Lecture #2: IoT security risks and challenges

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

University of Twente | May 11, 2022

UNIVERSITY OF TWENTE.

SIDN LABS

UNIVERSITY OF TWENTE.

SDN LABS

Today's agenda

- Admin
- Introduction to today's lecture
- Paper on Demystifying IoT Security
- Paper on the DNS in IoT
- Feedback

Admin

UNIVERSITY OF TWENTE.

SIDN LABS

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 oral exam

- Interactive format
  - Teachers summarize two papers per lecture
  - Multiple-choice and open questions (not graded) and discussion
  - ~~We ask at least one of you to share their thoughts on each paper (main lesson learned, etc.)~~
  - 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

UNIVERSITY OF TWENTE.

SIDN LABS

Experiment: interactive quizzes through wooclap

Multiple-choice questions: 30 seconds
Open questions: 1 minute

UNIVERSITY OF TWENTE.

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

No.	Date	Contents
1	Apr 26	Course introduction Guest lecture #1: IoT and SPIN
2	May 11	Lecture: IoT security risks and challenges
3	May 18	Lecture: IoT Botnet Measurements
4	May 24	Guest lecture #2: Intro to cyber-physical systems (Jeroen Gaiser, Rijkswaterstaat)
5	May 25	Lecture: IoT Malware Analysis
6	Jun 1	Lecture: IoT Edge Security Systems
7	Jun 7	Lecture: IoT Device Security
8	Jun 14	Guest lecture #3: Strengthening the IoT Ecosystem: Privacy Preserving IoT Security Management (Dr Anna Maria Mandalari, Imperial College London)
9	Jun 15	Lecture: IoT in Non-Carpeted Areas
10	Jun 22	Lecture: IoT Honeypots (re-sit)

UNIVERSITY OF TWENTE.

SIDN LABS

Important dates

- Two summaries per lecture: before the lecture (07:00 CEST) in which the papers will be discussed
- Lab report (PDF) and required files: **Sun June 26, 2022, 23:59 CEST**
- All to be submitted through CANVAS

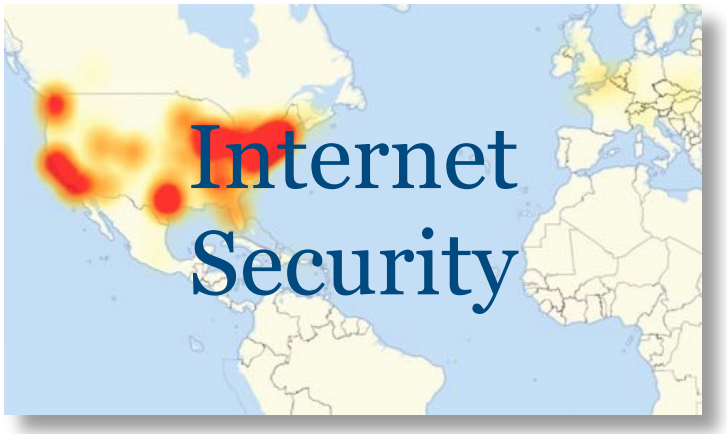
Introduction to today's lecture

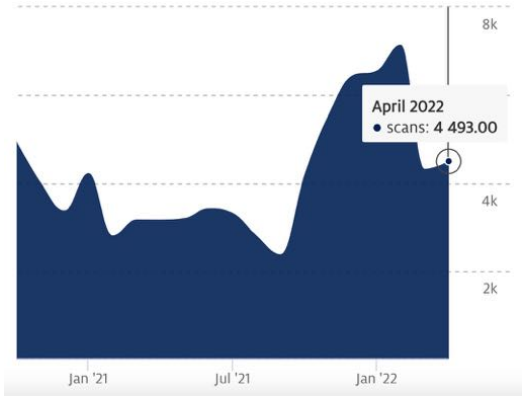
UNIVERSITY OF TWENTE.

SIDN LABS

Motivation: impact of insecure IoT devices

[Mirai] [SPIN]





https://stats.sidnlabs.nl/en/security.html#mirai%20scans

[Castle] [SPIN]

User Privacy

[DNSIoT] [Lora] [Traffic] [2stic.nl]

User Safety

UNIVERSITY OF TWENTE.

SIDN LABS

Today's papers

[IoTSurvey] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "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, 2019

[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

Today's learning objective

- After the lecture, you will be able to discuss different types of IoT security risks (vulnerabilities, attacks) and defense mechanisms to mitigate these risks

- Not very technical, 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"

“Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations”

IEEE Communications Surveys & Tutorials, 2019

UNIVERSITY OF TWENTE.

SIDN LABS

Security in IoT vs IT

- IoT applications require a stricter security due to potential to cause injury and drastic accidents leading to fatalities.

The Infamous 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/

UNIVERSITY OF TWENTE.

SIDN LABS

Challenges

- Resource limitations make it challenging to satisfy security best practices.
- Heterogeneity of IoT software and communication protocols demands security solutions different than traditional IT.
- Stakeholders think that others are responsible to mitigate security risks (called security externality.
- Short time-to-market results in overlooking security.

...

Addressing Resource Limitation

Edge security systems:

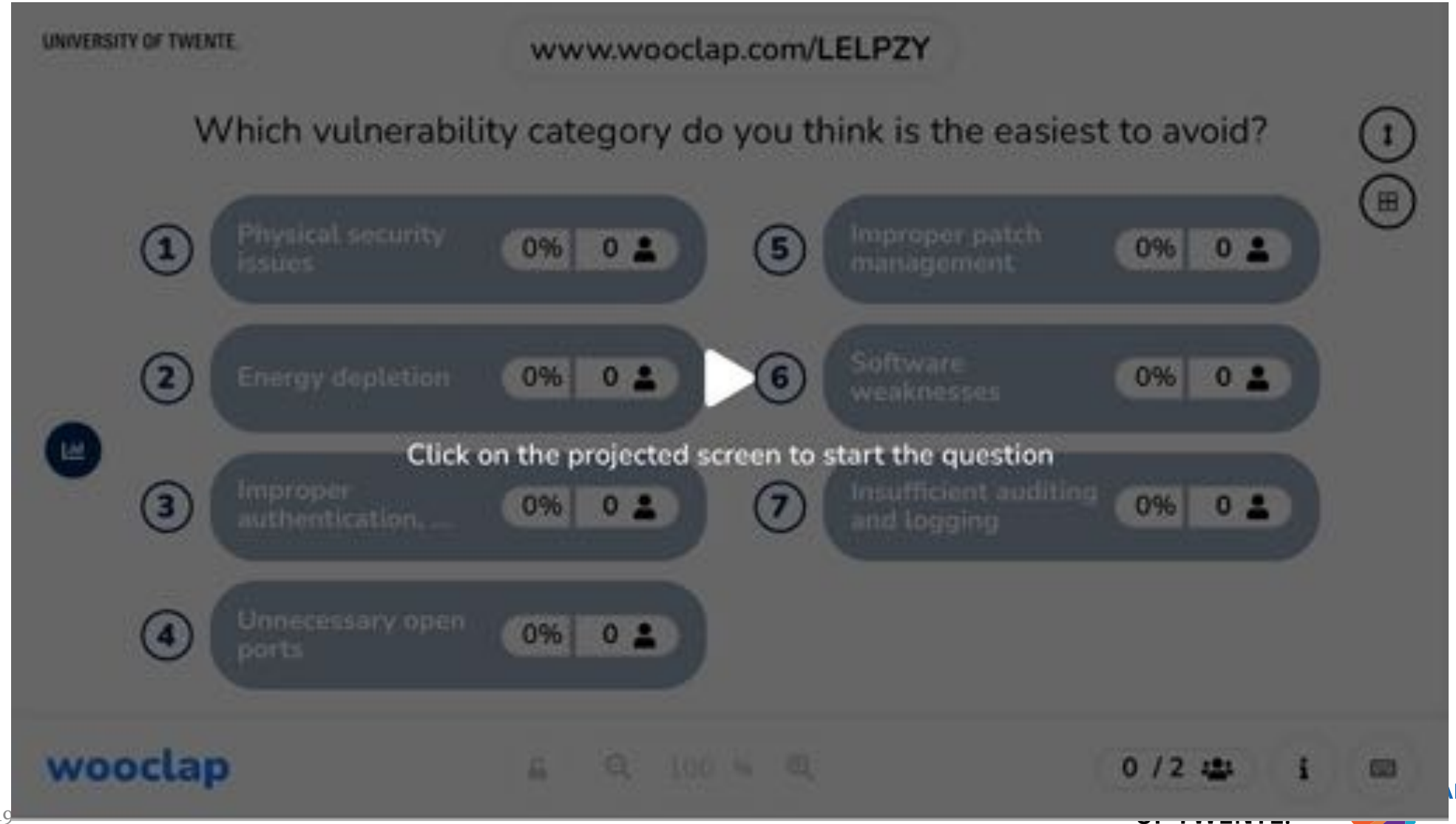
- Commercial solutions: it is unclear whether their claims match security requirements
- Research solutions: not deployed and tested in large scale Lecture#6 [ARA, DBolt]

UNIVERSITY OF TWENTE.

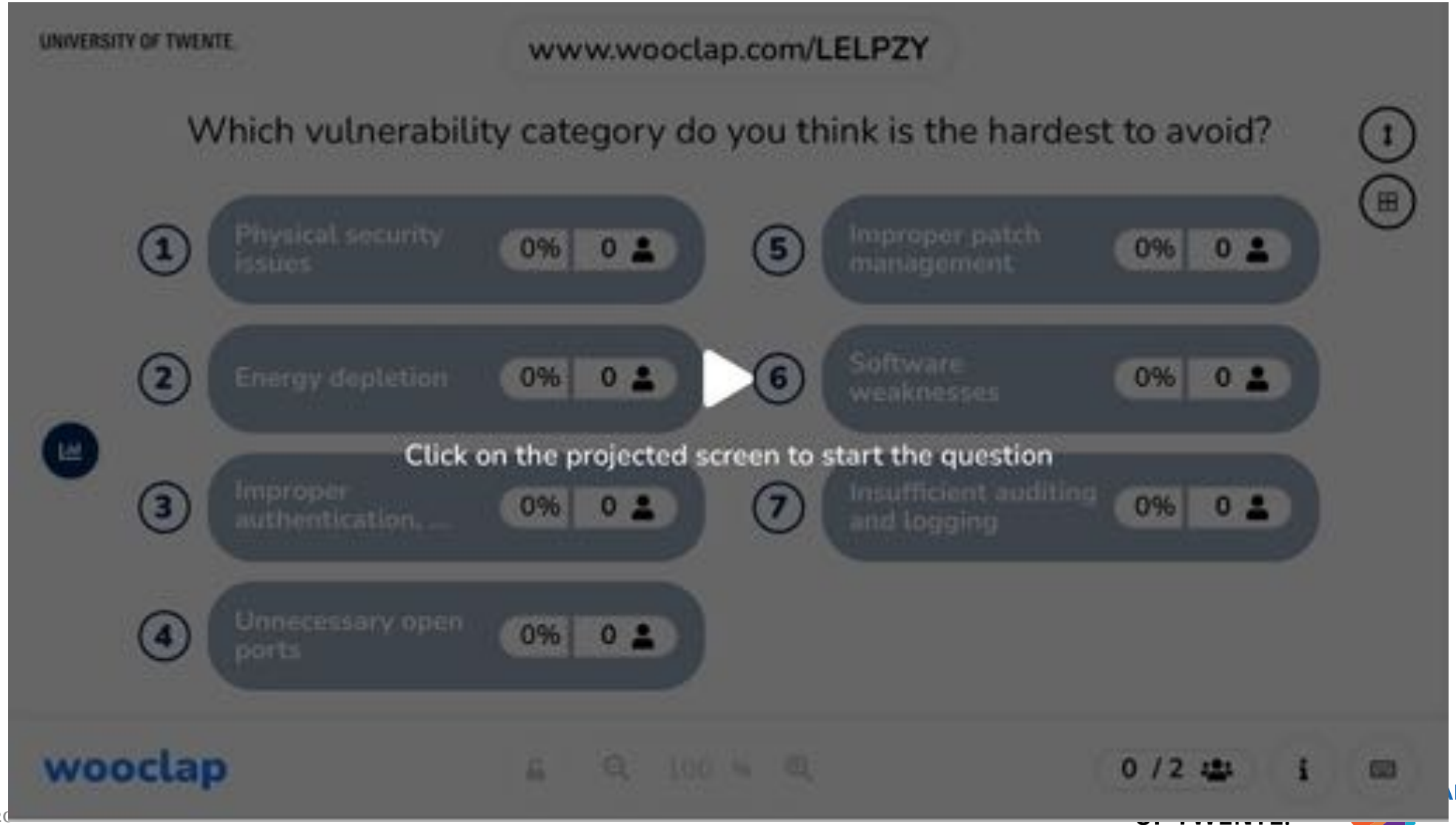
SIDN LABS

IoT Vulnerabilities

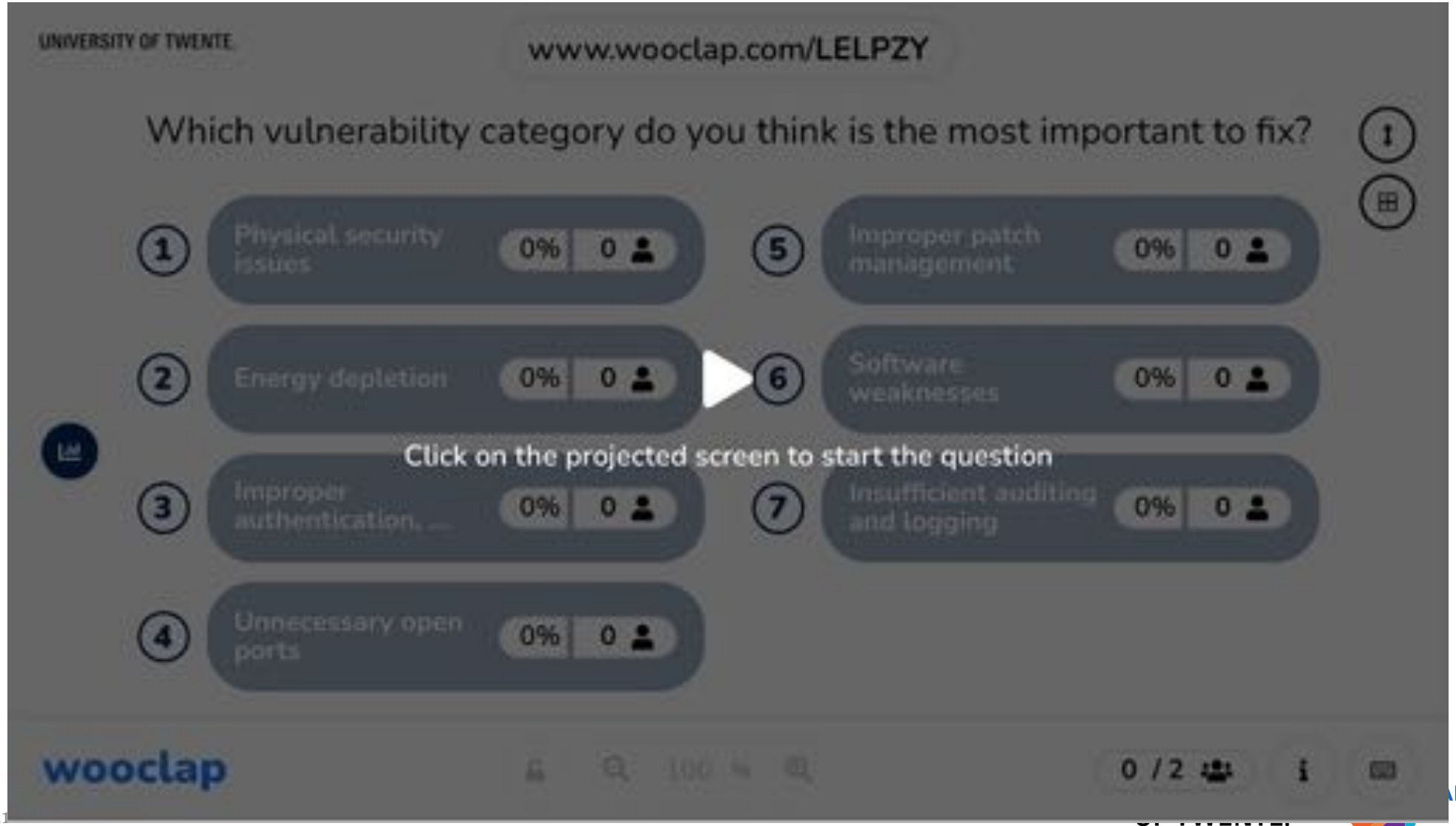
- Physical security issues
- Energy depletion Lecture #9 [Lora]
- Improper authentication, encryption and access control Lecture #3 [Mirai, Hajime], Lecture #7 [IoTLS]
- Unnecessary open ports Lecture #3 [Mirai, Hajime]
- Improper patch management Lecture #6 [DBolt]
- Software weaknesses Lecture #7 [IoTLS], Lecture #9 [Traffic]
- Insufficient auditing and logging Lecture #2 [DNSIoT]


UNIVERSITY OF TWENTE
www.wooclap.com/LELPZY
Which vulnerability category do you think is the easiest to avoid?
1
Physical security issues
0%
0
2
Energy depletion
0%
0
3
Improper authentication
0%
0
4
Unnecessary open ports
0%
0
5
Improper patch management
0%
0
6
Software weaknesses
0%
0
7
Insufficient auditing and logging
0%
0
Click on the projected screen to start the question
wooclap
0 / 2

Quiz 1/5


UNIVERSITY OF TWENTE
www.wooclap.com/LELPZY
Which vulnerability category do you think is the hardest to avoid?
1
Physical security issues
0%
0
2
Energy depletion
0%
0
3
Improper authentication
0%
0
4
Unnecessary open ports
0%
0
5
Improper patch management
0%
0
6
Software weaknesses
0%
0
7
Insufficient auditing and logging
0%
0
Click on the projected screen to start the question
wooclap
0 / 2

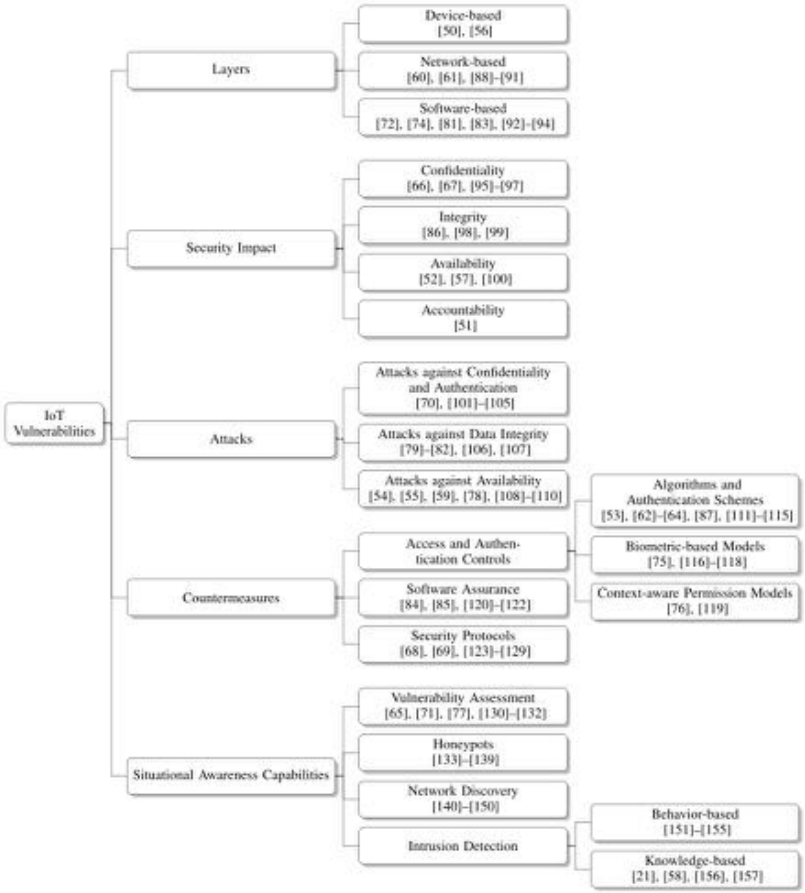
Quiz 2/5


UNIVERSITY OF TWENTE
www.wooclap.com/LELPZY
Which vulnerability category do you think is the most important to fix?
1
Physical security issues
0%
0
2
Energy depletion
0%
0
3
Improper authentication
0%
0
4
Unnecessary open ports
0%
0
5
Improper patch management
0%
0
6
Software weaknesses
0%
0
7
Insufficient auditing and logging
0%
0
Click on the projected screen to start the question
wooclap
0 / 2

Quiz 3/5

Taxonomy of IoT Security

- Layers
- Security Impact
- Attacks
- Countermeasures
- Situational Awareness Capabilities



UNIVERSITY OF TWENTE.

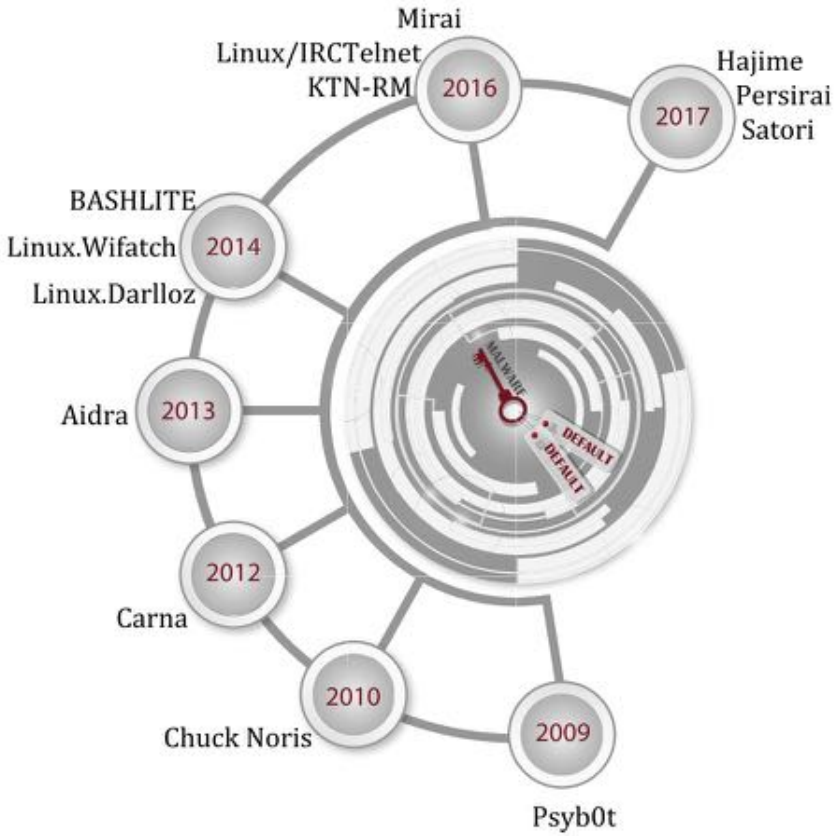
SIDN LABS

Layers: Where are the Vulnerabilities?

- Device-based
- Network-based Lecture #9 [Lora]
- Software-based Lecture #3 [Mirai, Hajime], Lecture #9 [Traffic]

IoT Malware

90% of investigated malware in [72] misuse default or weak credentials

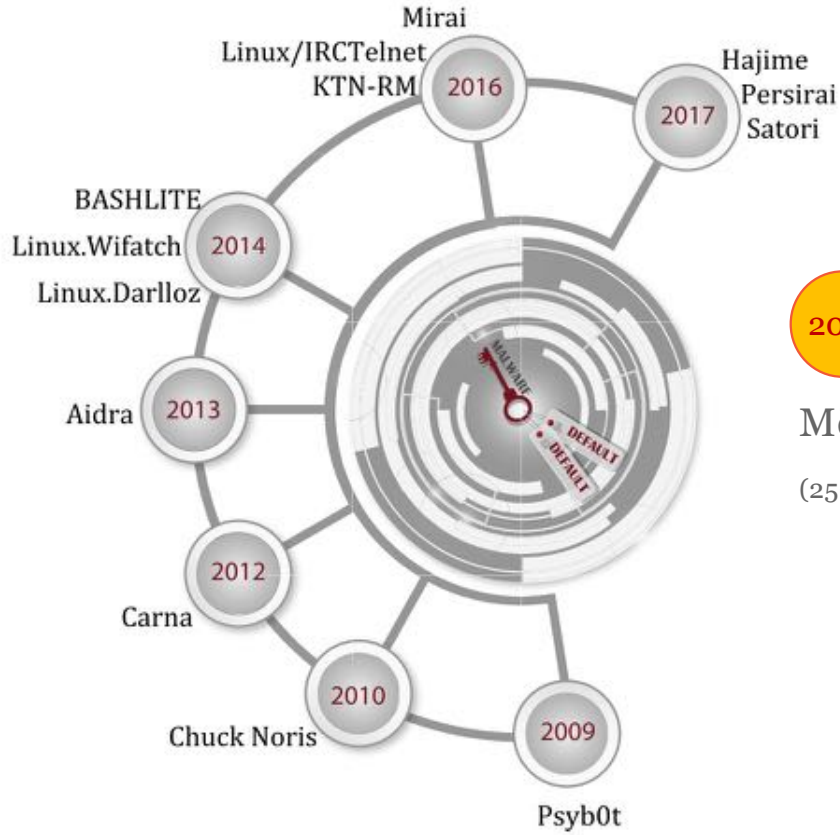


UNIVERSITY OF TWENTE.

SDN LABS

Mēris

- Vulnerability in RouterOS used in MikroTik routers
- "MikroTik RouterOS through 6.42 allows **unauthenticated** remote attackers to **read** arbitrary files and remote **authenticated** attackers to **write** arbitrary files due to a directory traversal vulnerability in the WinBox interface." [CVE-2018-14847]
- Patched in 2018 but many routers still use old versions or default credentials.



2021

Mēris

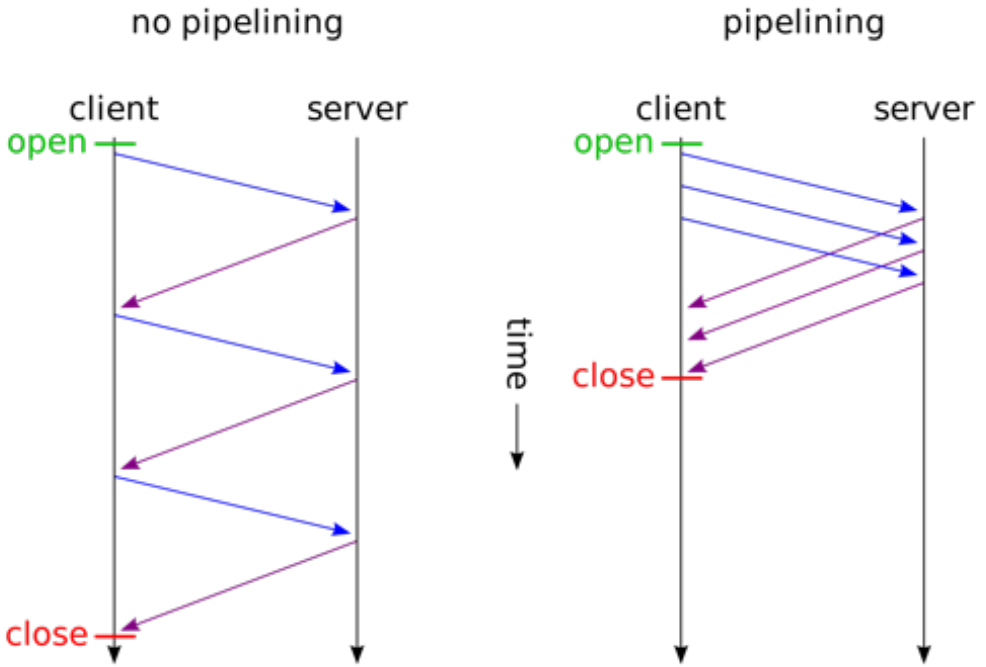
(250k infected MikroTik routers)

UNIVERSITY OF TWENTE.

SDN LABS

Mēris

- HTTP pipelining: **Browsers** usually don't use it, but **Bots** do so!!!
- Request flood (not volumetric)
- Routers are computationally and connectivity wise stronger than IoT devices
- Attacked Yandex using~56K attacking hosts



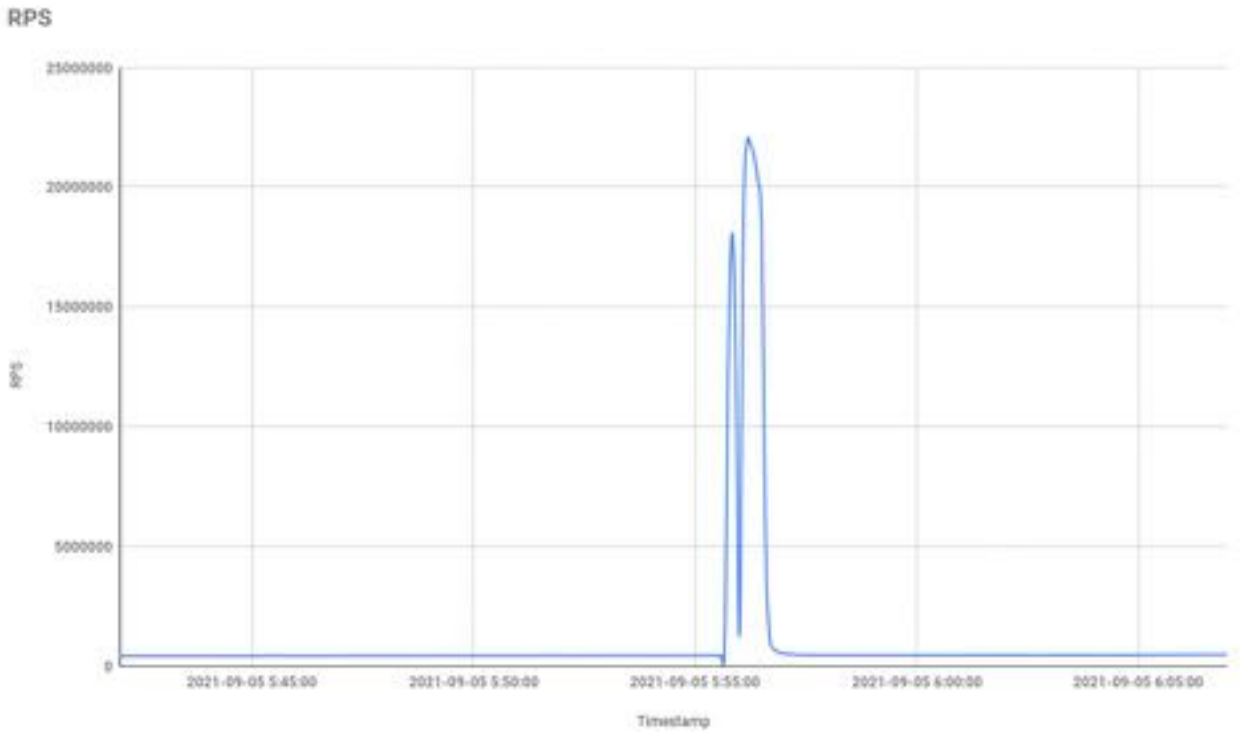
Source: Wikipedia

More details on: https://blog.qrator.net/en/meris-botnet-climbing-to-the-record_142/

UNIVERSITY OF TWENTE.

SDN LABS

Mēris



DDoS attack on Yandex, September 5, 2021

More details on: https://blog.qrator.net/en/meris-botnet-climbing-to-the-record_142/

UNIVERSITY OF TWENTE.

SIDN LABS

Security Impacts and Attacks

- **Confidentiality:** side channel attacks
- **Integrity:** firmware modification, BrickerBot (corrupting storage)
- **Availability:** DDoS (Mirai, Cold Finland), Permanent DoS (device capture)
- **Accountability** Lecture #2 [DNSIoT], Lecture #3 [Mirai]

Other examples?


UNIVERSITY OF TWENTE
www.wooclap.com/LELPZY
Which of the following doesn't directly facilitate a dictionary attack?
1
1 Unnecessary open ports 0% 0
2 Insufficient access control 0% 0
Click on the projected screen to start the question
3 Improper encryption 0% 0
4 Weak programming practices 0% 0
wooclap
0 / 2

Quiz 4/5

Cold Finland

- DDoS attacks knock down systems controlling heating during winter in the city of Lappeenranta in eastern Finland.
- Denied admins to remote access the system.
- Affected devices were detached from the Internet till traffic was filtered out by an upstream provider.

Source: http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter

UNIVERSITY OF TWENTE. SIDN LABS

Countermeasures

- Access and Authentication Controls Lecture#6 [ARA, DBolt]
- Software assurance
- Security protocols Lecture #7 [IoTLS]

Situational Awareness

- Vulnerability assessment
  - Designing IoT testbeds is not straightforward (e.g., they need human interaction)*
  - Delays in the code execution of medical devices are fatal
- Honeypots re-sit lecture [IoTPoT, Honware]
- Network discovery: Censys, Shodan, Shadowserver, etc.
- Intrusion detection Lecture#6 [ARA, DBolt]

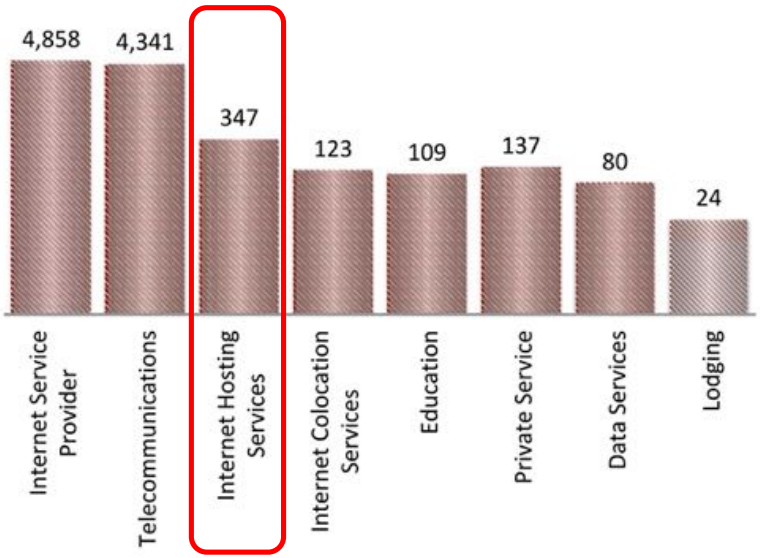
***Additional reading:** E. Leverett, R. Clayton, and R. Anderson, "Standardisation and Certification of the `Internet of Things'", 16th Annual Workshop on the Economics of Information Security (WEIS2017), USA, June 2017.


UNIVERSITY OF TWENTE
www.wooclap.com/LELPZY
What are the challenges in designing and running an IoT honeypot?
Let's vote!
Click on the projected screen to start the question
answers received
wooclap
0

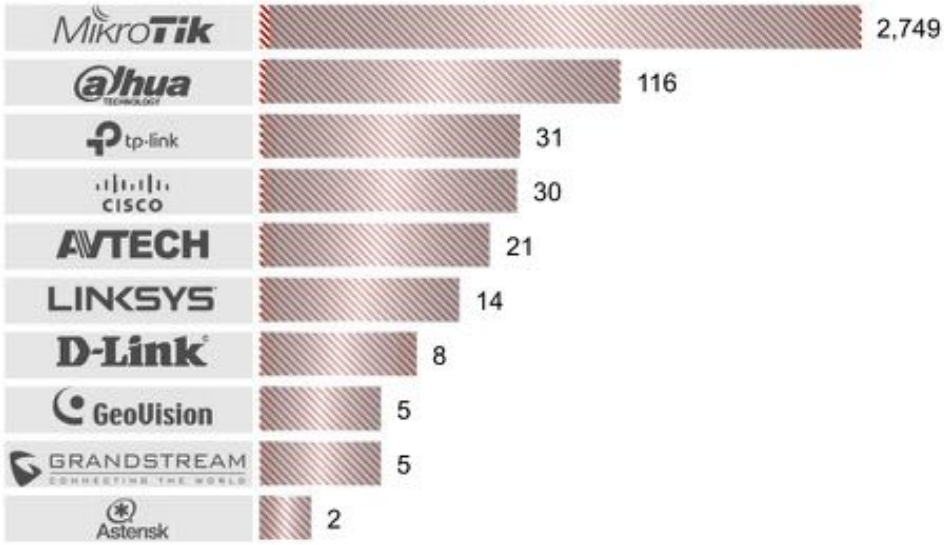
Quiz 5/5

Empirical Evaluation

Darknet data fused with Shodan data



Top sectors hosting exploited IoT devices



Top ten manufacturers of exploited IoT devices

UNIVERSITY OF TWENTE.

SIDN LABS

Key Takeaways

- IoT security impacts not only data, but also physical and human safety.
- Empirical studies play a big role in timely detection of IoT vulnerabilities.
- Patching IoT vulnerabilities is not always straightforward.

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

IEEE Internet Computing, July-Aug 2020

UNIVERSITY OF TWENTE.

SIDN LABS

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

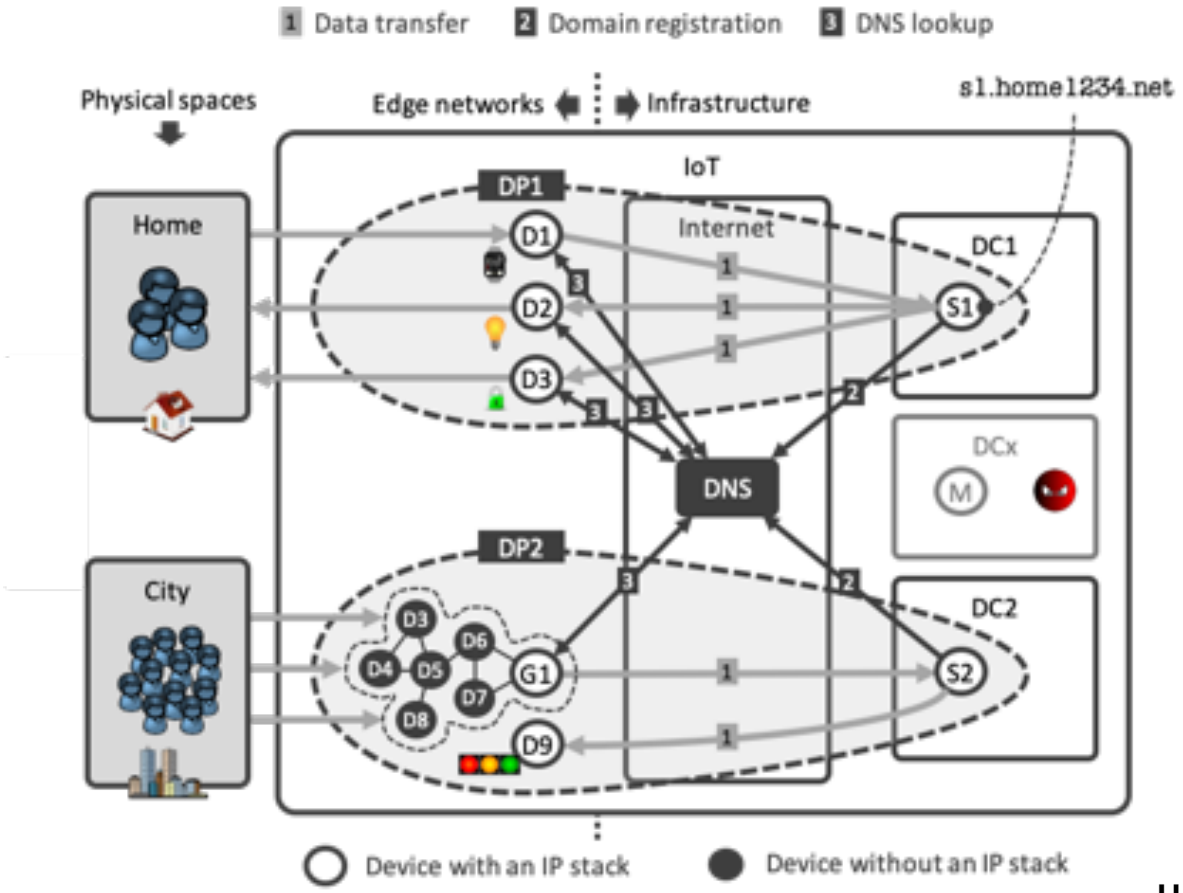
- Promises safer, smarter, more sustainable society, but **IoT security is a major challenge**

[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


UNIVERSITY OF TWENTE.
www.wooclap.com/LELPZY
What is the key characteristic of the IoT for you?
1
Let's vote!
0
answers received
00:56
wooclap
100 %
0

Quiz 1/6

IoT deployments and the Domain Name System (DNS)



DNS high-level operation

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

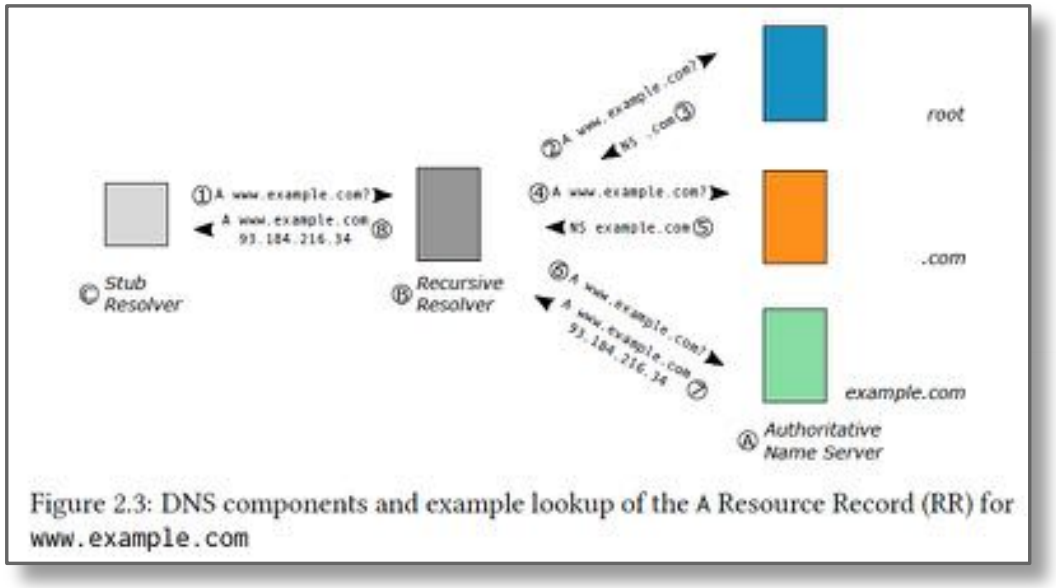
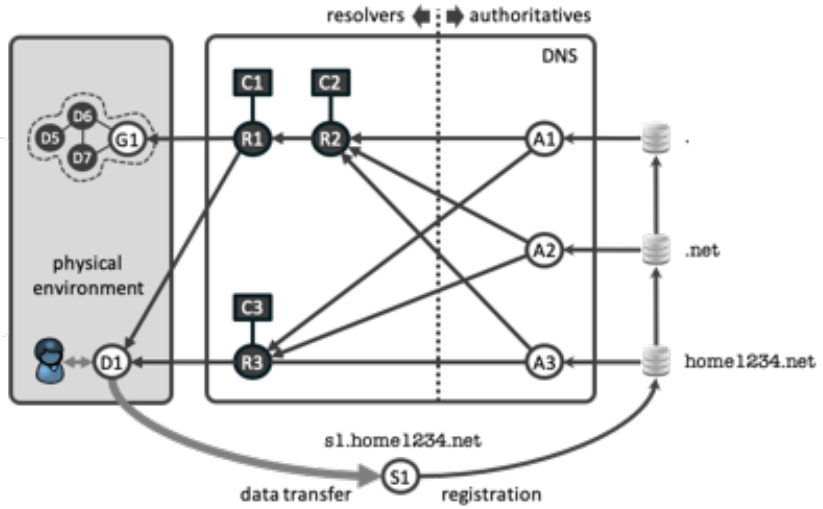
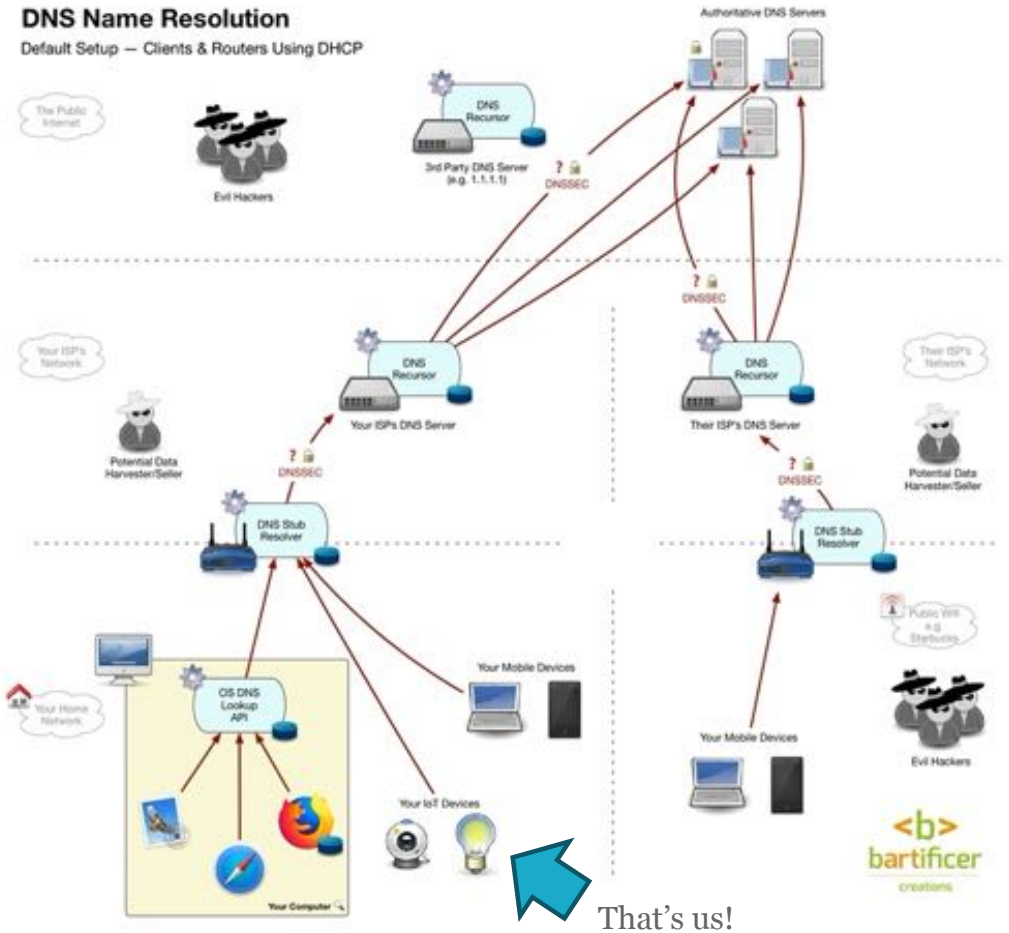


Figure 2.3: DNS components and example lookup of the A Resource Record (RR) for www.example.com



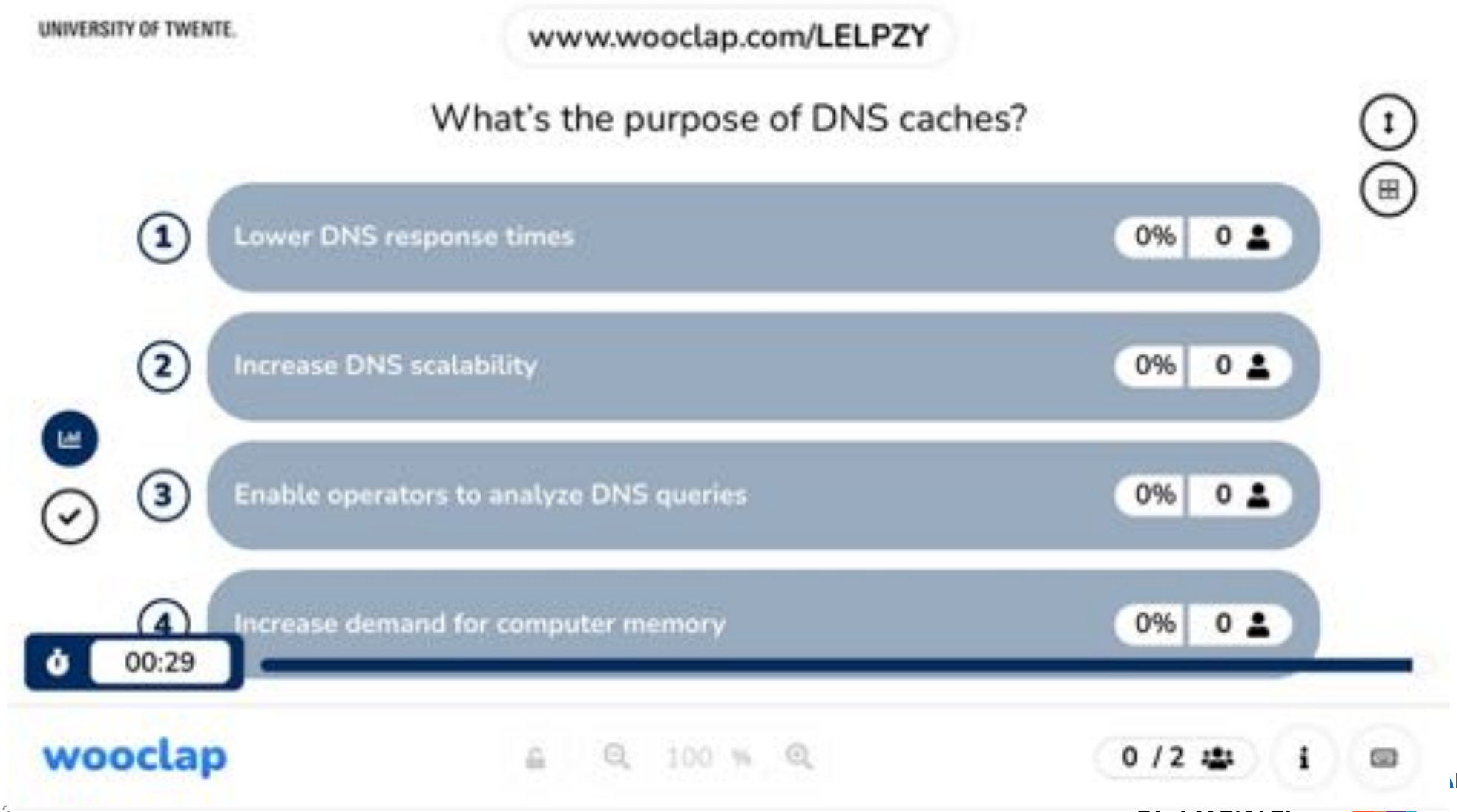
DNS ecosystem



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

UNIVERSITY OF TWENTE.

SIDN LABS


UNIVERSITY OF TWENTE.
www.wooclap.com/LELPZY
What's the purpose of DNS caches?
1
Lower DNS response times
0%
0
2
Increase DNS scalability
0%
0
3
Enable operators to analyze DNS queries
0%
0
4
Increase demand for computer memory
0%
0
00:29
wooclap
0 / 2

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

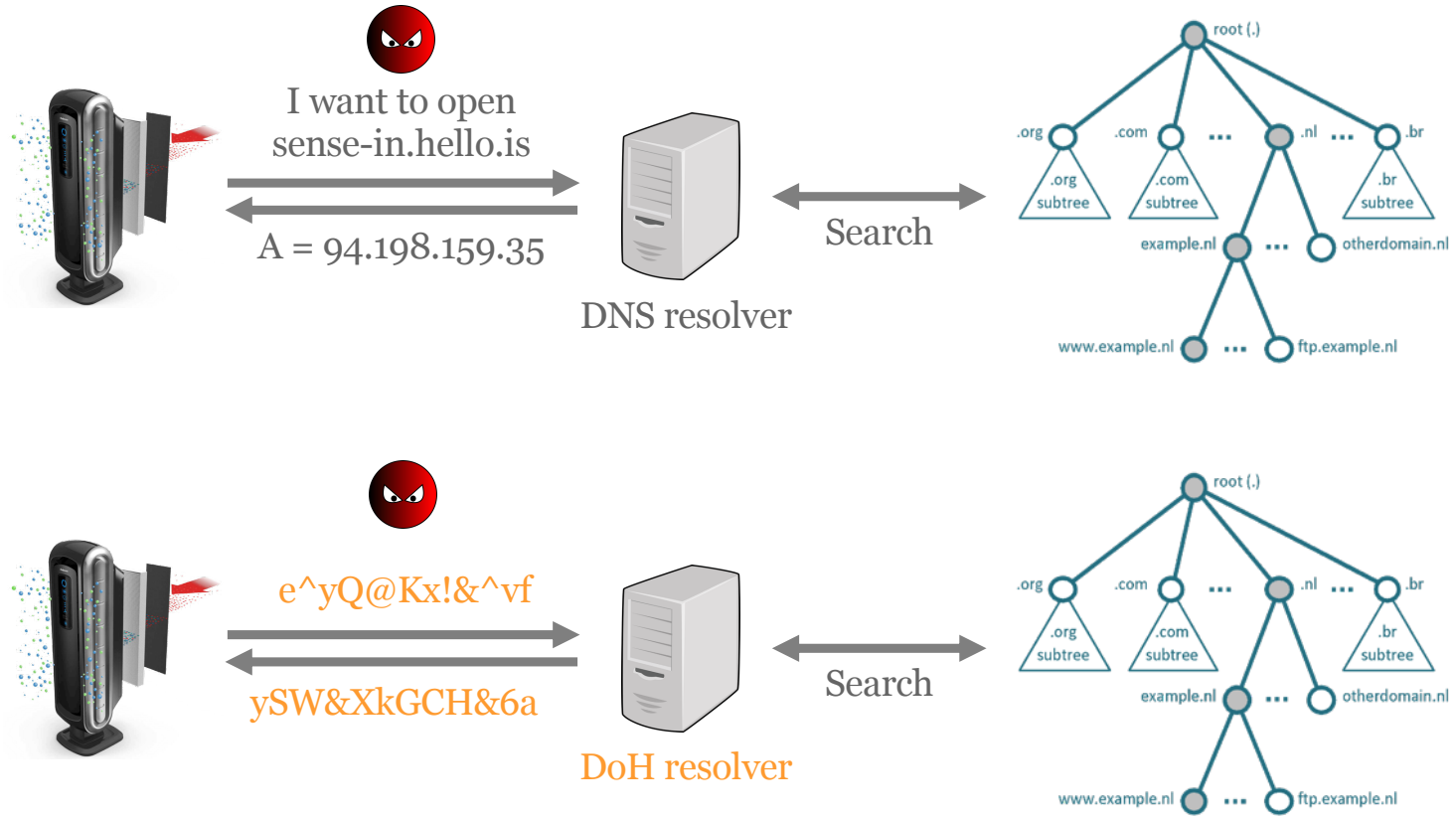
Technologies and systems that need to be developed

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

UNIVERSITY OF TWENTE.

SIDN LABS

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



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)

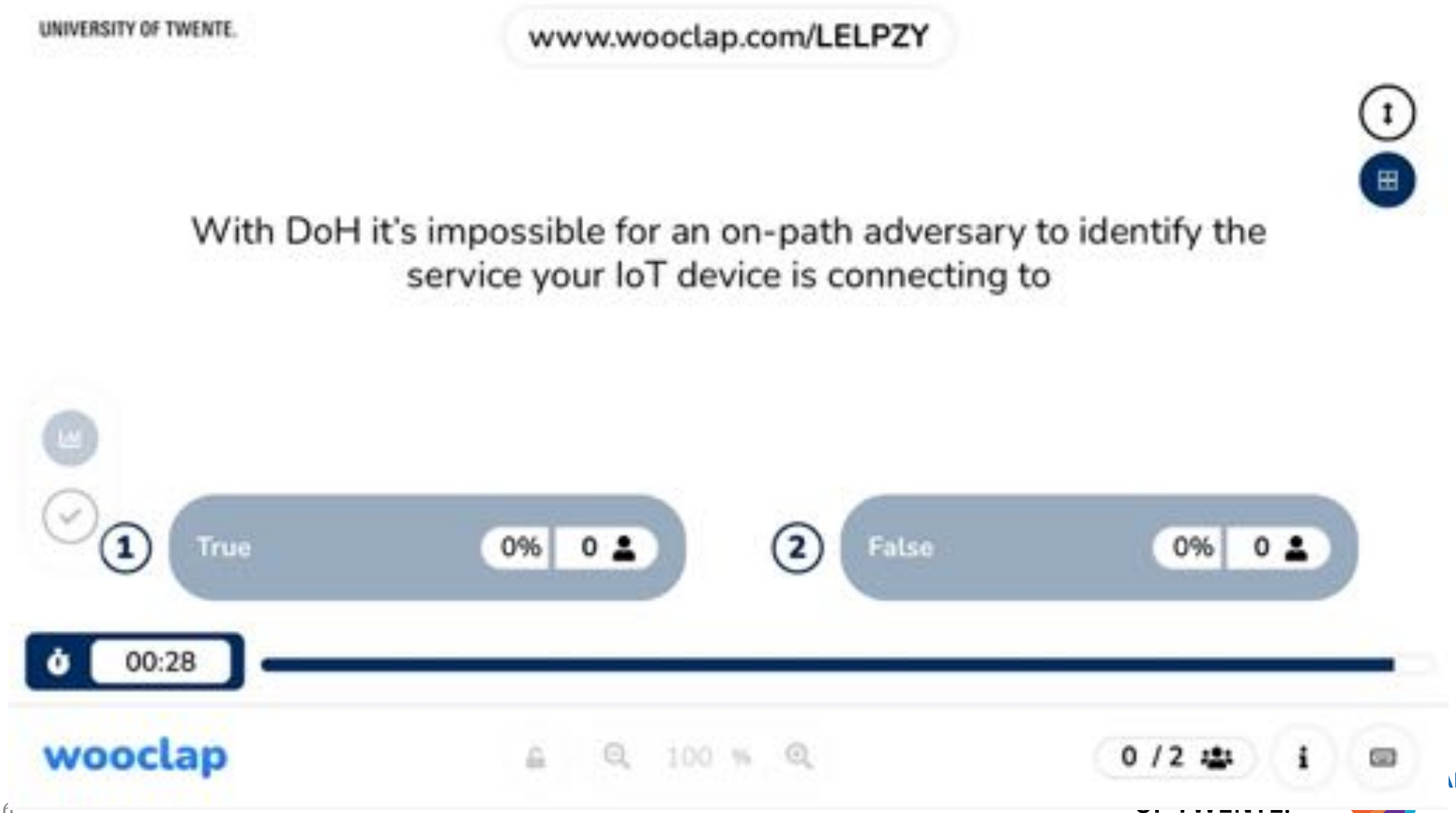
N. Apthorpe, D. Reisman, N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic", Workshop on Data and Algorithmic Transparency (DAT '16), New York University Law School, November 2016

Device	DNS Queries
Sense Sleep Monitor	hello-audio.s3.amazonaws.com hello-firmware.s3.amazonaws.com messyi.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	prodi-fs-xbcs-net-1101221371. us-east-1.elb.amazonaws.com prodi-api-xbcs-net-888336557. us-east-1.elb.amazonaws.com
Amazon Echo	am3-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.

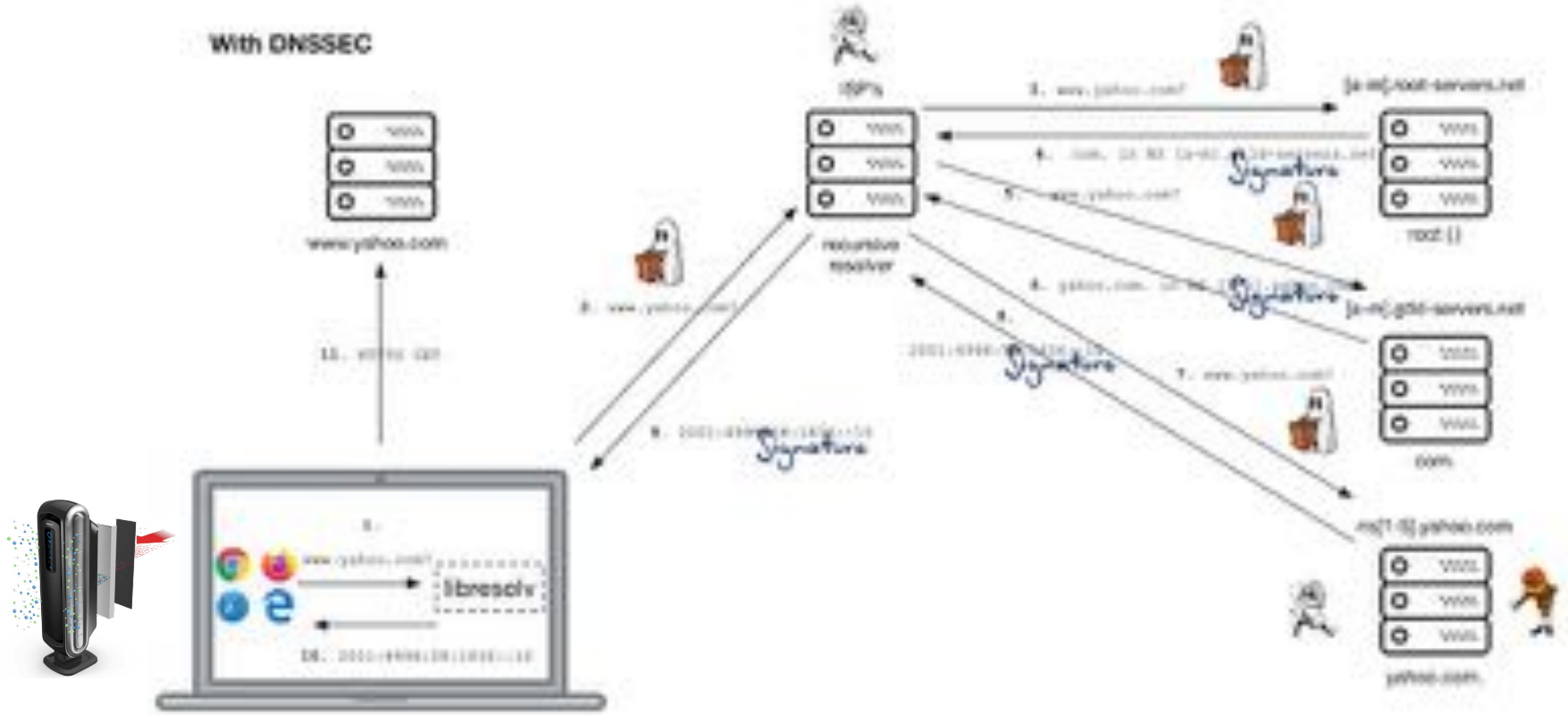
UNIVERSITY OF TWENTE.

SIDN LABS


UNIVERSITY OF TWENTE.
www.wooclap.com/LELPZY
With DoH it's impossible for an on-path adversary to identify the service your IoT device is connecting to
1
True
0%
0
2
False
0%
0
00:28
wooclap
0 / 2

Quiz 3/6

O2: Signing DNS responses with DNSSEC



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

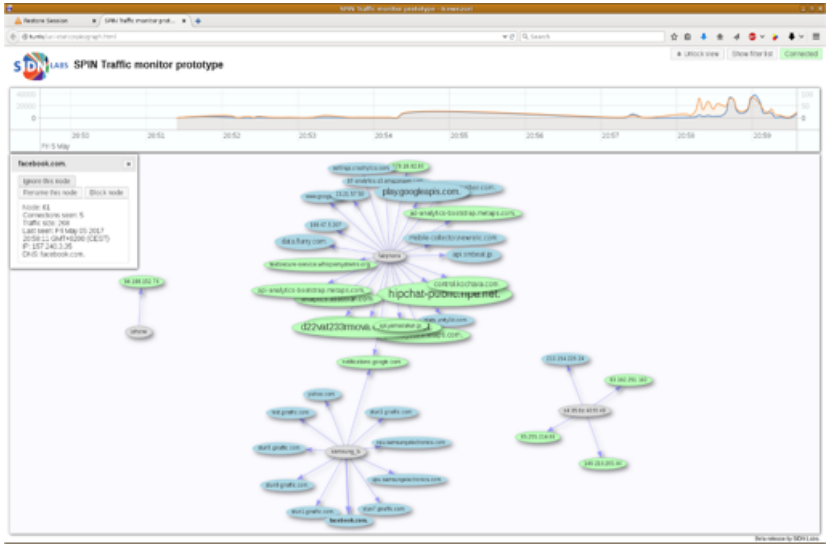
UNIVERSITY OF TWENTE.

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

O3: DNS queries



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

[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

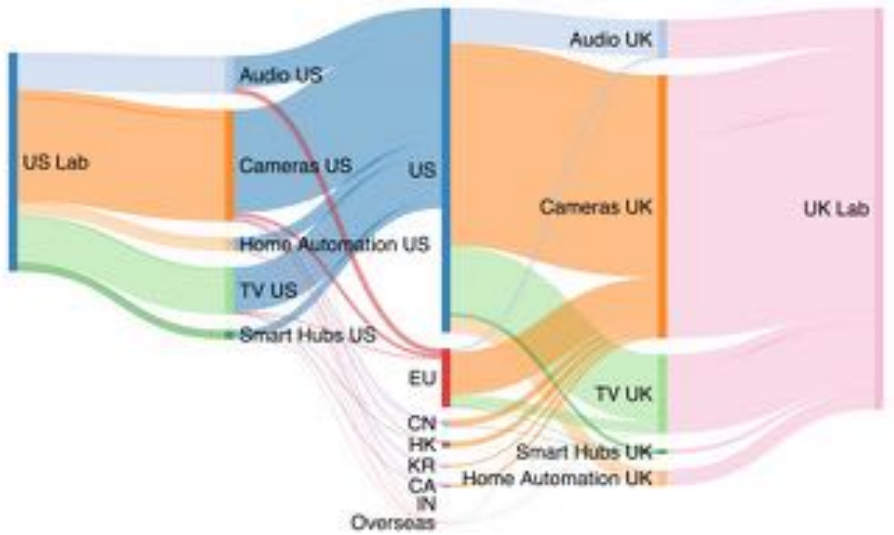
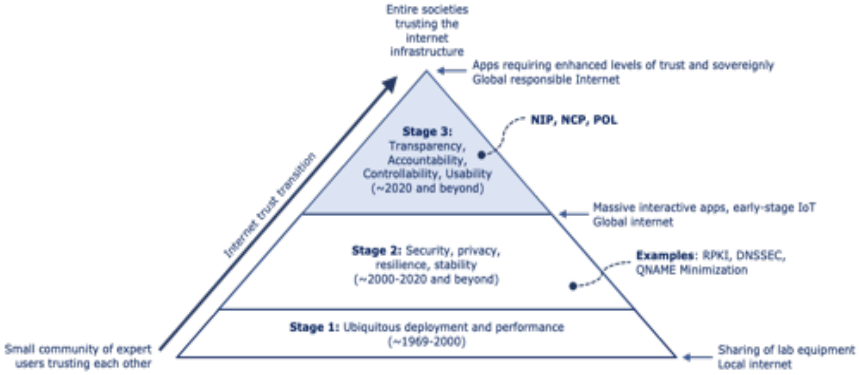


Figure 2: Volume of network traffic between the US (left) and UK (right) labs to the top 7 destination regions (center), grouped by category (middle left and right). Most traffic terminates the US, even for the UK lab; many devices send traffic to countries outside of their testbed's privacy jurisdiction.

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



UNIVERSITY OF TWENTE.

SIDN LABS


UNIVERSITY OF TWENTE.
www.wooclap.com/LELPZY
How would you make the IoT more transparent?
Let's vote!
0
answers received
00:58
wooclap
100 %
0

Quiz 4/6

R1: DNS-unfriendly programming at IoT scale

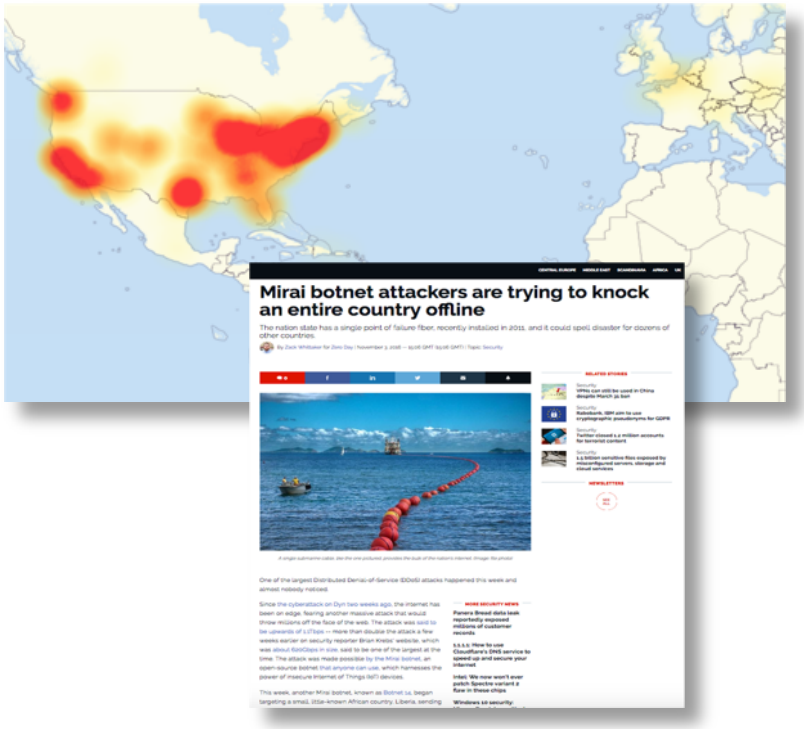
- TuneIn app example: 700 iPhones generating random queries `www.<random-string>.com`
- In the stone age (2012), but still: imagine millions of unsupported devices exhibiting that kind of behavior after a software update
- High-level APIs abstract DNS away from developers

UNIVERSITY OF TWENTE.

SIDN LABS

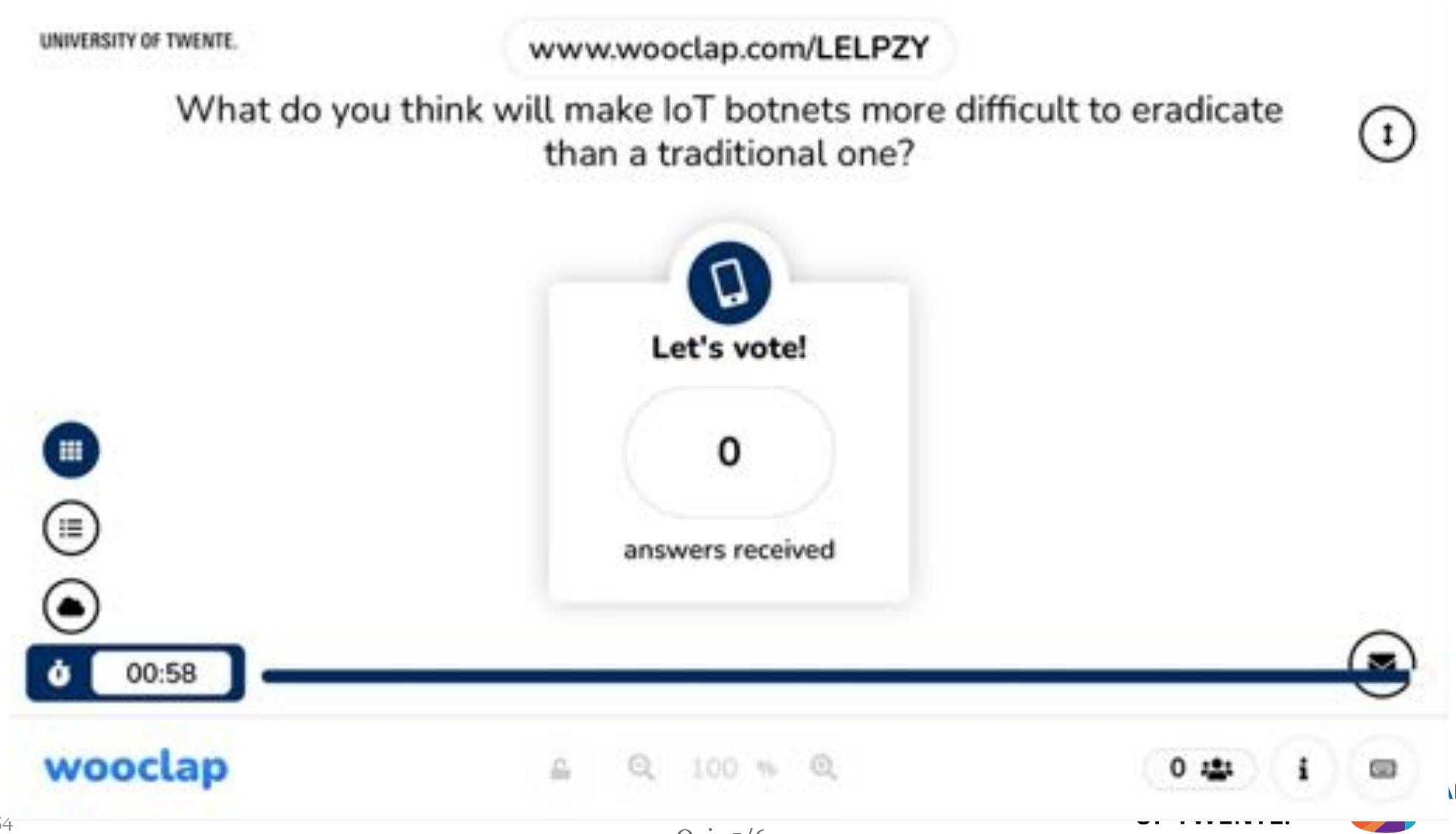
R2: DDoS attacks by IoT botnets

- 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


UNIVERSITY OF TWENTE.
www.wooclap.com/LELPZY
What do you think will make IoT botnets more difficult to eradicate than a traditional one?
Let's vote!
0
answers received
00:58
wooclap
100 %
0

Quiz 5/6

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

UNIVERSITY OF TWENTE.

SIDN LABS

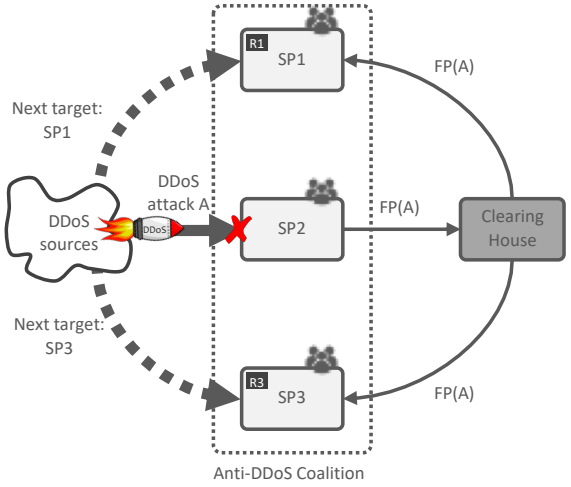
Why collaborative?

- 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


UNIVERSITY OF TWENTE.
www.wooclap.com/LELPZY
What do you think is the most important challenge for IoT security?
1
1 Flexible mitigation of IoT-powered DDoS traffic
2 Developing a DNS security and transparency library for IoT devices
3 Developing a system to share information on IoT botnets
Other...
00:28
wooclap
100 %
0 / 2

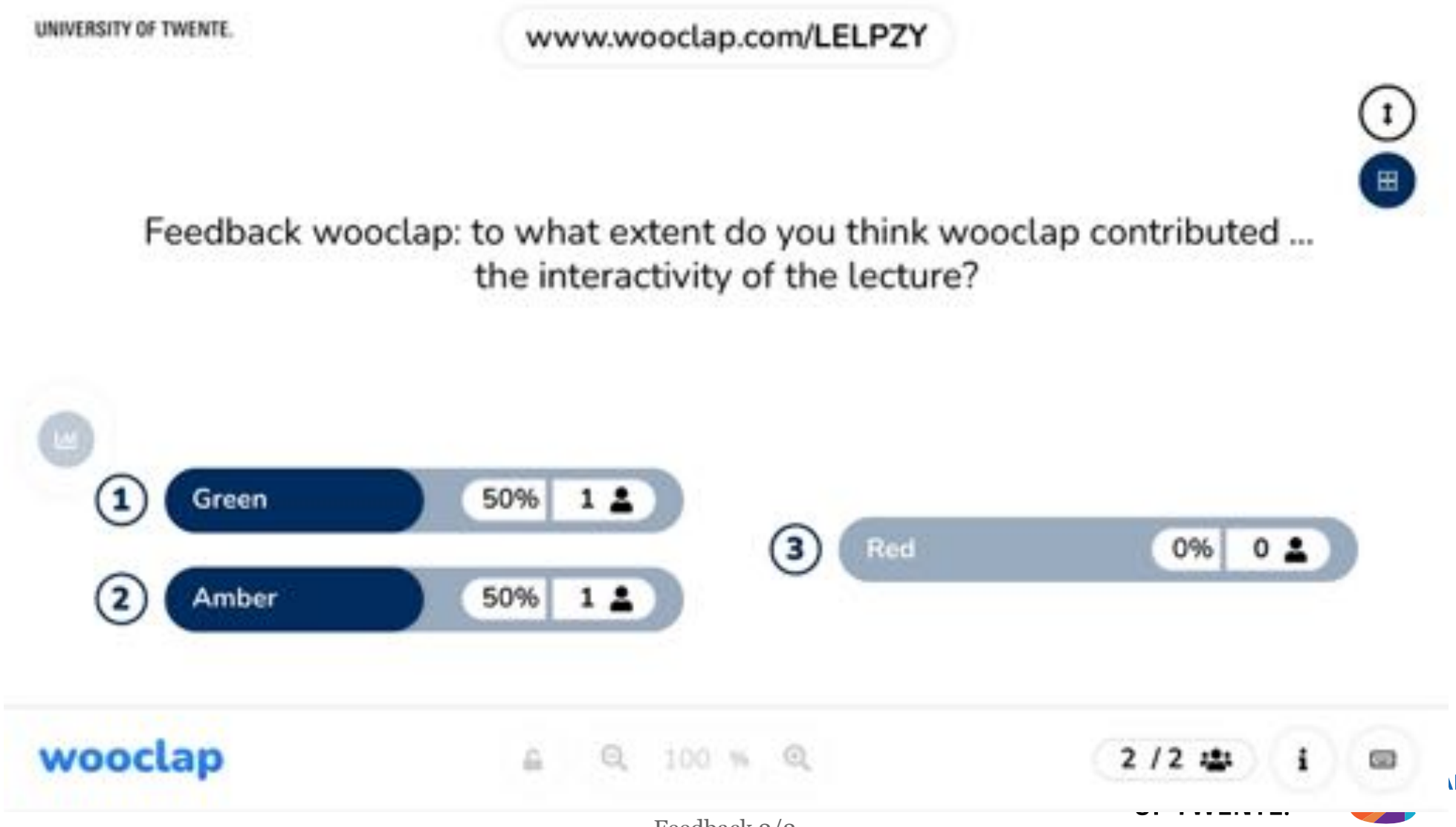
Key takeaways

- 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


UNIVERSITY OF TWENTE.
www.wooclap.com/LELPZY
Feedback learning objective: to what extent do you think you'll be abl...
to discuss different types of IoT security risks (vulnerabilities, attacks)
and defense mechanisms to mitigate these risks?
1 Green 0% 0
2 Amber 0% 0
3 Red 0% 0
wooclap
100 %
0 / 2


UNIVERSITY OF TWENTE.
www.wooclap.com/LELPZY
Feedback wooclap: to what extent do you think wooclap contributed ... the interactivity of the lecture?
1 Green 50% 1
2 Amber 50% 1
3 Red 0% 0
wooclap
2 / 2

Feedback 2/2

Volg ons

SIDN.nl

@SIDN

SIDN

Q&A

Next lecture: **Wed May 18, 10:45-12:30**

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