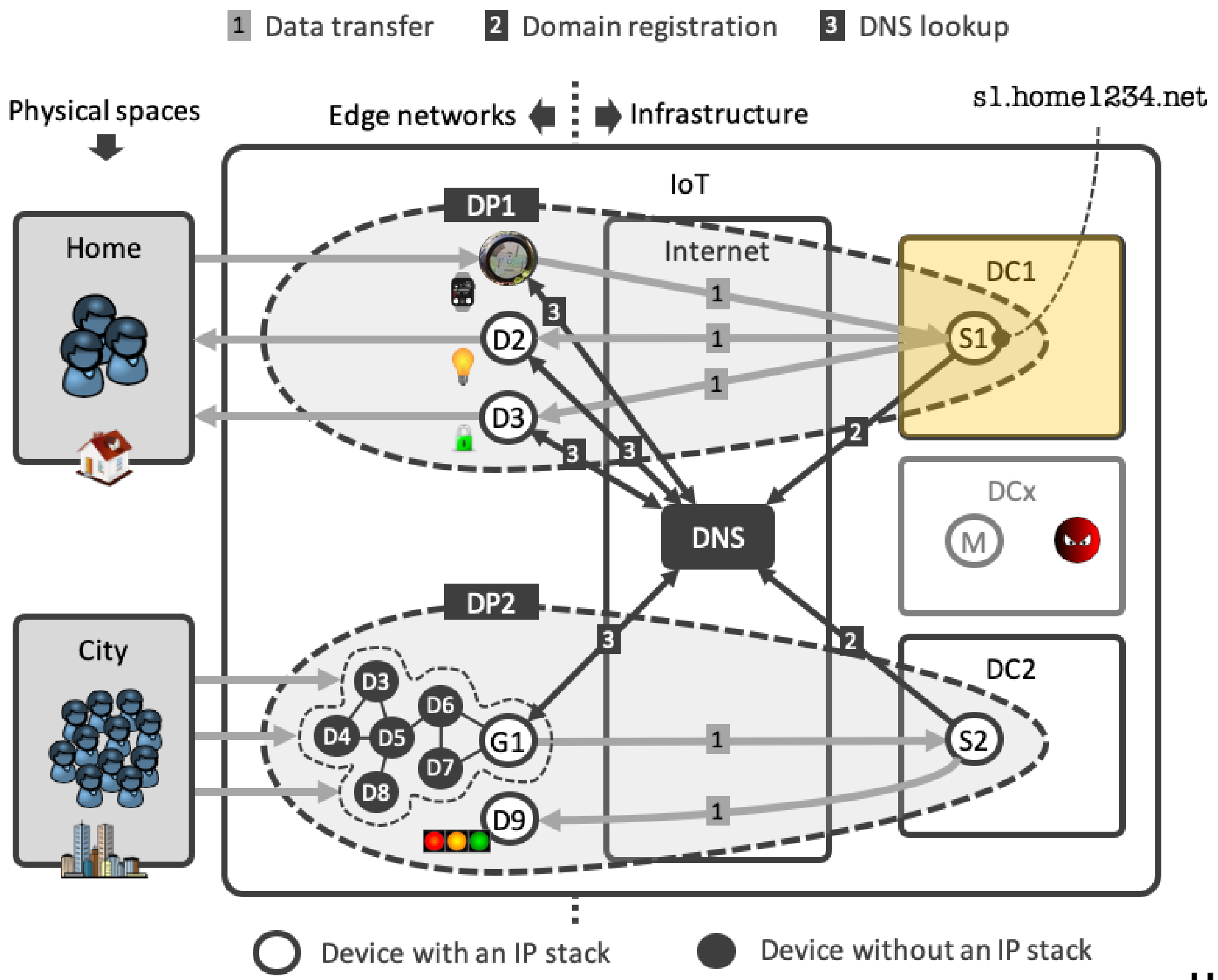
IoT deployments and the Domain Name System (DNS)



UNIVERSITY OF TWENTE.

SIDN LABS

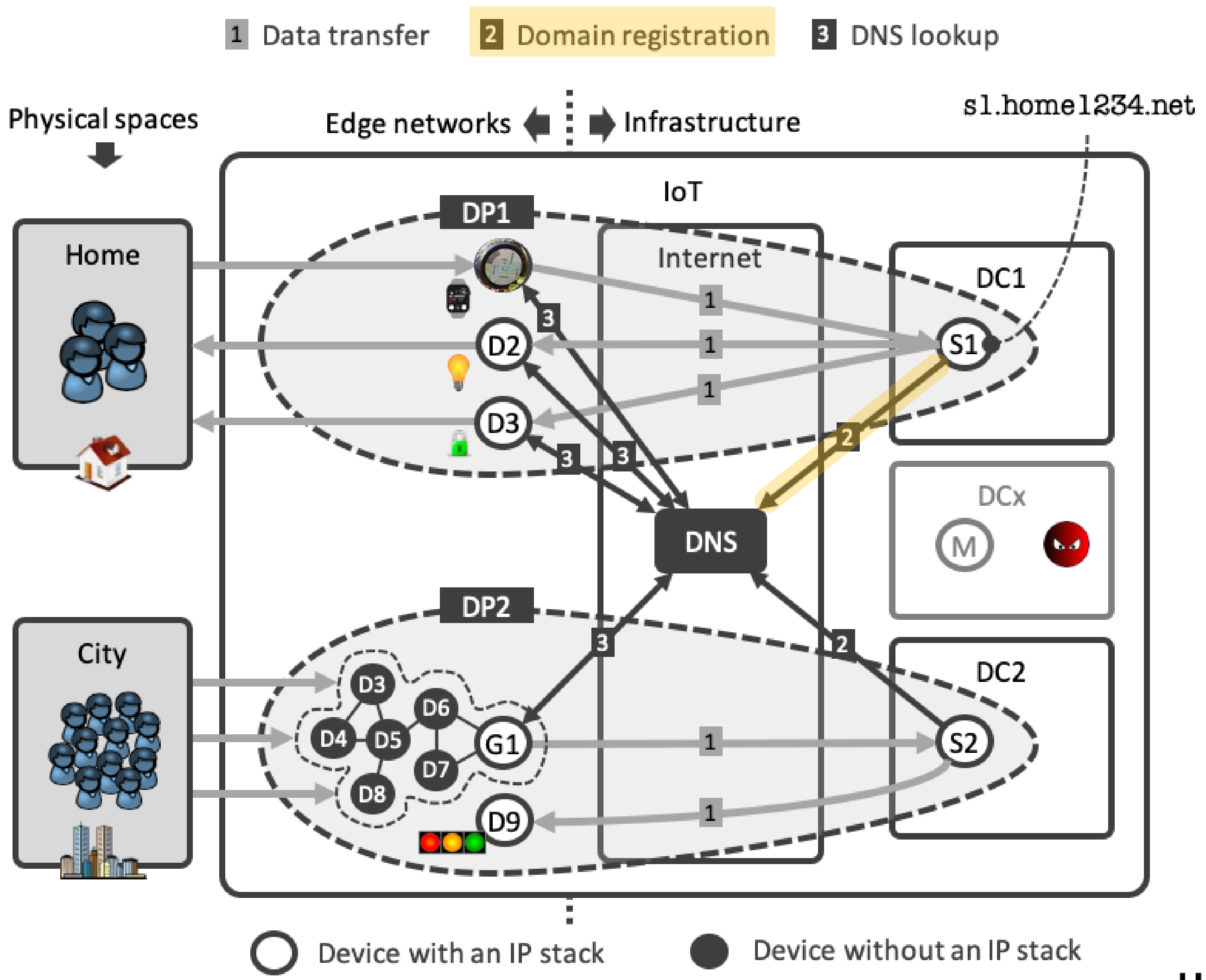
IoT deployments and the Domain Name System (DNS)



UNIVERSITY OF TWENTE.

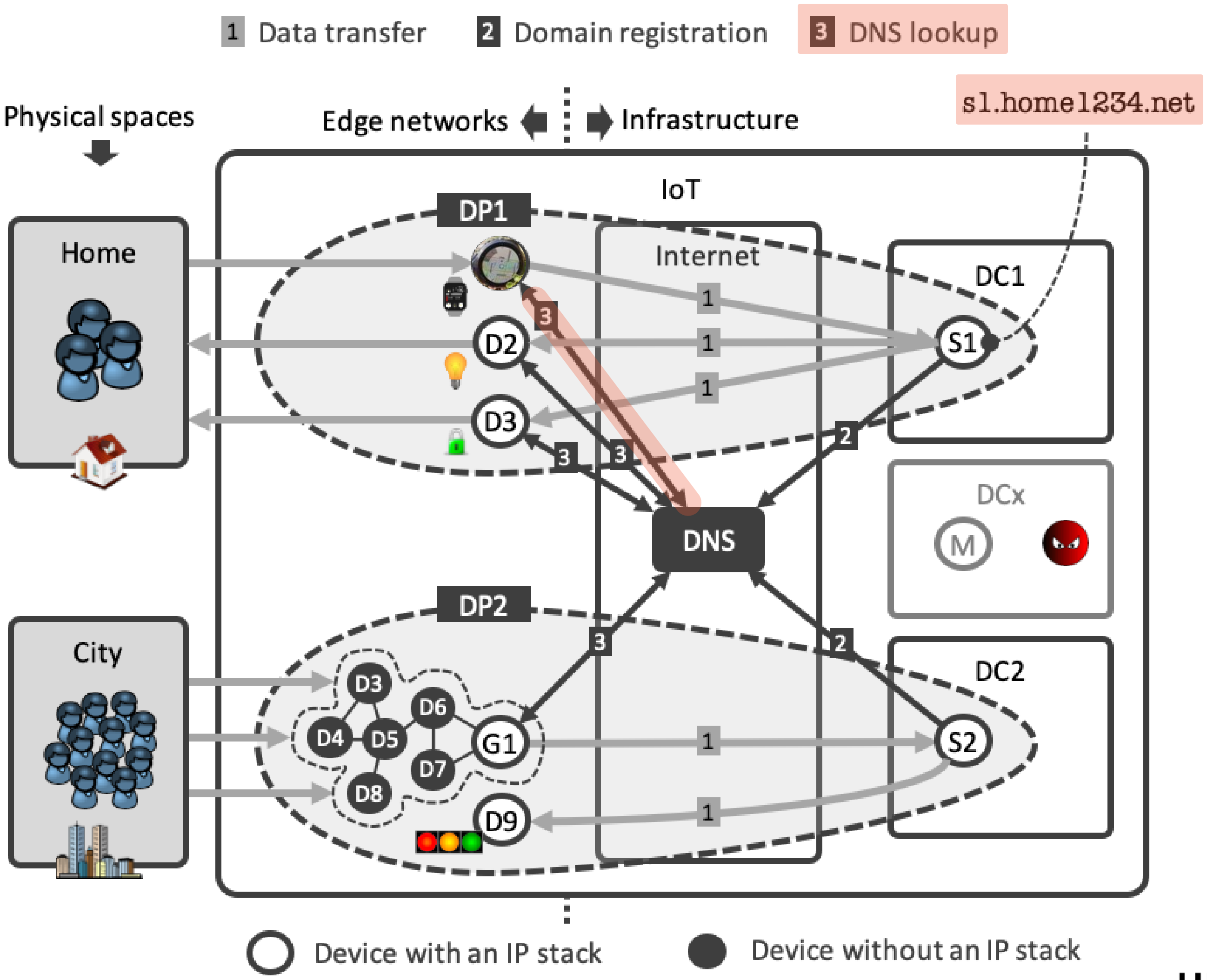
SIDN LABS

IoT deployments and the Domain Name System (DNS)

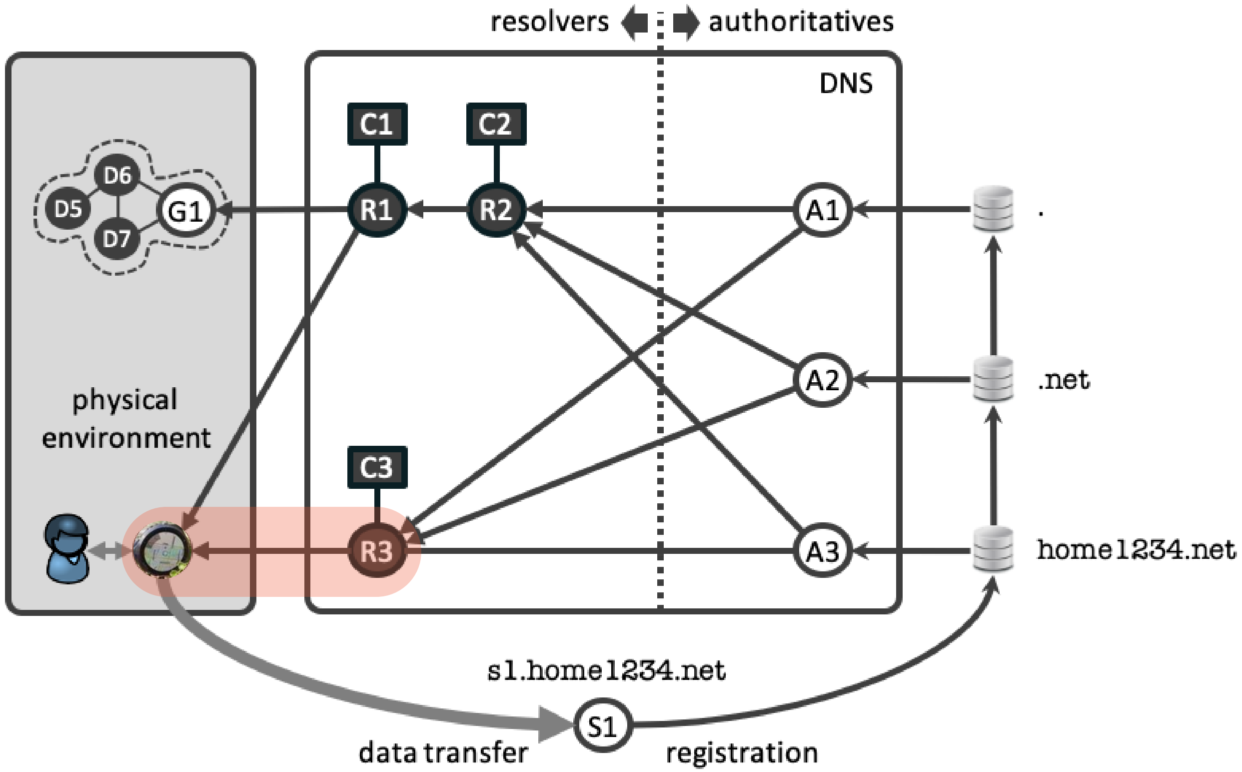


UNIVERSITY OF TWENTE. SIDN LABS

IoT deployments and the Domain Name System (DNS)

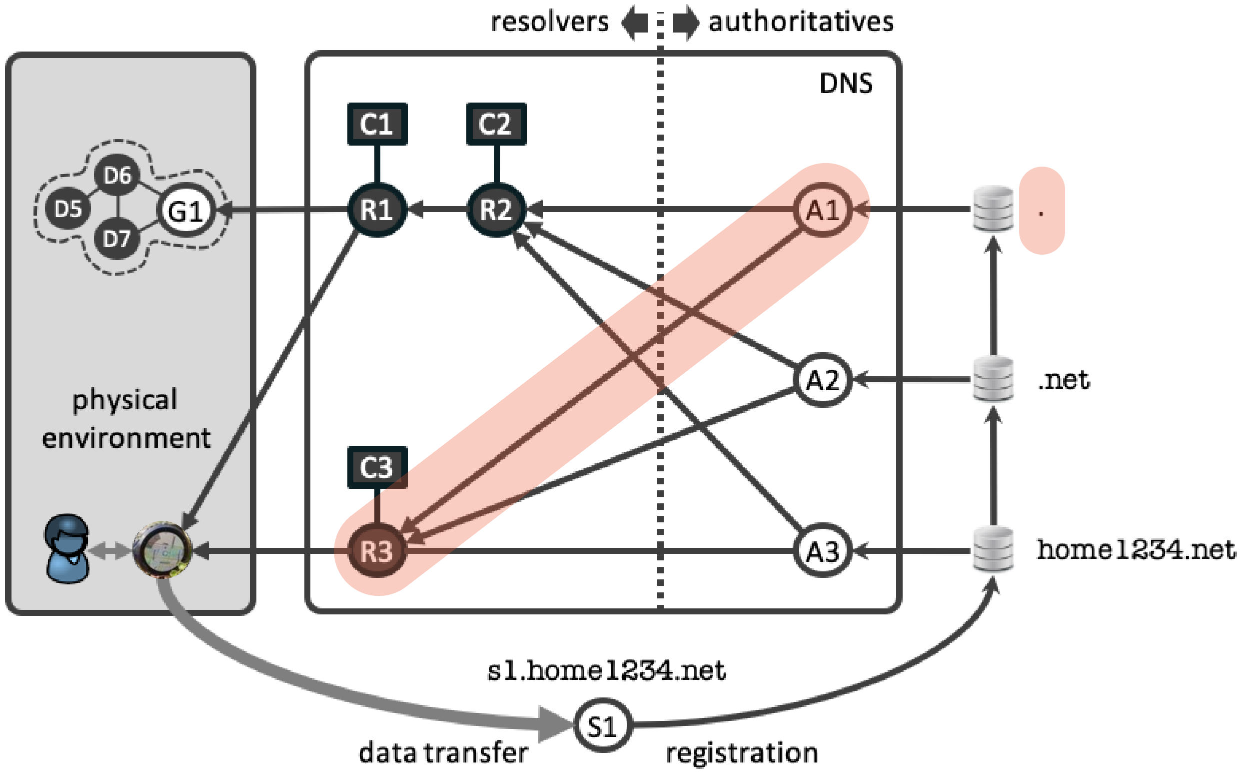


DNS high-level operation



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

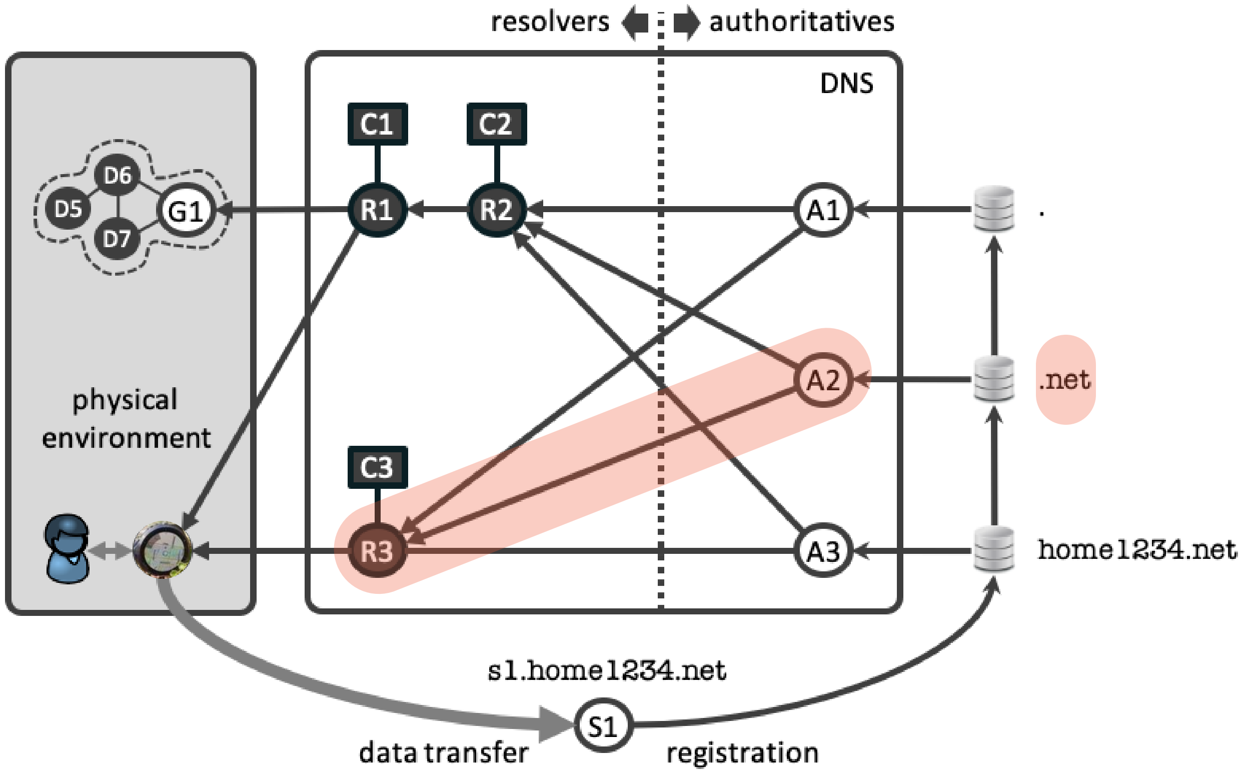


DNS Root Server

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)

UNIVERSITY OF TWENTE. SDN LABS

DNS high-level operation



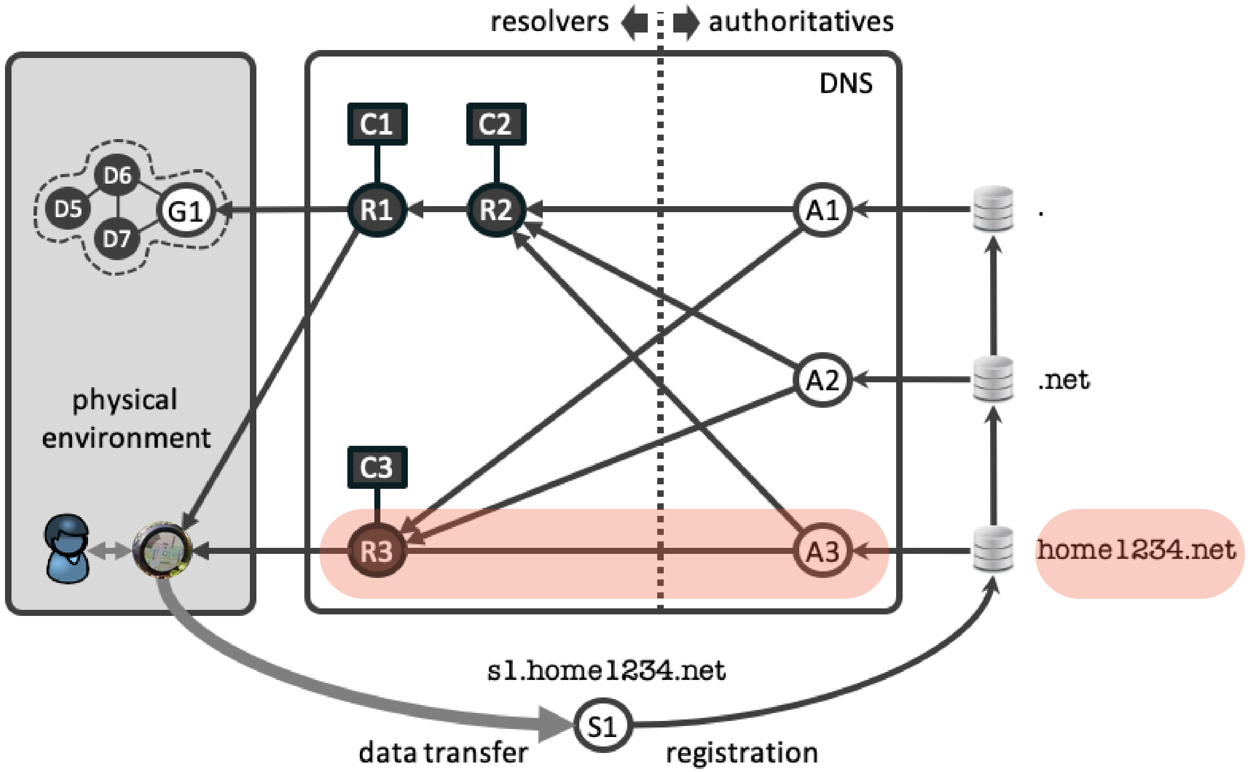
TLD Name Server

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)

UNIVERSITY OF TWENTE.

SIDN LABS

DNS high-level operation



Authoritative 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)

UNIVERSITY OF TWENTE.

SIDN LABS

DNS high-level operation

M. Müller, “Making DNSSEC Future Proof”, Ph.D. thesis,
University of Twente, September 2021

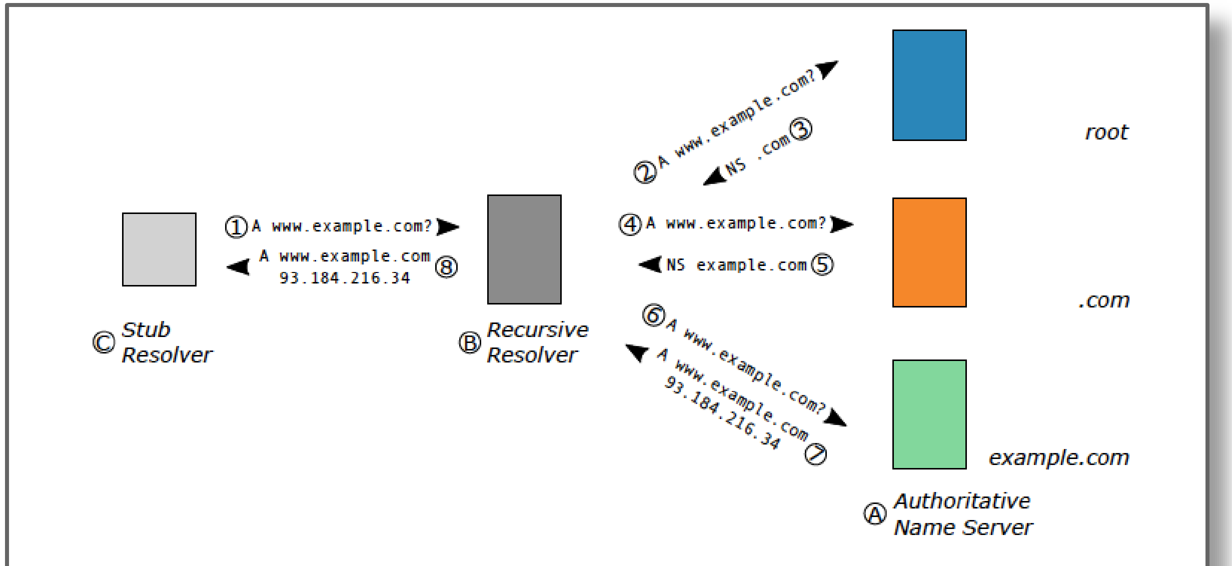
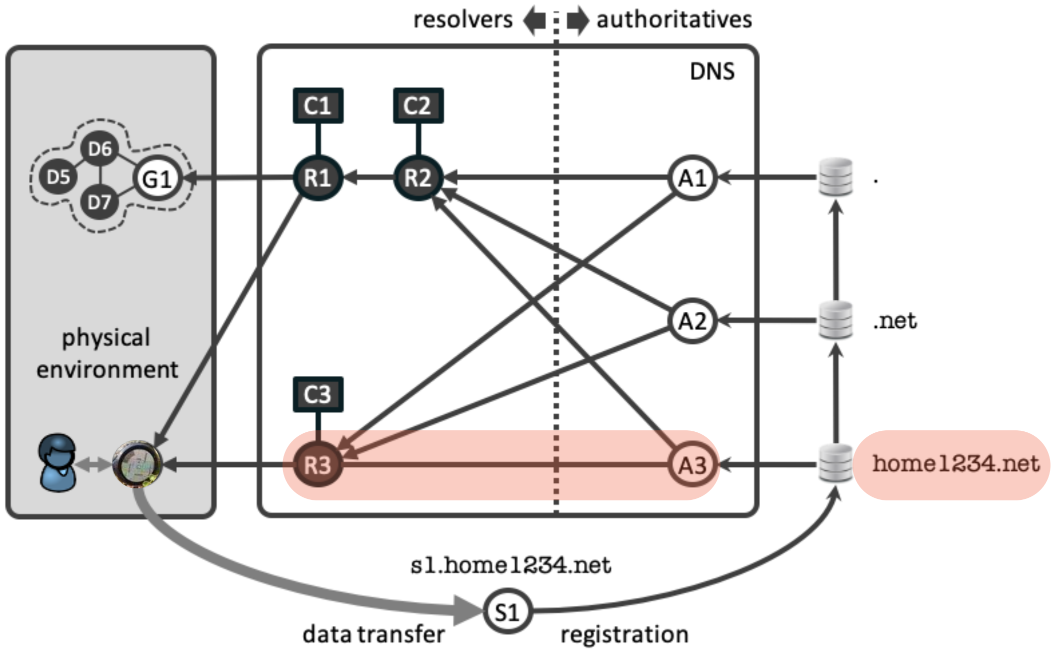
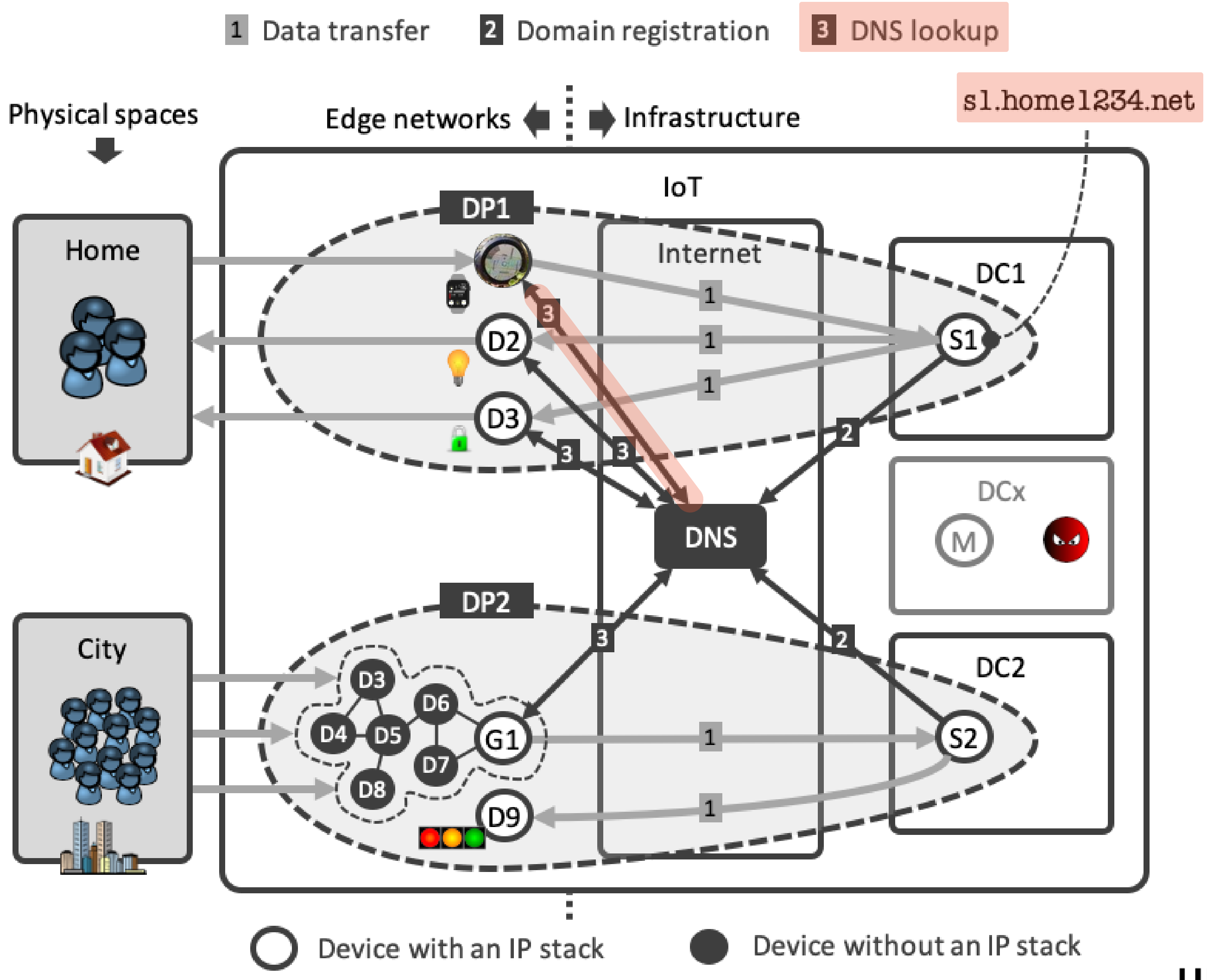


Figure 2.3: DNS components and example lookup of the A Resource Record (RR) for `www.example.com`



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)

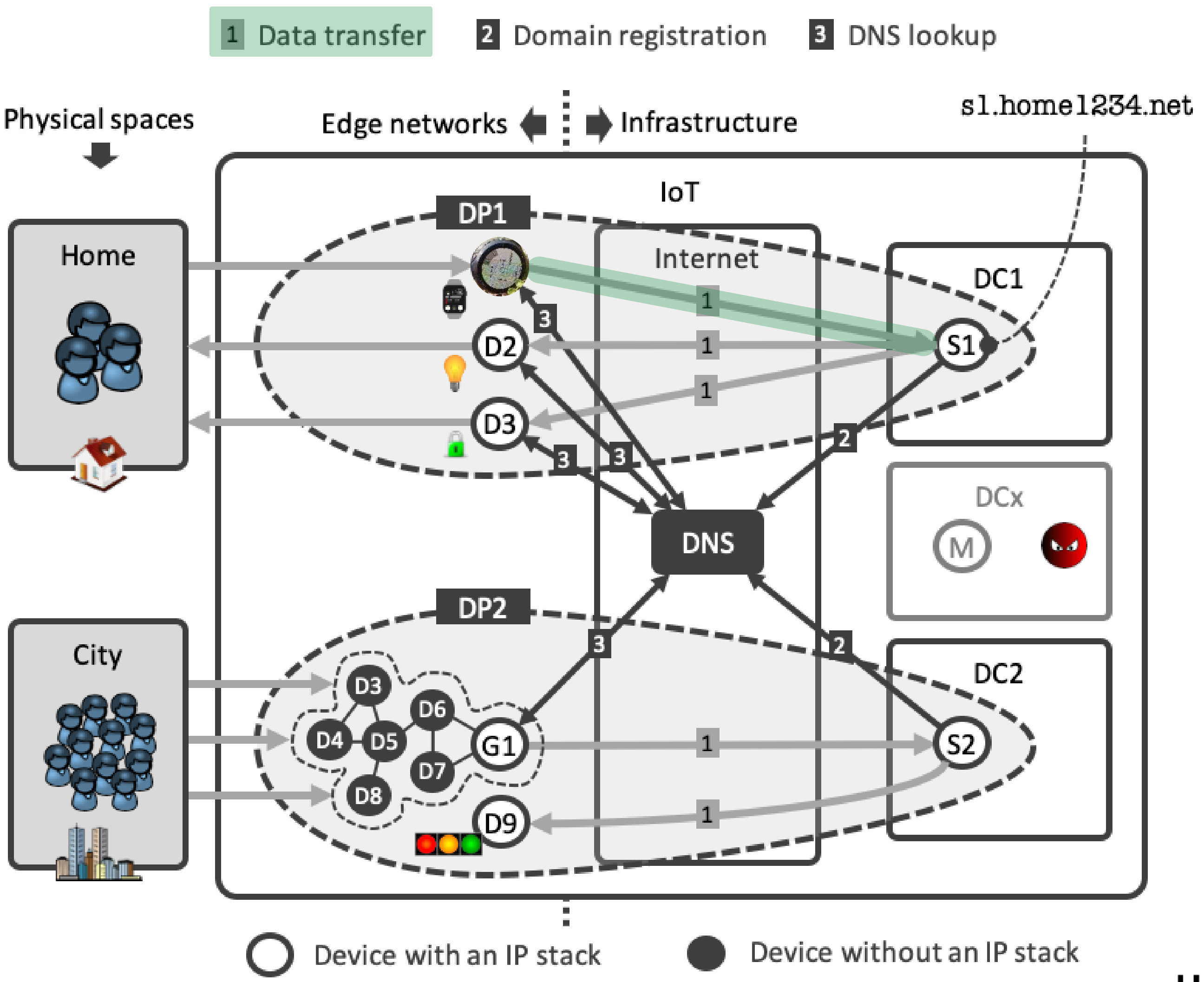
IoT deployments and the Domain Name System (DNS)



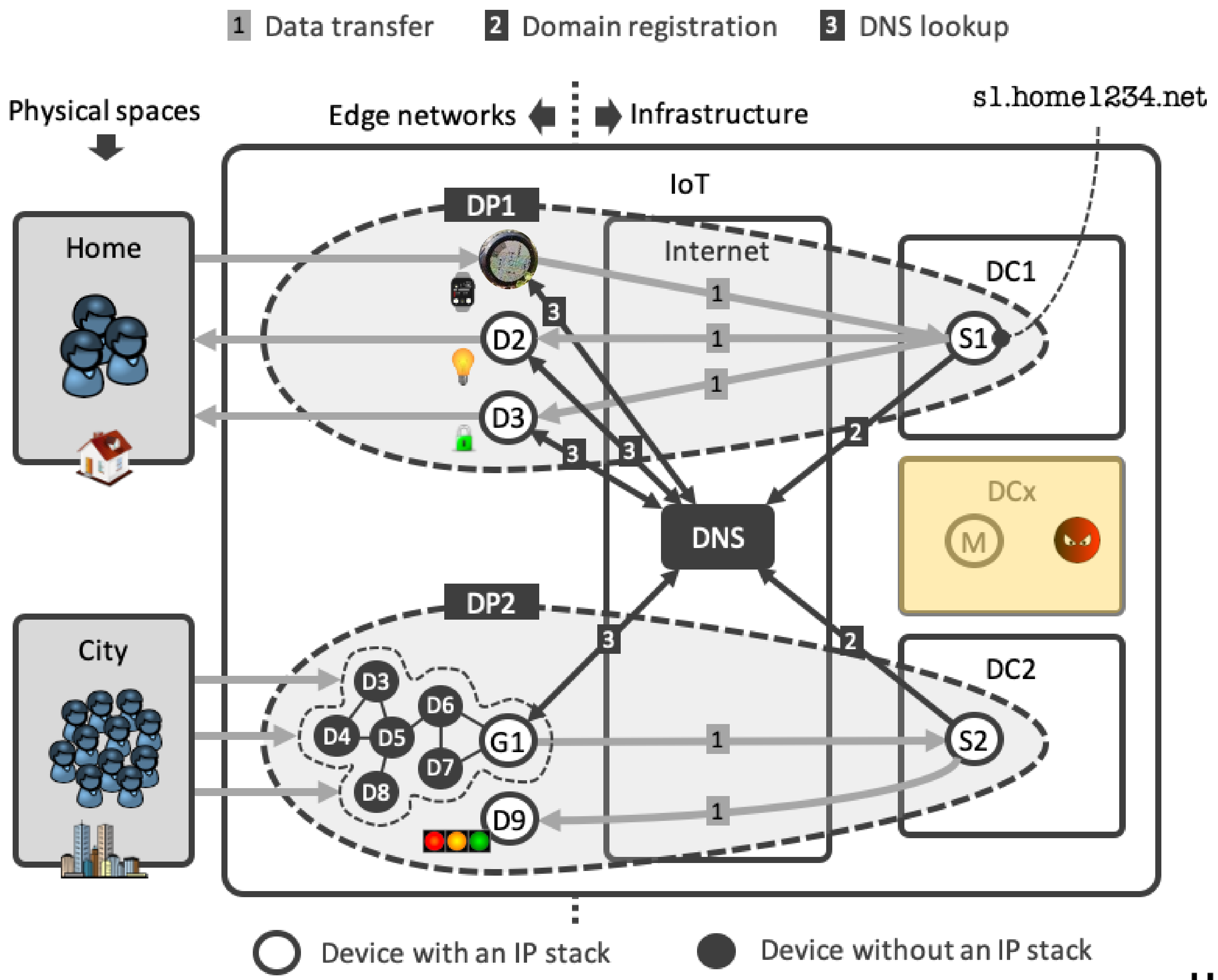
UNIVERSITY OF TWENTE.

SIDN LABS

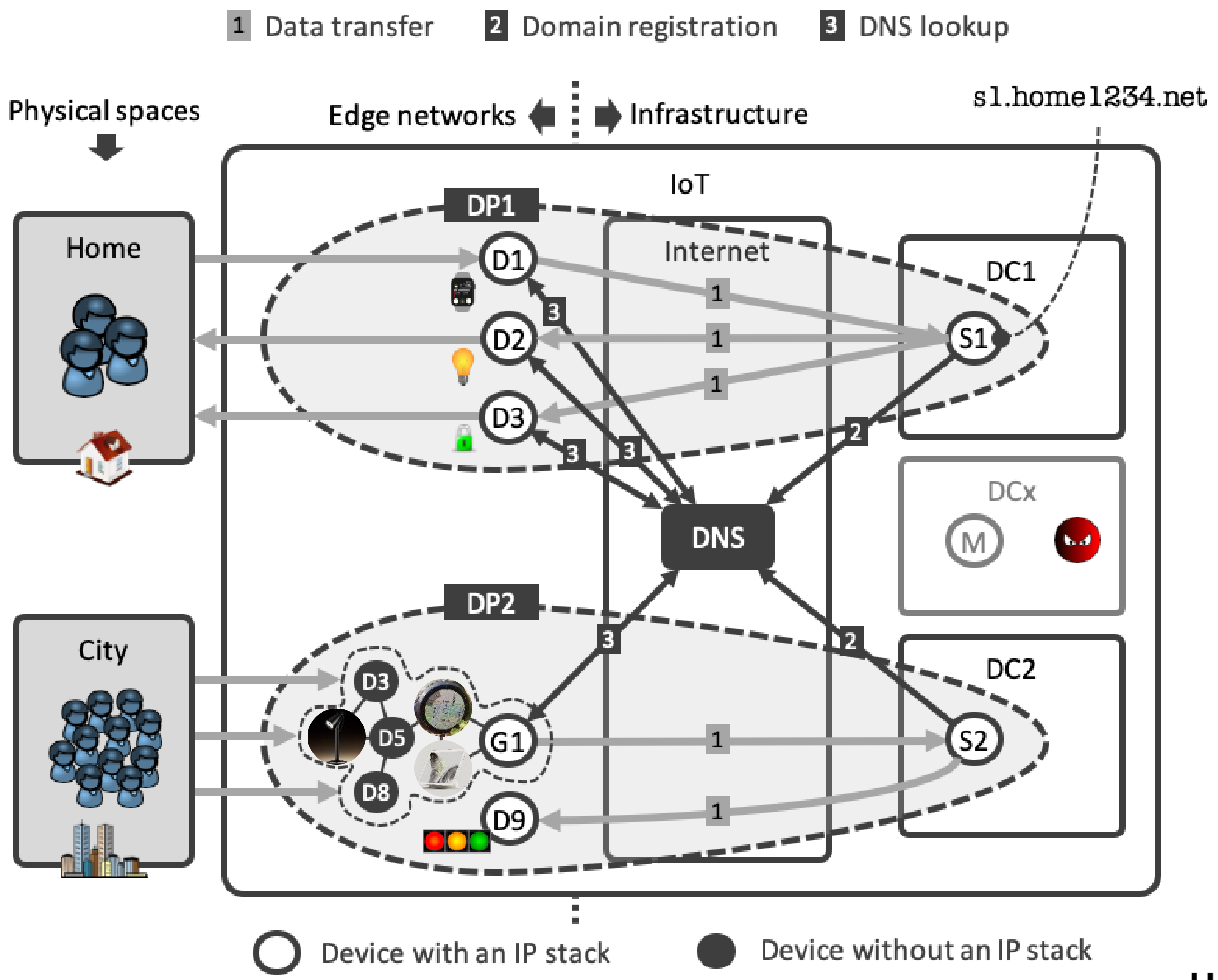
IoT deployments and the Domain Name System (DNS)



IoT deployments and the Domain Name System (DNS)



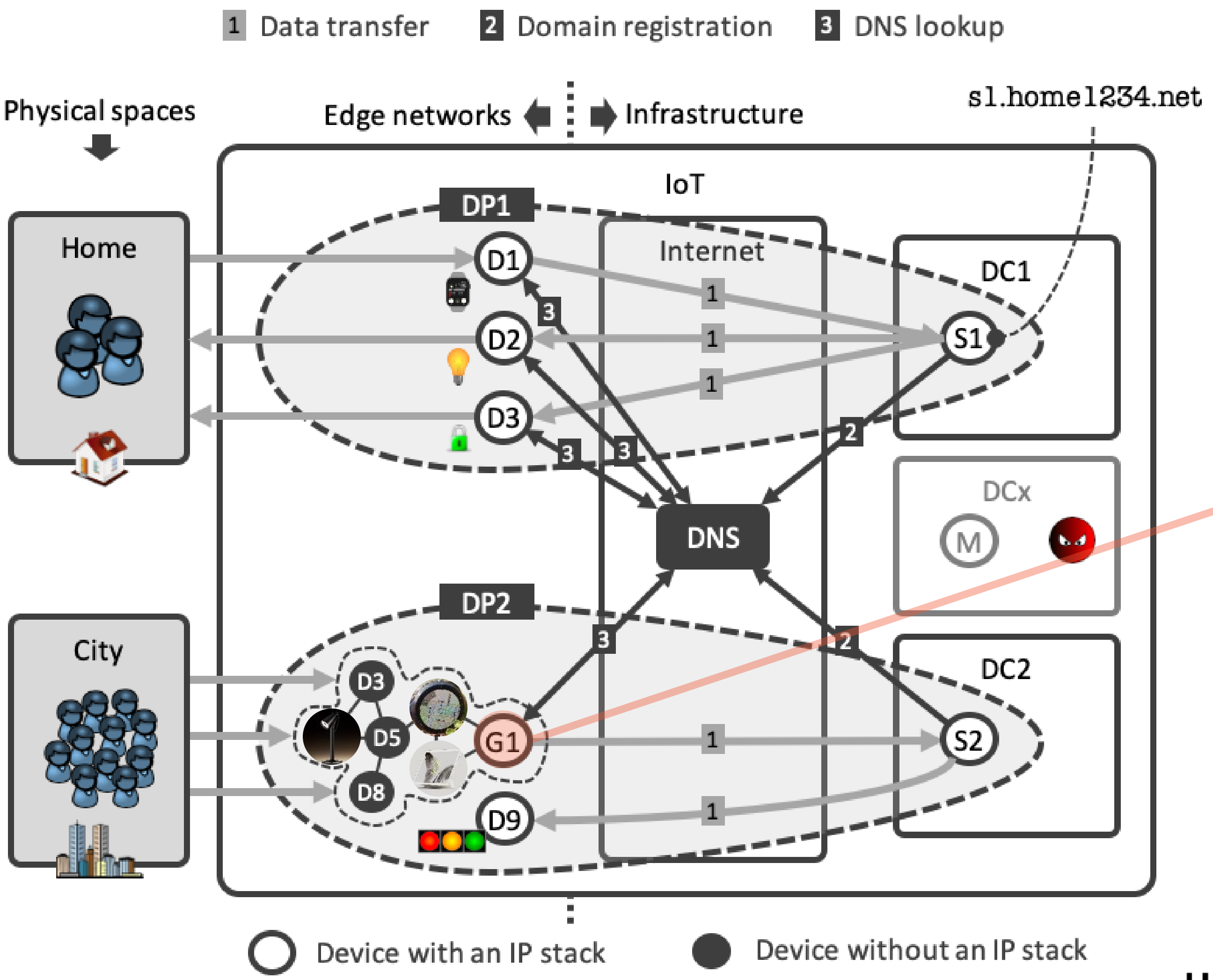
IoT deployments and the Domain Name System (DNS)



UNIVERSITY OF TWENTE.

SIDN LABS

IoT deployments and the Domain Name System (DNS)



DNS Lookup Checked!

How about DNS caches?

UNIVERSITY OF TWENTE. SIDN LABS

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
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

Challenges

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

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

O1 Using DoH/DoT to encrypt DNS queries

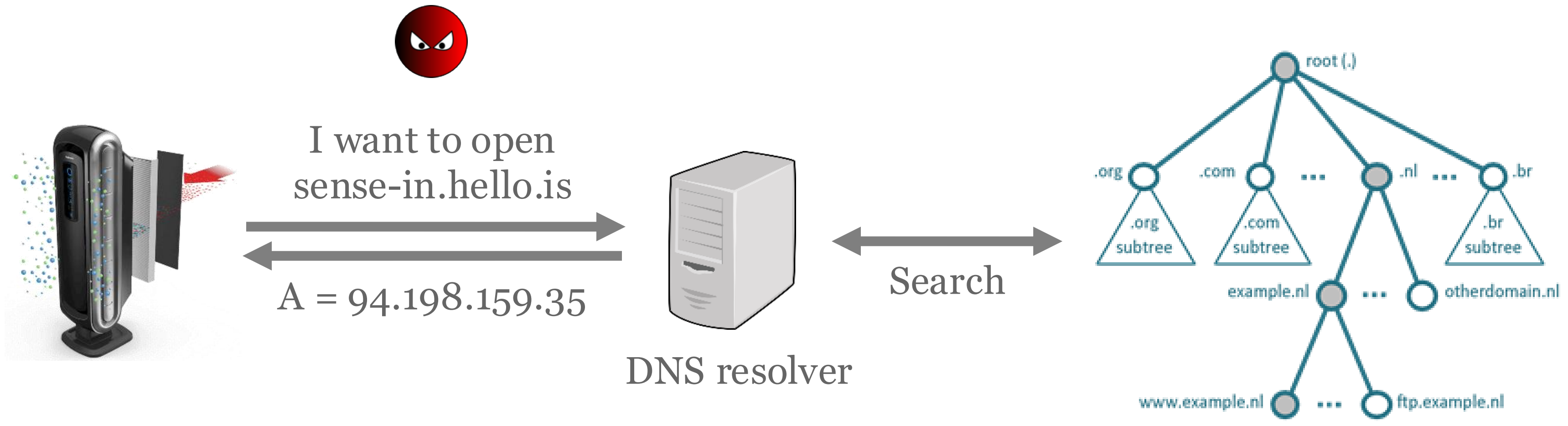
"**DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT)**

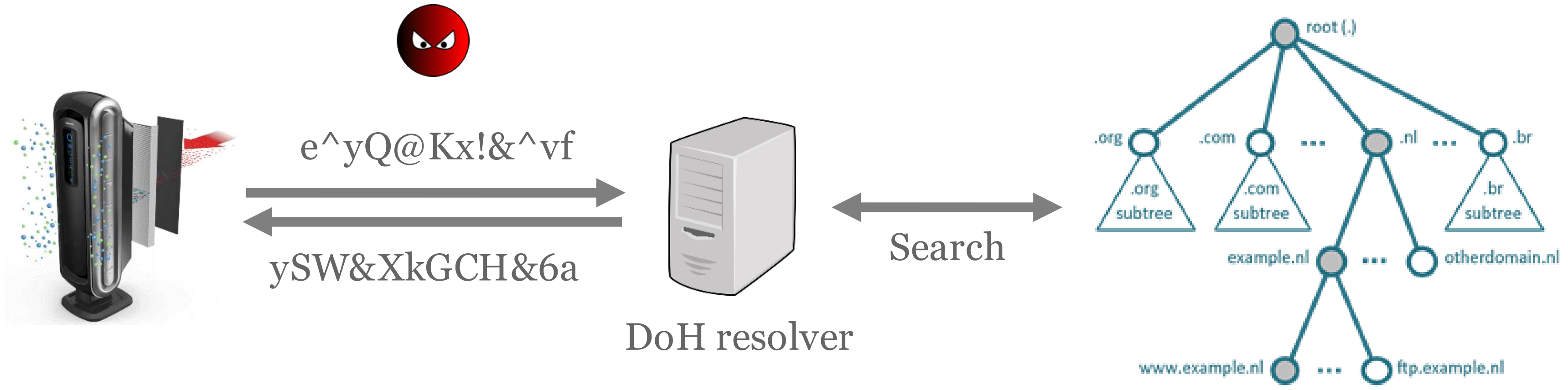
are two new protocols that encrypt DNS messages between a DNS client and its resolver, thus hiding domain lookups and responses from on-path inspection and/or alteration."

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, 2020.

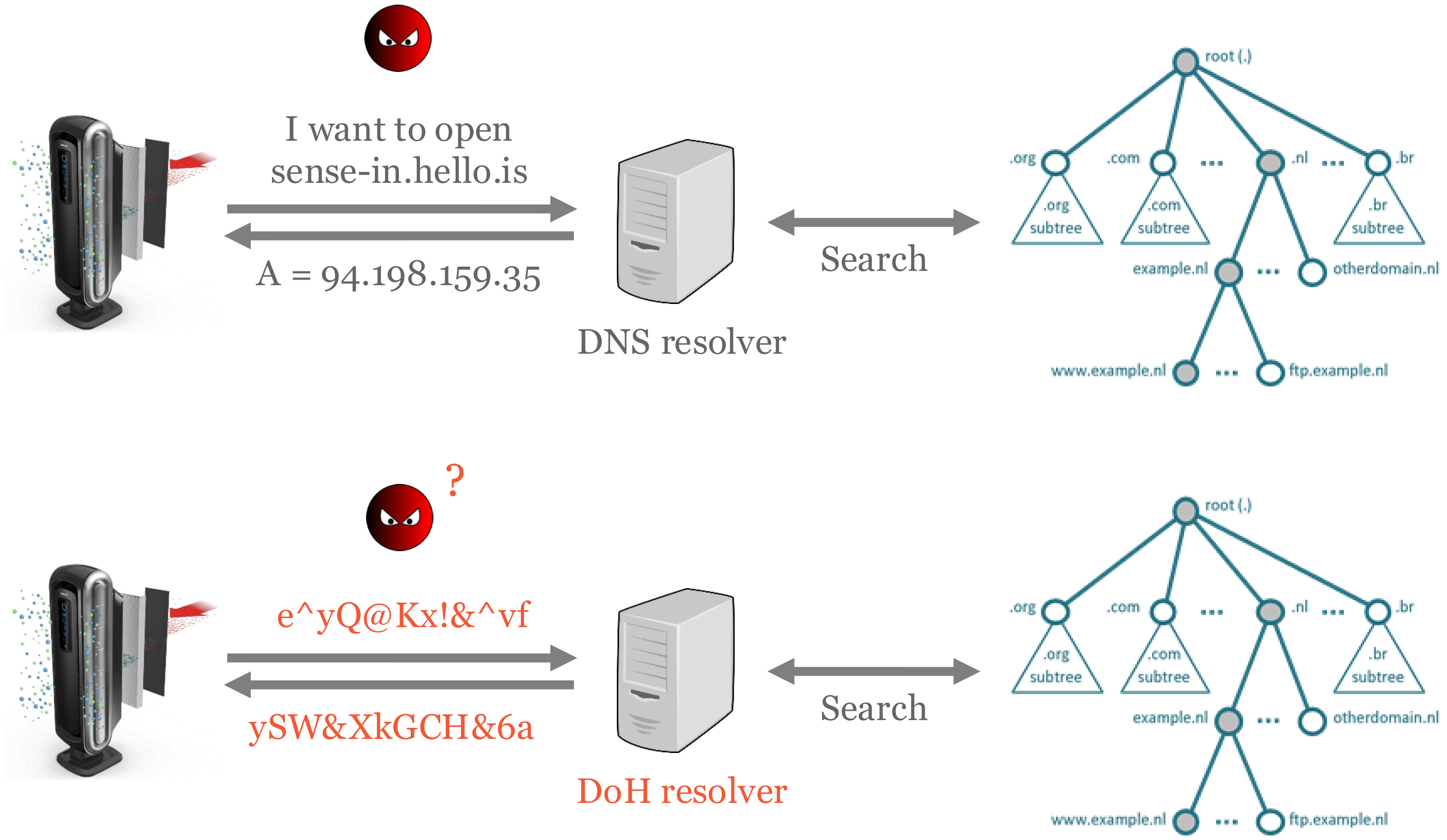
UNIVERSITY OF TWENTE. SIDN LABS

O1 Using DoH/DoT to encrypt DNS queries





O1 Using DNS-over-HTTPS to encrypt DNS queries



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)
- Lecture: IoT TLS (May 27th)

[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

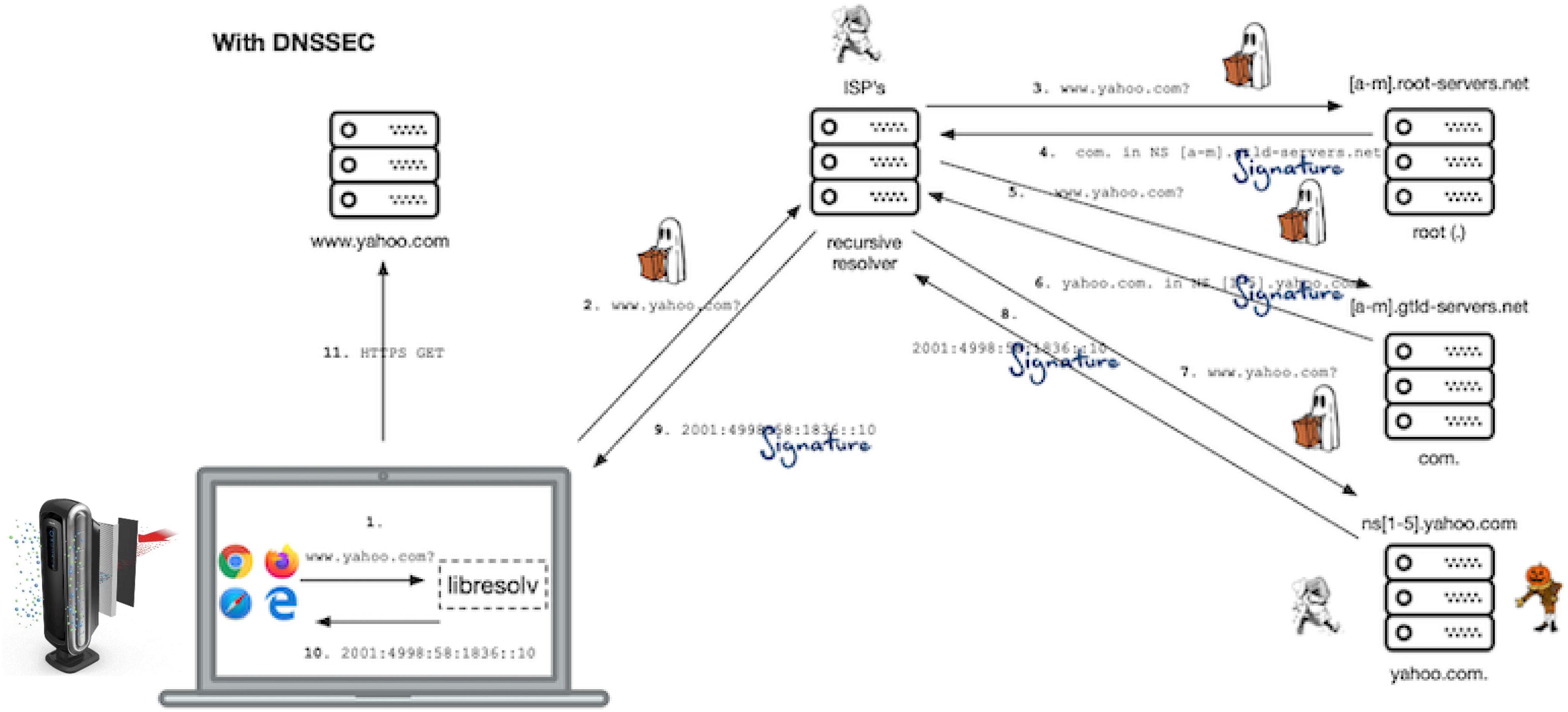
O2 Signing DNS responses with DNSSEC

"The purpose of the DNSSEC protocol

is to verify that the response to a DNS query comes from an authoritative server and was not altered in transit. DNSSEC works by adding cryptographic signatures to DNS records, which resolvers validate using DNSSEC's chain of trust."

E. Osterweil, M. Ryan, D. Massey, and L. Zhang, "Quantifying the operational status of the DNSSEC deployment," in Proc. Internet Meas. Conf., Oct. 2008.

O2 Signing DNS responses with DNSSEC



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

UNIVERSITY OF TWENTE. SDN 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)

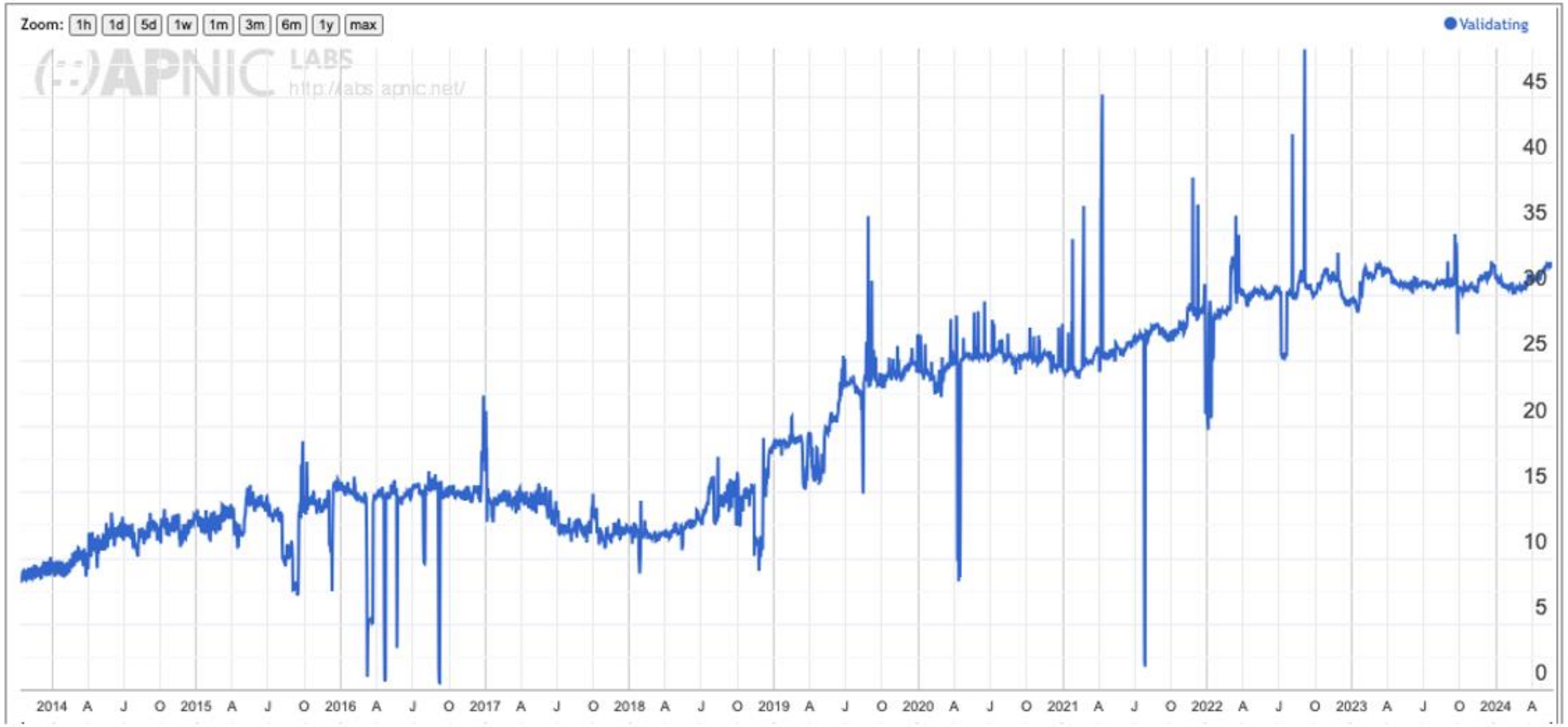
- Most secure setup: signature validation on IoT devices

If you’re the IT operators

Would you apply these? What are the pros and cons?

The Adoption of DNSSEC

Use of DNSSEC Validation for World (XA)

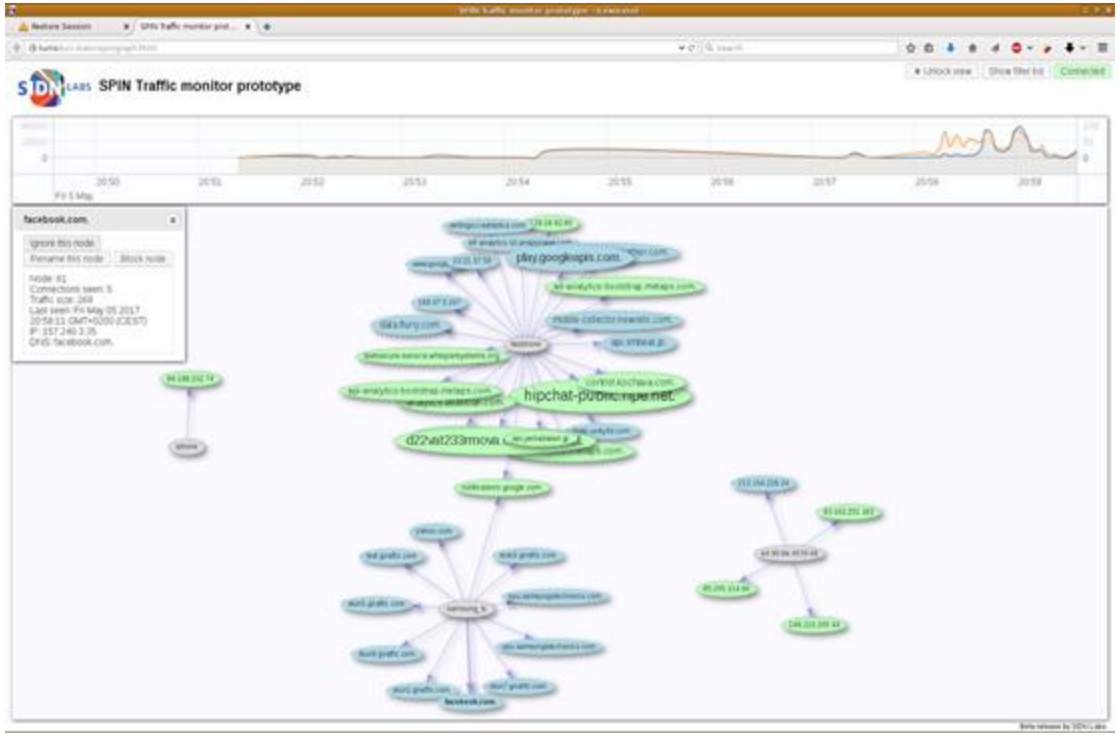


Source: https://blog.apnic.net/2024/05/28/calling-time-on-dnssec/

UNIVERSITY OF TWENTE.

SIDN LABS

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

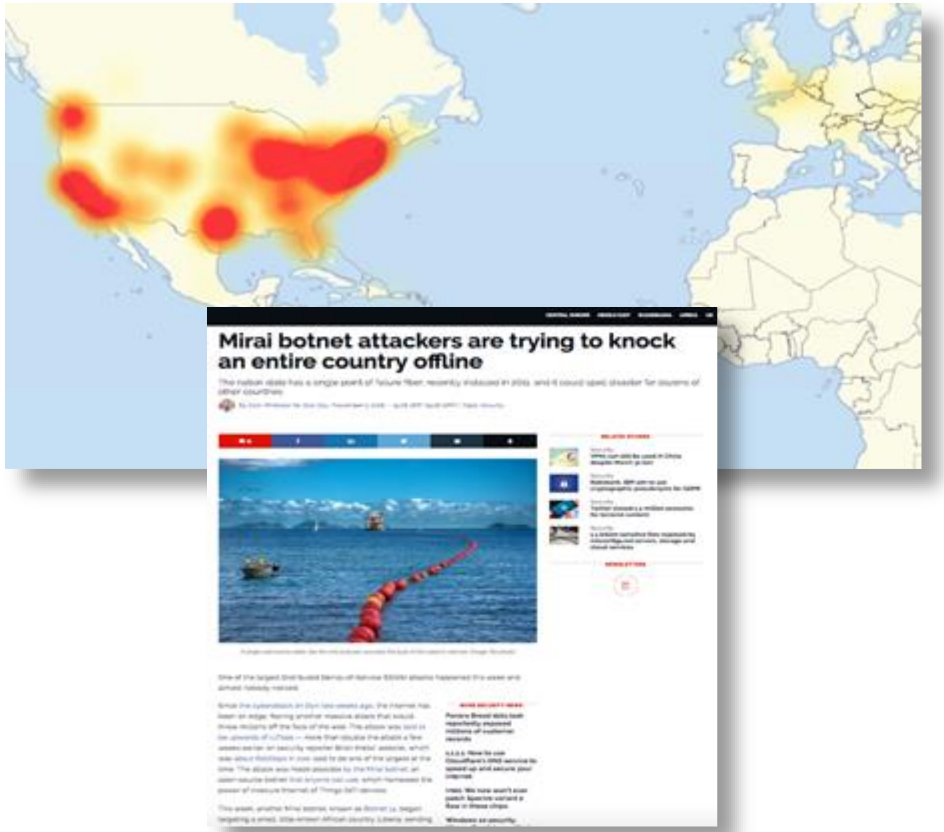
- Actually, this does not apply to DNS alone. Unfriendly programming and Software update can cause trouble everywhere like large company

If you’re the manager/engineer

What would you do to prevent this?

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, reported by Shadowserver)
- Lecture: IoT Botnet Measurement (May 23)



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

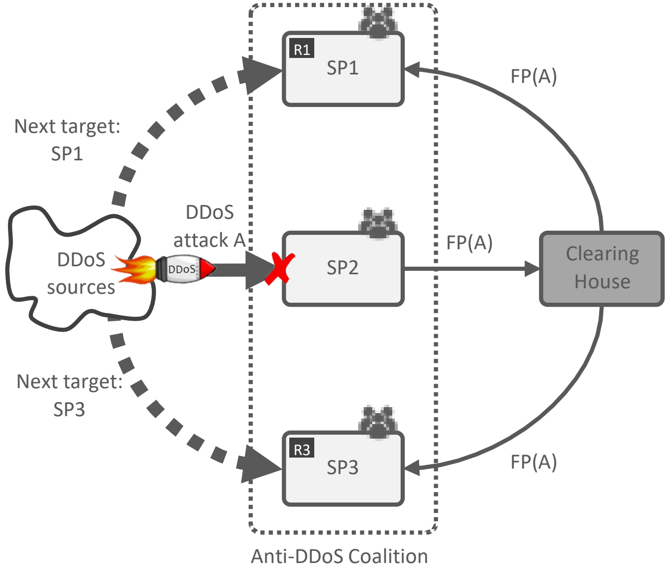
Why collaborative?

- 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

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

UNIVERSITY OF TWENTE. SIDN LABS

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

You need to know your enemies

Do you think your device is safe?

What will you do after this lecture?

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

Special Lecture – 11th of June (09:00 to 14:30)

- How the Ministry of Defence tracked down Chinese hackers
- A guest lecture by an employee of the Ministry of Defence (defensie.nl)
- A practical reverse engineering session by our guest
- https://www.utwente.nl/en/digital-society/research/cybersecurity_tuccr/events-upcoming/

UNIVERSITY OF TWENTE.

SIDN LABS

“Illuminating Large-Scale IPv6 Scanning in the Internet”

22nd ACM Internet Measurement Conference (IMC ’22), New York, NY, USA, 410–418, 2022,

UNIVERSITY OF TWENTE. SIDN LABS

Learning Goals

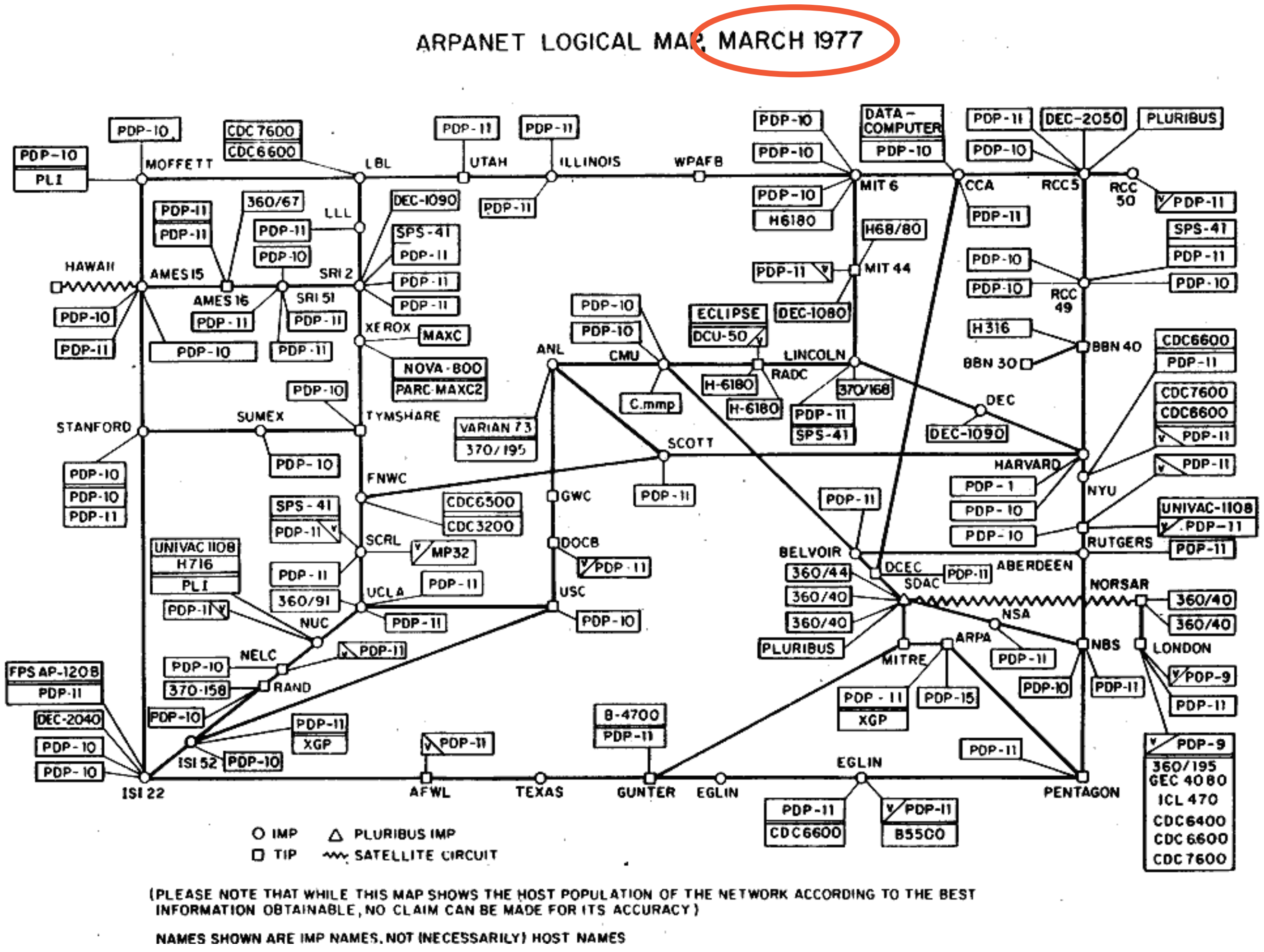
- To understand challenges of IPv6 scanning and scan detection
- To become familiar with common scanning practices in IPv6 in the wild

640k...

UNIVERSITY OF TWENTE.

SDN LABS

Map of the early Internet (ARPANET)



UNIVERSITY OF TWENTE. SDN LABS

RFC 760 and 791

[RFC Home] [TEXT|PDF|HTML] [Tracker] [IPR] [Info page]

Obsoleted by: 791 UNKNOWN
Updated by: 777
RFC: 760
IEN: 128

DOD STANDARD

INTERNET PROTOCOL

January 1980

prepared for

Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209

by

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90291

January 1980
Internet Protocol

[RFC Home] [TEXT|PDF|HTML] [Tracker] [IPR] [Errata] [Info page]

INTERNET STANDARD
Updated by: 1349, 2474, 6864 Errata Exist
RFC: 791

INTERNET PROTOCOL

DARPA INTERNET PROGRAM

PROTOCOL SPECIFICATION

September 1981

prepared for

Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209

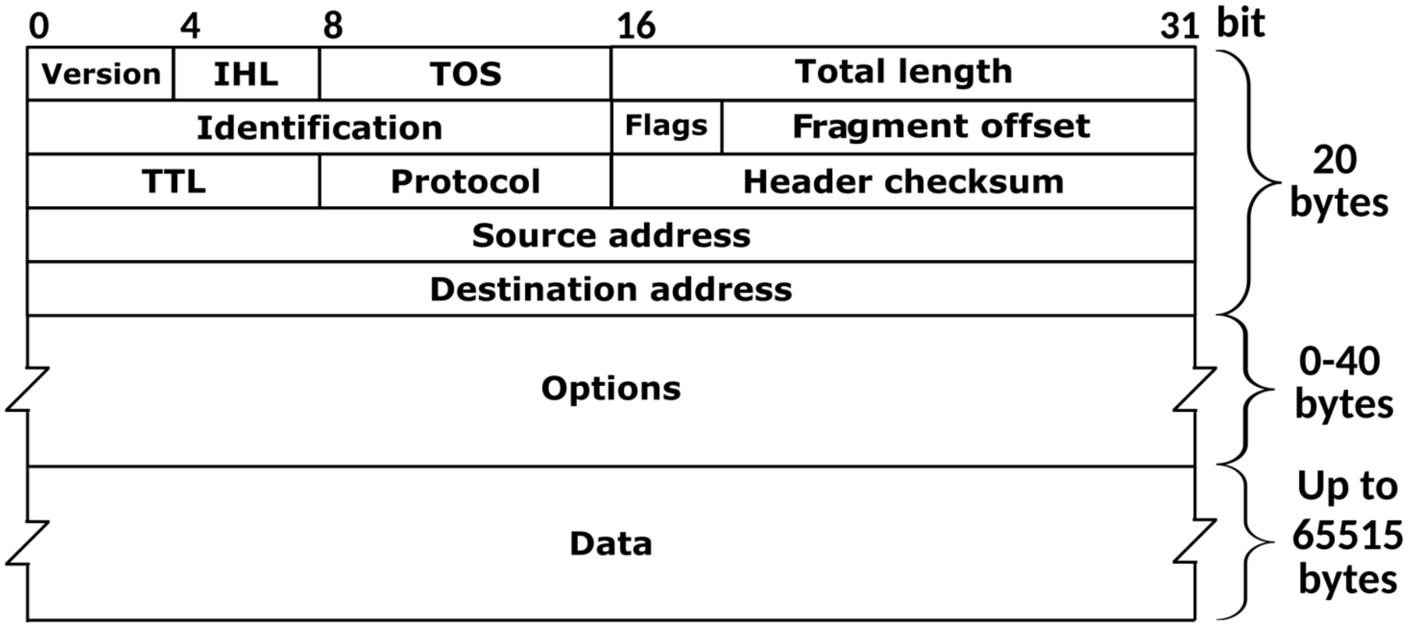
by

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90291

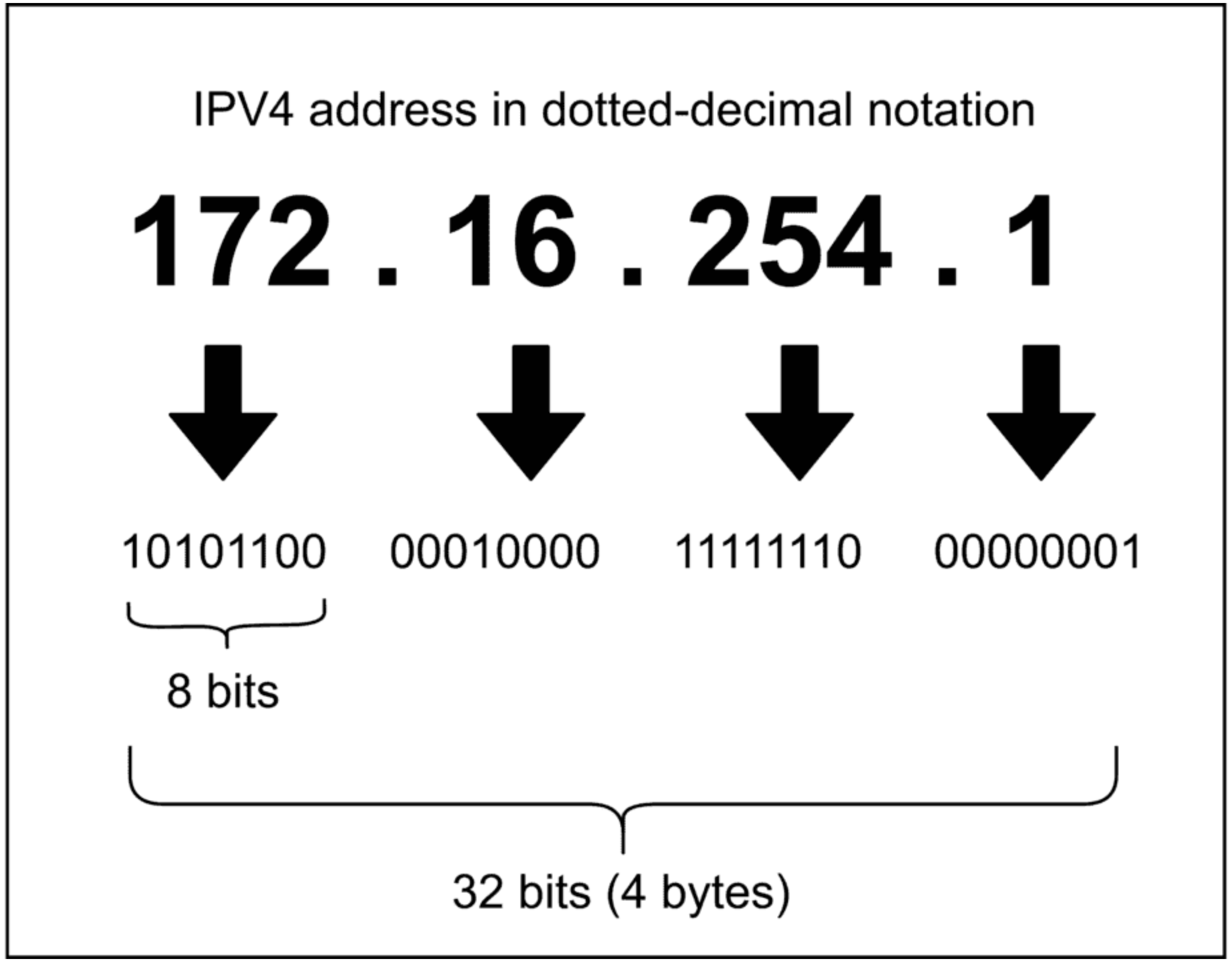
September 1981
Internet Protocol

IP header

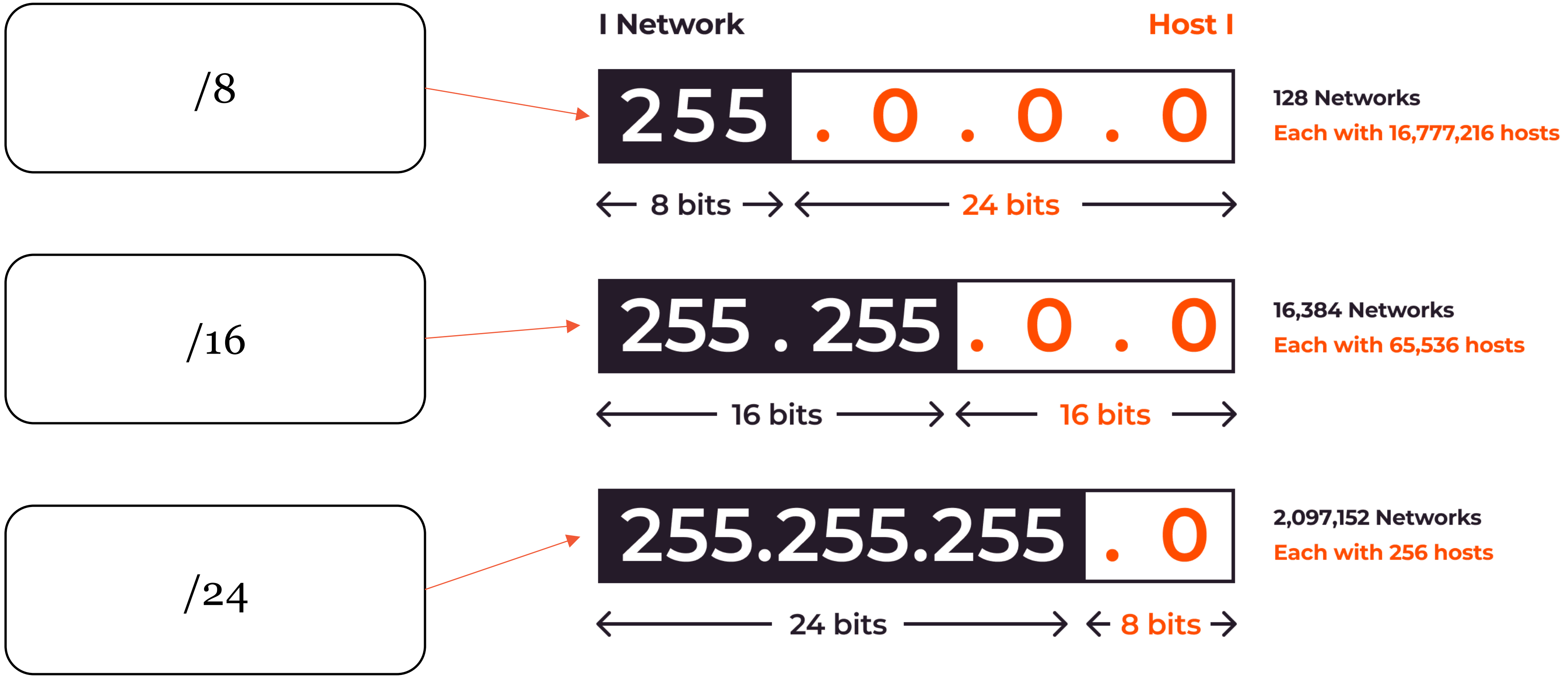
- Only a few thousand computers
- Intel 386 (32-bit); releases Oct. 1985
  (Relevant for memory and page alignment)



Decimals to bits



Subnet


/8
/16
/24
I Network
Host I
255 . 0 . 0 . 0
8 bits
24 bits
128 Networks
Each with 16,777,216 hosts
255 . 255 . 0 . 0
16 bits
16 bits
16,384 Networks
Each with 65,536 hosts
255.255.255 . 0
24 bits
8 bits
2,097,152 Networks
Each with 256 hosts

University of Twente as seen on https://bgp.he.net

Announced By			
Origin	Origin Registrant	Prefix	Prefix Registrant
AS1133	SURF B.V.	130.89.0.0/16	Universiteit Twente

Matching Delegations			
Registry	Status	Prefix	CC
ripencc	assigned	130.89.0.0/16	NL

UNIVERSITY OF TWENTE.

SIDN LABS

Quiz Question

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

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

Have you already experimented with Internet-wide scans?

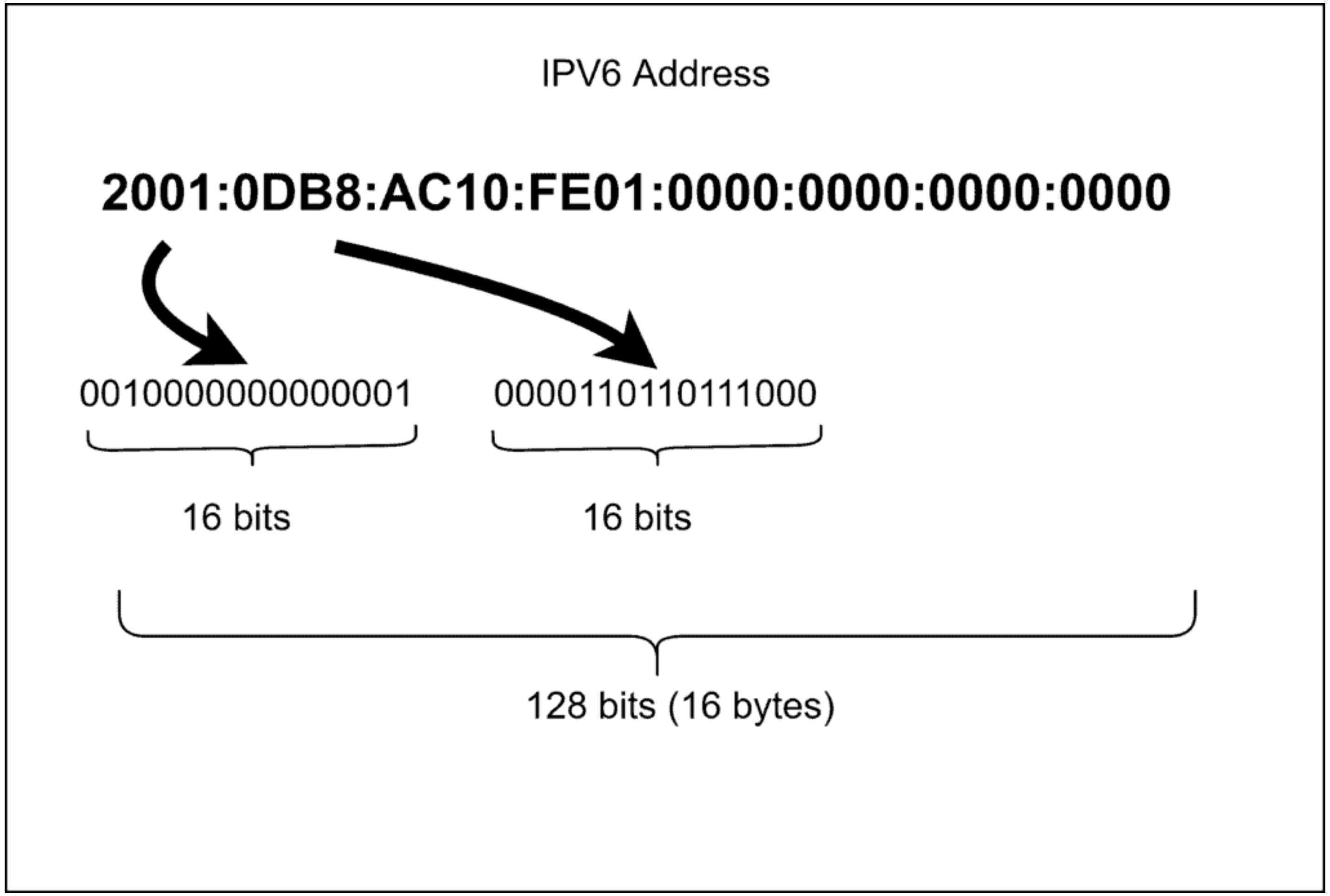
How long would it take to scan IPv6?

~~640k…~~ 4’294’967’29

- 4’294’96 … ad … *REALLY* … nt … e enough for … ny … dy

FALSE

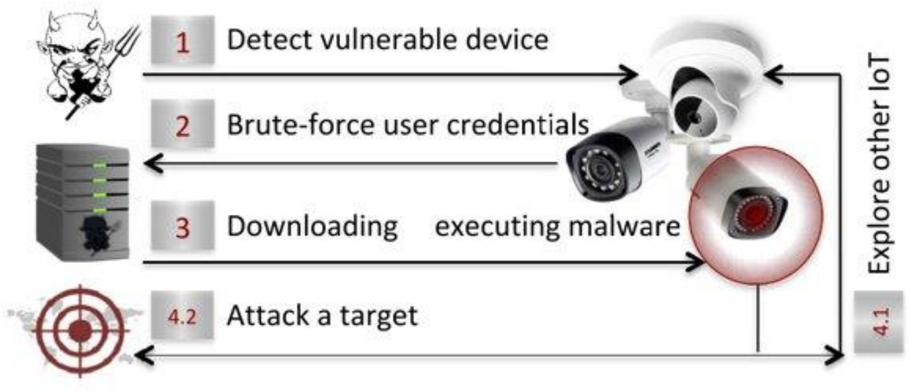
128 bits to the rescue

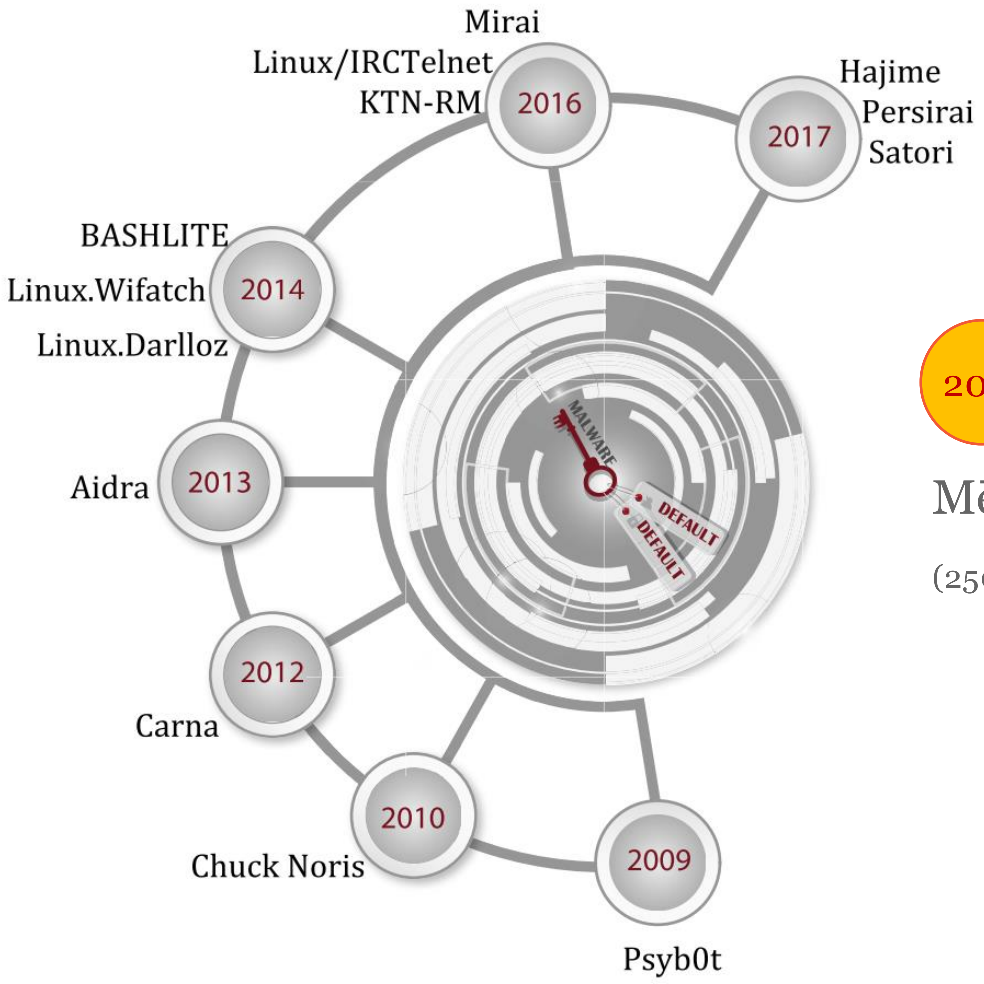


Discussion Question #1

- How would you scan IPv6?
- How would your scanning infrastructure look like?

IoT Botnets





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

UNIVERSITY OF TWENTE. SIDN LABS

Full IPv6 Scanning

- Using the current rates of IPv4 scans, it would take

$9*10^{24}$ years[1]

to run a full IPv6 scan[2].

- Not even scalable if we use all IoT devices[2] in the world to conduct the scan!

1) $2^{128}/(2^{32}*24*365)$

2) This includes reserved ranges as well, which are not typical scan targets.

3) Estimated to be 20B~30B

Allocated IPv6 Scanning

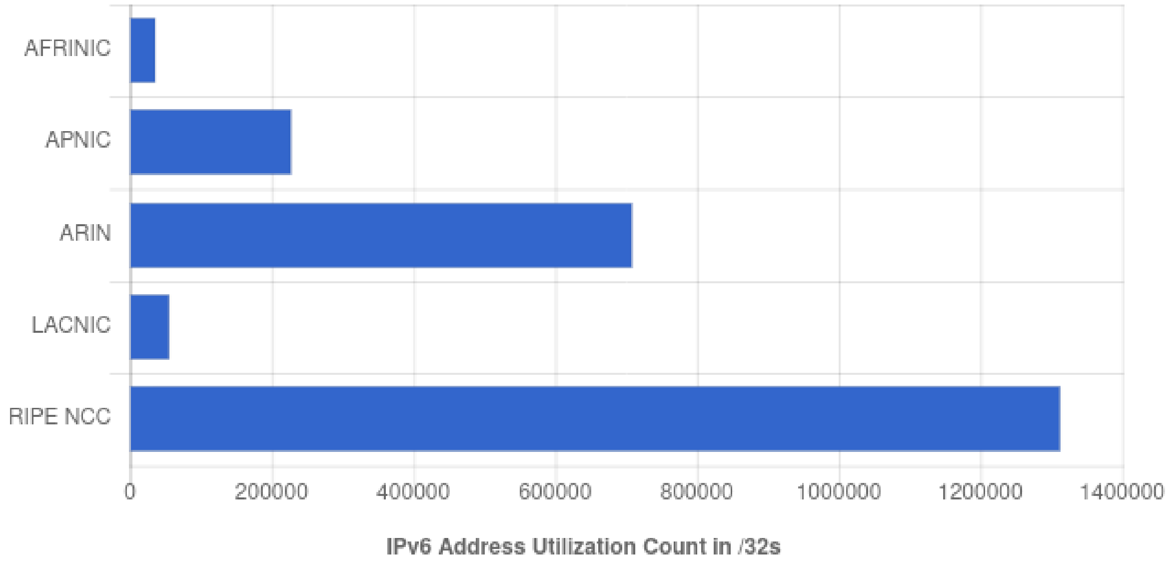
How long would it take to scan the already allocated IPv6 address space?

Currently* 2344177 /32s are allocated.

$2^{96} * 2344177 \approx 1.86 * 10^{35}$ individual IPs

Still would take $5 * 10^{21}$ years to scan!

Next Step to reduce our search space?



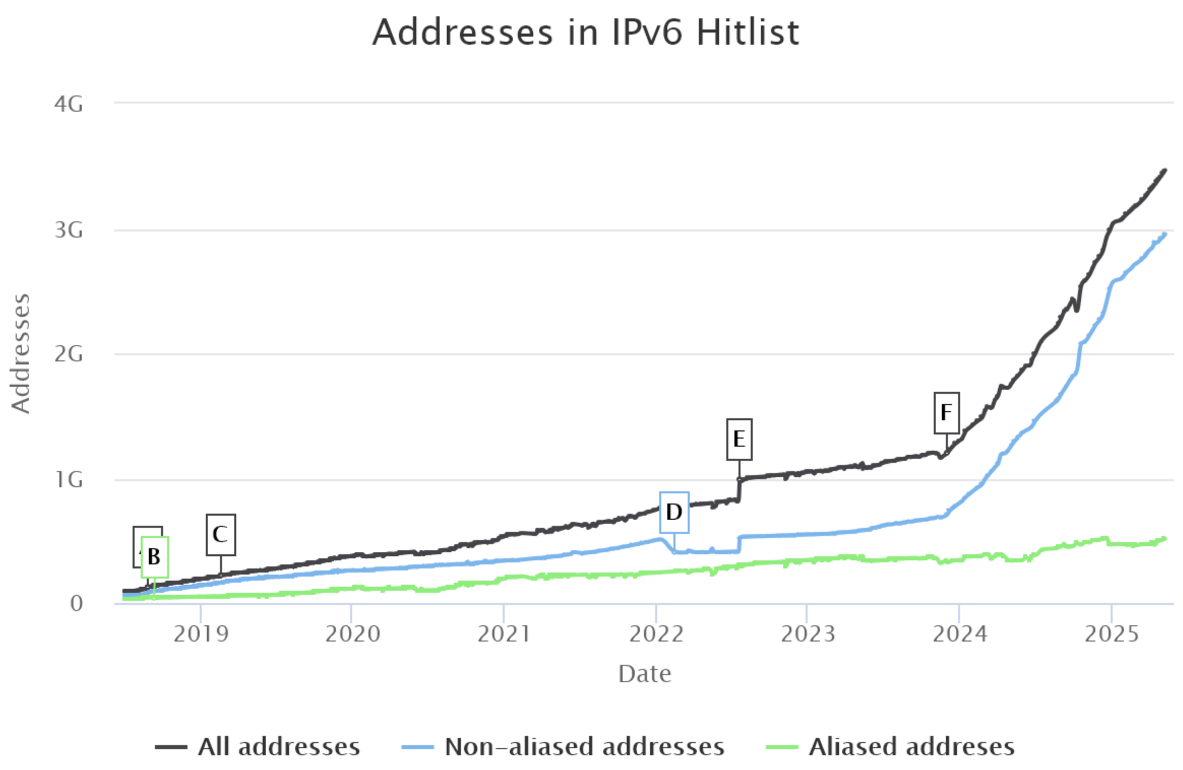
Source: https://www.iana.org/numbers/allocations/

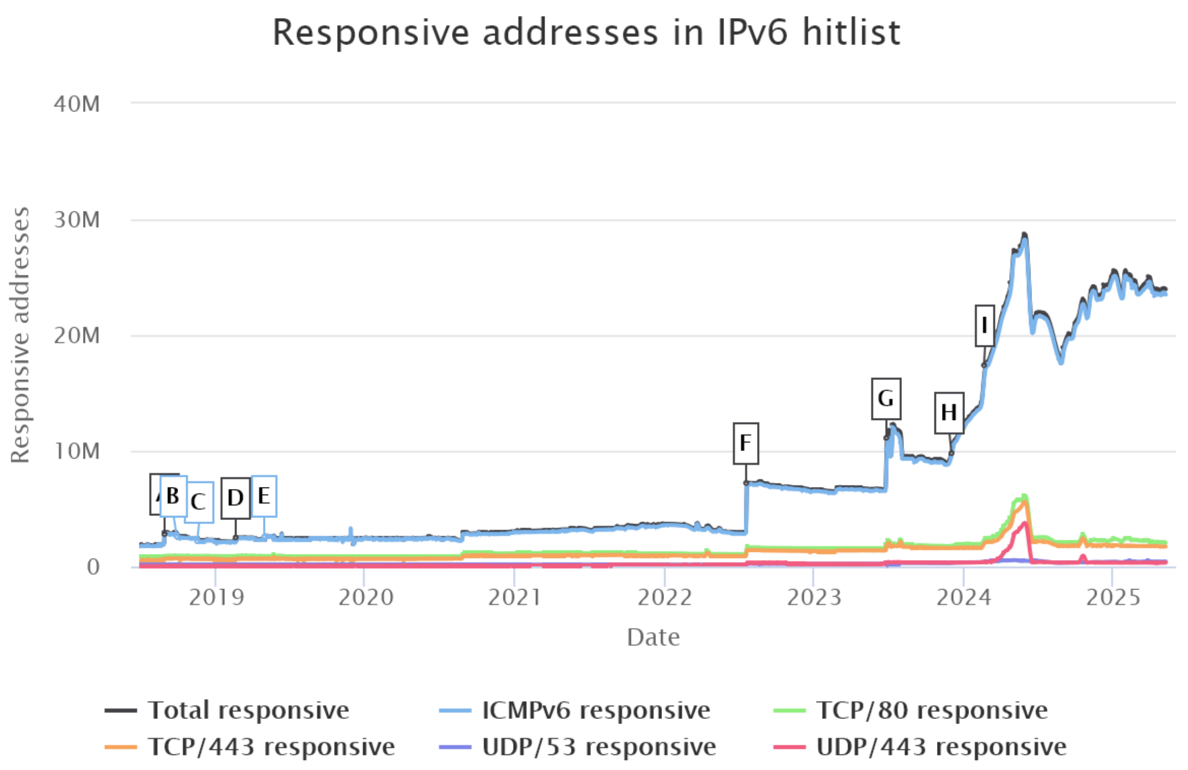
* On 2023-May-02

Target Addresses

- Authors investigate forward DNS entries: 75% of the /64s only target addresses in DNS.
- How would you create an IPv6 hitlist?
- The paper proposes using DNS records and then scanning other nearby addresses (this doesn't hold for all scanners, though).

IPv6 hitlists (new)





https://ipv6hitlist.github.io/

UNIVERSITY OF TWENTE.

SIDN LABS

Additional Reading (not on the exam)

- 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.
- Steger et al., "Target Acquired? Evaluating Target Generation Algorithms for IPv6", TMA 2023.

UNIVERSITY OF TWENTE. SIDN LABS

Discussion Question #2

- How would you detect IPv6 scanners?
    - Detection vantage points
    - Aggregation level (too coarse: conflating individual scan actors, too specific: can lead to missing scanning activities in part or entirely)
    - Other design choices?
- What would be a sound IDS policy to block IPv6 scanners? Can we have an adaptive aggregation?

What’s their methodology?

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

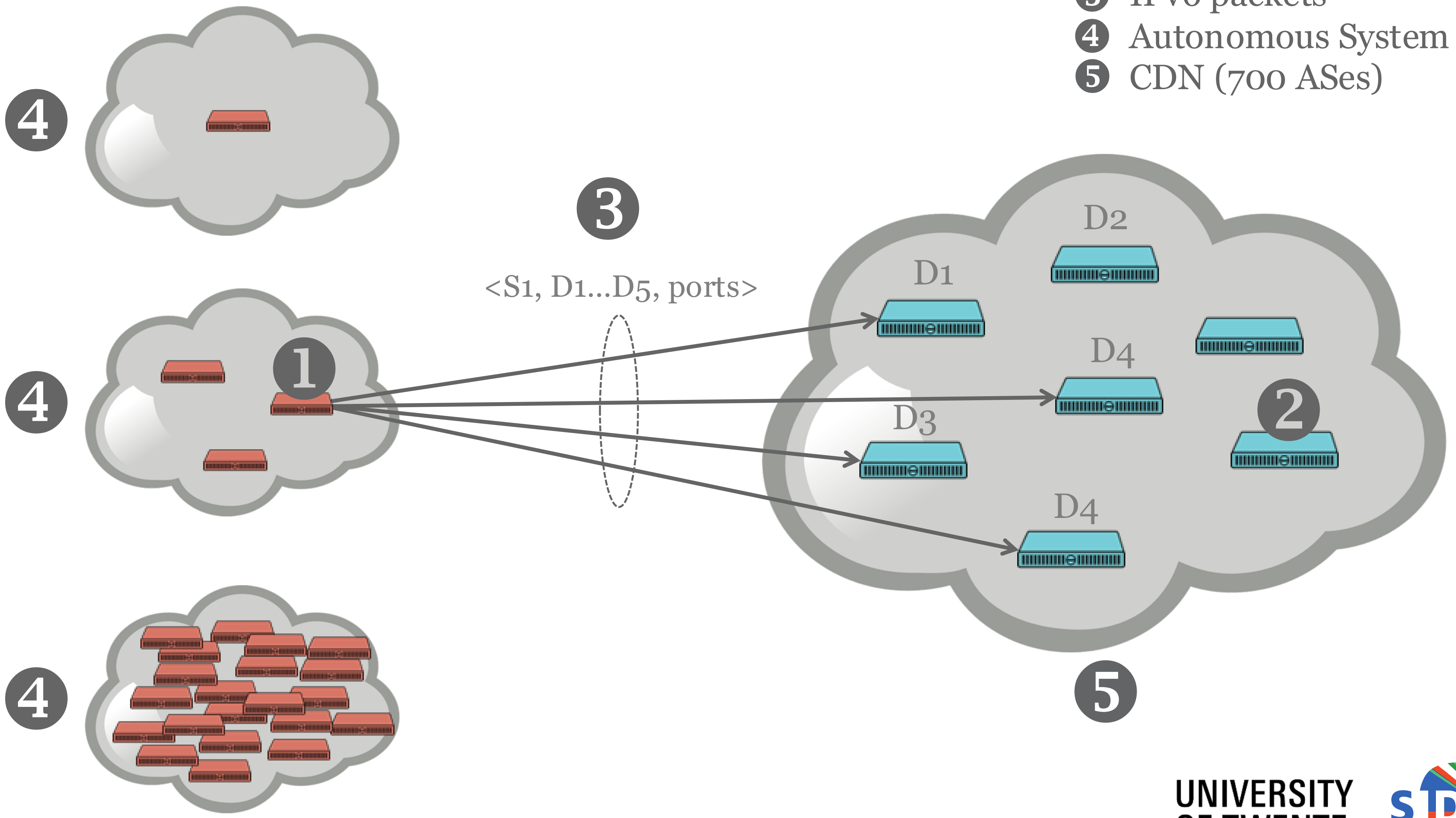
2. Create clusters of IPv6 addresses (scan sources)
   - Using well-known IPv6 prefixes
   - /48, /64, and /128

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

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

Paper measurement setup

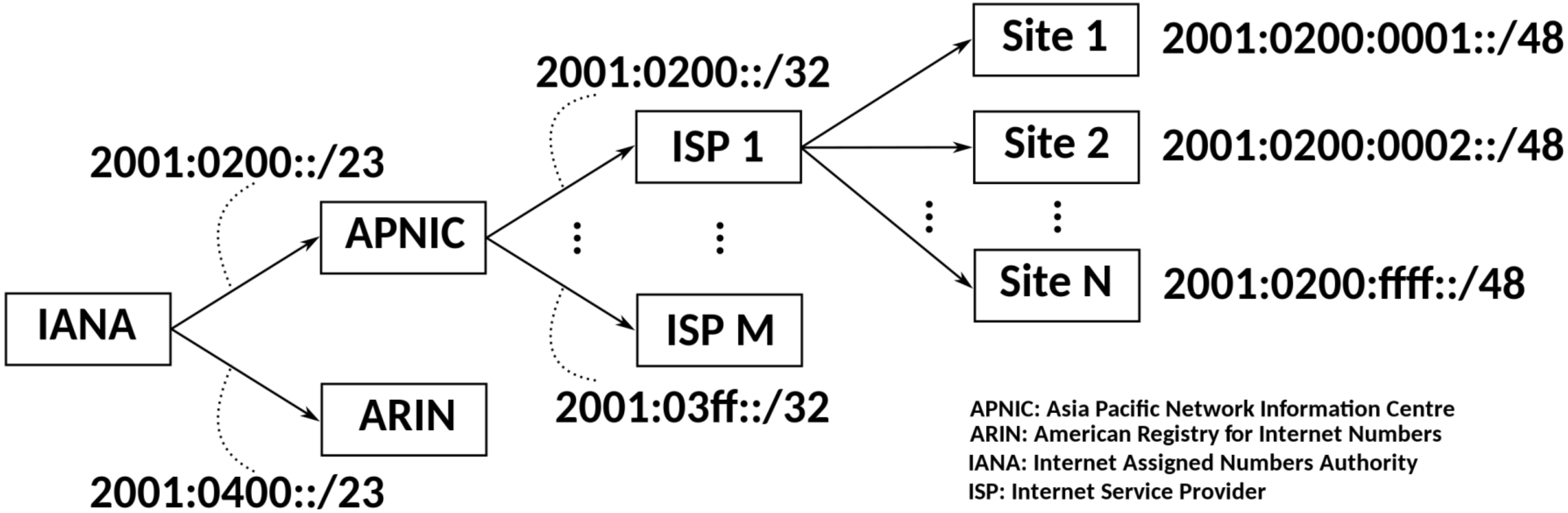
1. Scannning source
2. Server (320K)
3. IPv6 packets
4. Autonomous System (1 AS)
5. CDN (700 ASes)



UNIVERSITY OF TWENTE. SIDN LABS

/48, /64, and /128 aggregation

- Why is this aggregation special?



- Host size (Interface ID) is fixed to 64 bits.
  128 – 48 – 64 = 16 bits for subnet

n bits	m bits	128-n-m bits
Global unicast prefix	Subnet ID	Interface ID

UNIVERSITY OF TWENTE. SIDN LABS

Scan Sources

- The top-10 source ASes account for more than 99% of scan packets.
- Scans in IPv6 are mostly limited to datacenters and cloud providers. No exclusively residential ISPs in the top 20.
- What else do you find interesting from these two tables?

aggregation	scans	packets	sources	ASes
/128	65,485	2.04B	3,542	55
/64	5,199	2.14B	1,326	62
/48	5,019	2.15B	1,372	76

Table 1: Detected scans over the course of our measurement window (Jan 2021 until Mar 2022). Depending on the aggregation of source IP addresses, the number of scans and scan sources changes dramatically.

			scan sources		
rank	AS type	packets	/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

Target Ports

- IPv6 scans currently scan a range of ports similar to penetration testing (IPv4 scans typically target a single port).
    - 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.
- Which ports would you scan?

Key Takeaways

- IPv6 not only makes scanning itself more complicated, but also its detection.
- IPv6 scanners target a broad range of ports, in contrast to IPv4 scans.
- IPv6 scanning is presumably not yet originating from IoT botnets.

UNIVERSITY OF TWENTE. SIDN LABS

Today's learning objective revisited

To what extent to you think you'll be able to discuss the correlation between IoT security and Internet core protocols?

Q&A

Next lecture: **Fri May 23, 08:45-10:30**