Security Services for the IoT: Introduction

Cristian Hesselman, Elmer Lastdrager, Ramin Yazdani, Etienne Khan, and Ting-Han Chen

UNIVERSITY OF TWENTE.

SIDN LABS

Teaching team

Cristian Hesselman
(teacher)

Elmer Lastdrager
(teacher)

Ramin Yazdani
(teaching assistant)

Etienne Khan
(teaching assistant)

Ting-Han Chen
(teaching assistant)

UNIVERSITY OF TWENTE.

SDN LABS

Today's goal

- Provide an overview of Security Services for the IoT (SSI)
- Answer any questions you may have on assessment, deliverables, etc.
- Result: understanding of SSI, the work you'll need to carry out, and some IoT inspiration

Agenda

- Four-slide high-level introduction to IoT security
- Course overview
- Brief introduction of SIDN Labs
- (Some more IoT slides)

Security issues in the IoT?

UNIVERSITY OF TWENTE.

SDN LABS

Internet of Things (IoT)

- Internet application that extends “network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers” (ISOC)

- 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

Intelligent Transport Systems

Smart energy grids

Smart homes and cities

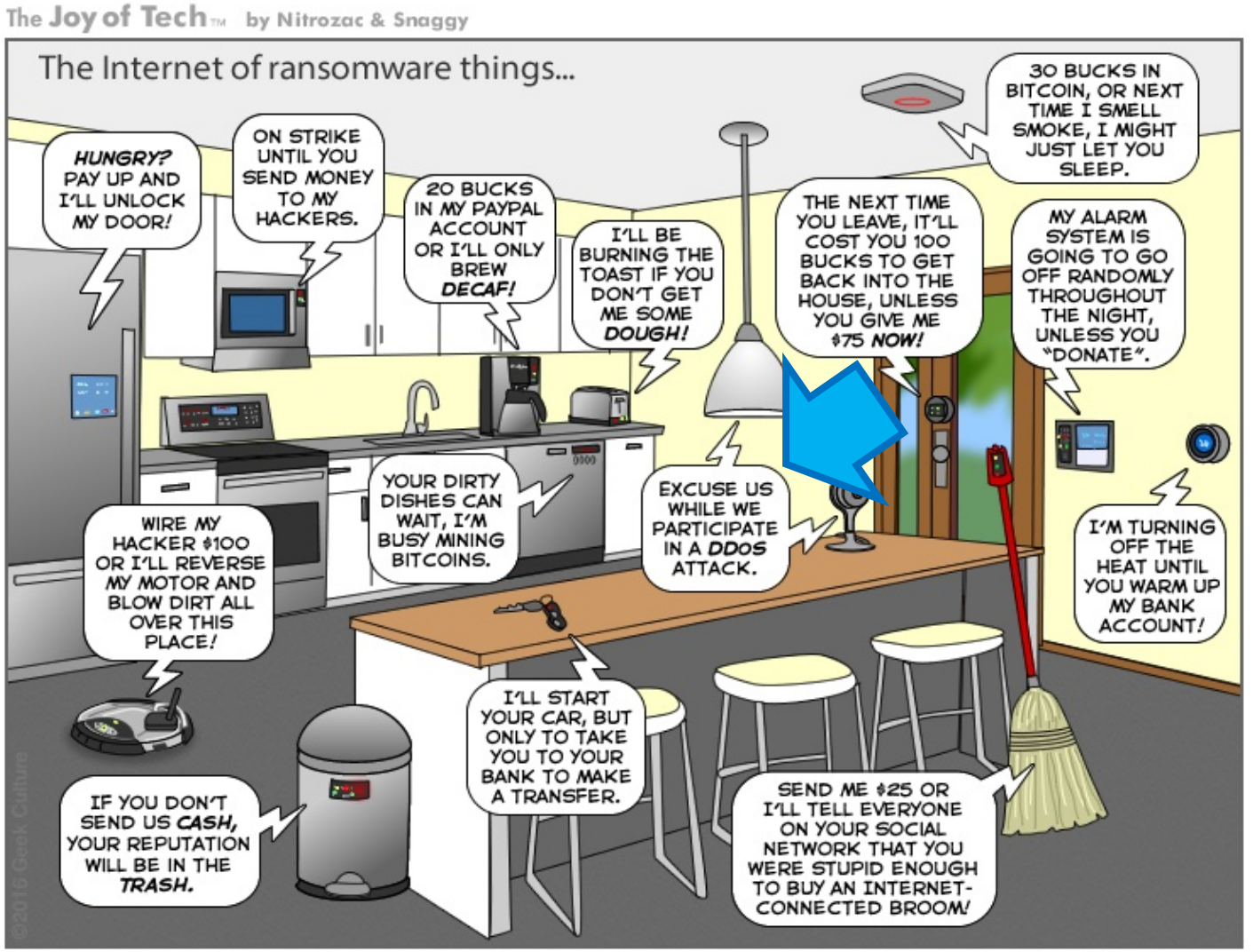
- Promises safer, smarter, more sustainable society, **but IoT security is a major challenge**

Further reading: [WEIS] [DNSIoT]

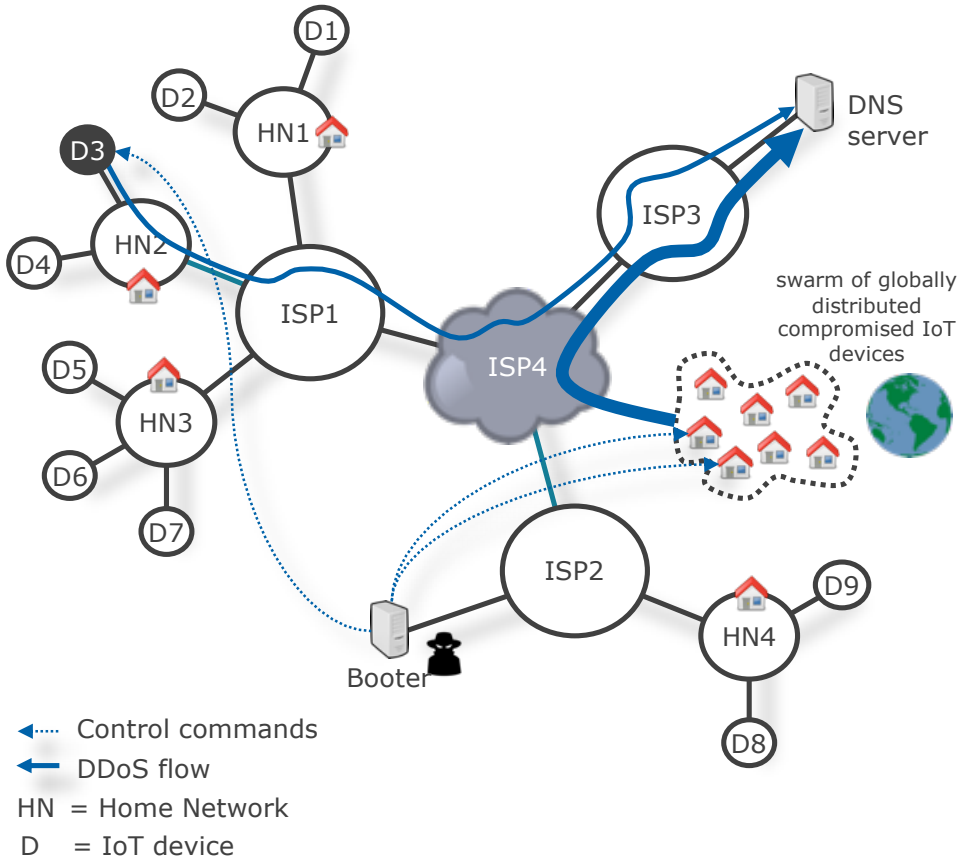
UNIVERSITY OF TWENTE.

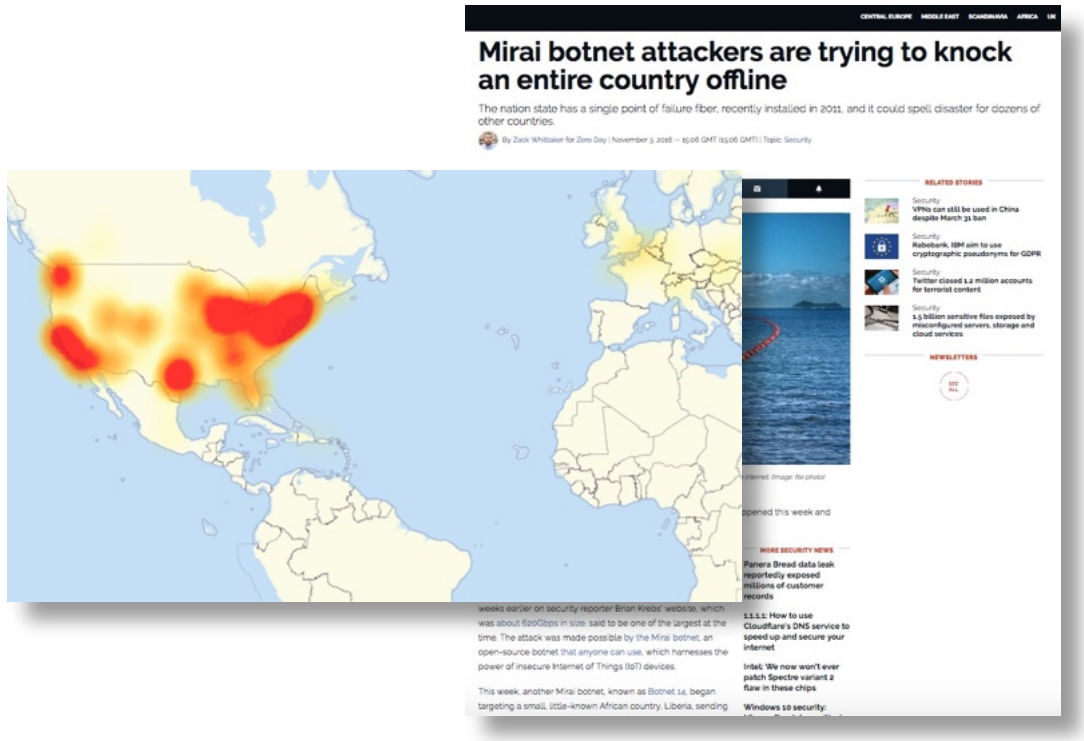
SDN LABS

“The Internet of Insecure Things”



IoT wakeup call: Mirai-powered DDoS attacks (2016)





Other targets: OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

Further reading: [Mirai], [Hajime], [DNSIoT]

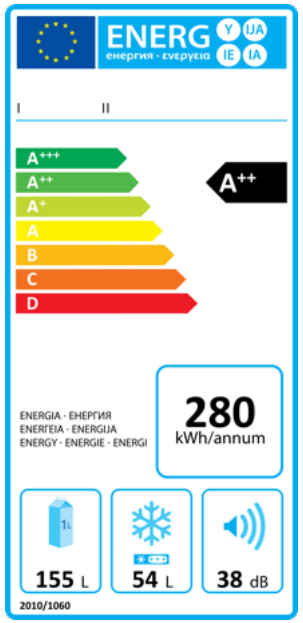
UNIVERSITY OF TWENTE.

SIDN LABS

Key challenges

- **Topline:** enable safer, smarter, and more sustainable society through the IoT, **while** protecting the Internet and its users (at home and elsewhere)

- Specific challenges, such as
  - Deployment of IoT security solutions
  - Interoperability between IoT devices and security services
  - More transparent IoT (data autonomy)
  - Continuous measurements and analysis of the IoT
  - Explainable security, legal and regulatory (e.g., a cybersecurity label)



- We'll be discussing papers that address these issues

UNIVERSITY OF TWENTE.

SDN LABS

Course overview

Learning goals

- Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF

- Be able to analyze network traffic of IoT devices and create device profiles that describe this behavior

- Understand the operational business of DNS operators and the impact the IoT may have on them (industry perspective)

SSI is an 'overview' course

UNIVERSITY OF TWENTE.

SIDN LABS

Assessment

- Goal: evaluate to what extent you attained SSI's learning goals

- Total score = [(score of oral exam) × 50% + (score of the lab assignment) × 50%] × (all paper summaries submitted 0=no or 1=yes)

- Deliverables
  - 12 **summaries** of papers (2 per lecture) => your input for oral exam
  - A five-page report on your **lab assignment**

Make sure to **browse** a few of the SSI papers this week to verify that SSI matches your interests, study plan, prerequisites, etc.

Deliverable #1: 12 paper summaries

- One summary for each of the papers we'll discuss during the lectures
- 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
- Due **before 7AM** on the **day of the lecture** in which the papers will be discussed

- Submit through Canvas

UNIVERSITY OF TWENTE. SDN LABS

Deliverable #2: lab report

Group-based project:
a measurement-based study

Group signups open later today

Firm deadline: **Friday 23 June 2023, 23:59 CEST**

UNIVERSITY OF TWENTE.

SDN LABS

Deliverable #2: measurement-based lab report

- Outcome of your lab assignment (see next slide)
- Discuss results of your measurements of **2+ IoT devices**, analysis and observations
- Your proposal on novel usages of MUD or extensions of MUD profiles
- Five-page lab report in two-column IEEE format, MUD spec, PCAP file, README file
- Evaluation: introduction, methodology, results, discussion, clarity (detail on SSI homepage)

Lab experiment

- Measure network traffic of **2+** IoT devices in groups of **three**, **one** report per team
- Use IoT devices **without a browser-like interface**
- Examples: camera, audio speaker, light bulb, thermostat, doorbell
- We have a couple of devices if you really can't find an IoT device
- Do not use multi-purpose devices like tablets, phones, laptops
- Use WireShark, TCPdump, or (for example) a SPIN device.
- Etienne & Ting-Han available for assistance

UNIVERSITY OF TWENTE.

SDN LABS

Writing your lab report

- **Group effort:** write together, everybody is equally responsible for the final report
- How to write a paper (30 mins): https://www.youtube.com/watch?v=5zthkvzyTfk
- We **evaluate** your report in a **double-blind** way, similar to how many academic conferences review papers (details on the SSI site)
- Examples of reviewers' questions:
  - What are their key findings? Did they sufficiently discuss background and cite papers?
  - Would I be able to **reproduce** their experiments based on their methodology?
  - How well did they analyze their measurements? To what extent did they explain the limitations of their methodology?

Lab groups: selection & management

Form groups with members having **similar skills/background**.

We suggest making a **brief summary** of each group meeting:

- Who attended?
- Key action points?
- Who is reponsible for each task?

Submit draft lab report three weeks before deadline, avoid last-minute rushing.

UNIVERSITY OF TWENTE.

SIDN LABS

Best paper award

UNIVERSITY OF TWENTE.
SIDN LABS

Plagiarism

- As per the university's policy, no forms of plagiarism are tolerated

- We configured Canvas such that it will automatically check your report for plagiarism

Style		Example
Citing	✓	In our lab experiment, we use Manufacturer Usage Descriptions (MUDs) [RFC8250] to describe the network behavior of IoT devices.
Quoting	✓	MUD was designed to "provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function" [RFC8250]
Copying	✗	MUD was designed to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function [RFC8250]

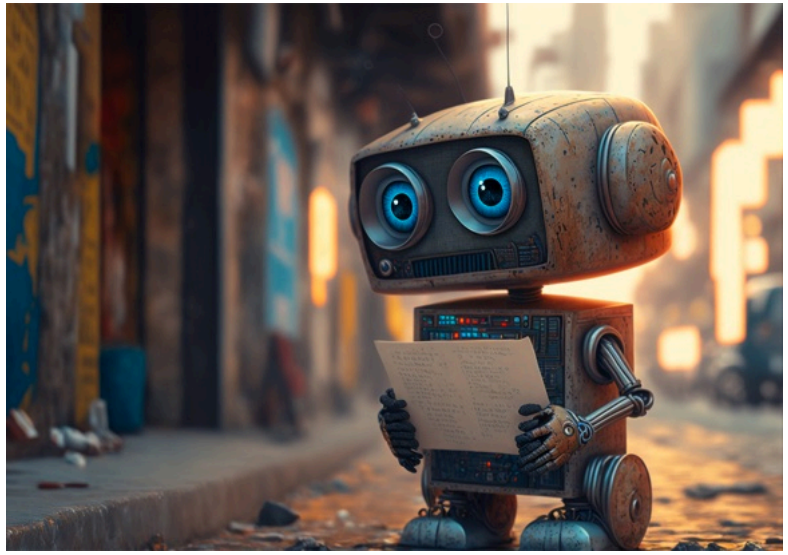
- Also cite and quote sources where you are a co-author

Oral exam

- Q&A with an SSI teacher and a teaching assistant
- Covers the 12 papers you studied; you may use the summaries you wrote
- Takes about 45 minutes and will take place from June 21 through July 6
- You can pick a timeslot in the weeks before the oral exams
- The oral exams will take place on campus, room to be announced.

LLM's (ChatGPT)

- In the oral exams, we will spend up to 10 min on the Lab report (e.g., methodology).



- In Lab report, in the 'who-did-what'-section, acknowledge any external help.

- Q: How would you use LLM's for a course?
- Q: How do you expect to use LLM's in your future working life?

Important dates

- Two summaries per lecture: before the lecture (07:00) in which the papers will be discussed
- Lab report (PDF) and required files: **Fri 23 June 2023, 23:59 CEST**
- All to be submitted through CANVAS

UNIVERSITY OF TWENTE.

SDN LABS

Lectures

- Two **guest lectures** to provide you with non-academic perspectives

- Six **technical lectures**:
  - Teachers discuss two papers per lecture
  - Interactive discussion
  - We ask at least one of you to share their thoughts on each paper (pros, cons)
  - 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

Schedule

No.	Date	Contents
1	Apr 26	Course introduction
2	May 3	Lecture: IoT and Internet Core Protocols
3	May 10	Lecture: IoT Botnet Measurements 1
4	May 17	Lecture: IoT Edge Security Systems
5	???	Guest lecture #1: t.b.d
6	May 24	Lecture: IoT Device Security
7	May 31	Lecture: IoT Botnet Measurements 2
8	Jun 7	Lecture: IoT Security in Non-Carpeted Areas
9	???	Guest lecture #2: t.b.d
10	Jun 14	Lecture: IoT Honeypots (re-sit)

Staying up to date

- SSI homepage at https://courses.sidnlabs.nl/ssi
- Authoritative source for information about SSI
- Recommend visiting it every now and then

UNIVERSITY OF TWENTE.

SIDN LABS

Common pitfalls

- Forgetting to submit summaries or submitting the wrong ones ;-)

- Starting too late with the lab report

> *"I love deadlines. I love the whooshing noise they make as they go by."*
>
> *-- Douglas Adams*

- Properly test your measurement setup. Consider reproducibility early on.

- "Oh, I just copy this paragraph from this website"

Changes from last year's edition

Based on the student feedback we received last year

- Removed design-based lab assignment
- Replaced 2 papers
- Included project management tips
- Clarified lecture topics and why papers are selected

SSI fact sheet

Security Services for the IoT (SSI)	
EC	5 (140 hours)
Coordinator	Cristian Hesselman (SIDN Labs, University of Twente)
E-mail	c.e.w.hesselman@utwente.nl
Lecturers	prof.dr. Cristian Hesselman (SIDN Labs; University of Twente) dr. Elmer Lastdrager (SIDN Labs)
Teaching Assistents	Ramin Yazdani (University of Twente) Etienne Khan (University of Twente) Ting-Han Chen (University of Twente)
Fourth quartile	April 24 – July 7, 2023
Academic year	2022/2023

UNIVERSITY OF TWENTE.

SIDN LABS

Poll: who are you?

1. Which study program are you following?
2. What made you feel interested in this course?
3. Who knows what anycast is? Or BGP? Or IPv6?

SIDN Labs?

UNIVERSITY OF TWENTE.

SIDN LABS

SIDN is the operator of the .nl TLD

- Objective: increase society's confidence in the Internet

- Provide secure and fault-tolerant registry services for .nl
  - Anycasted DNS services with DNSSEC support
  - Registration and domain protection services

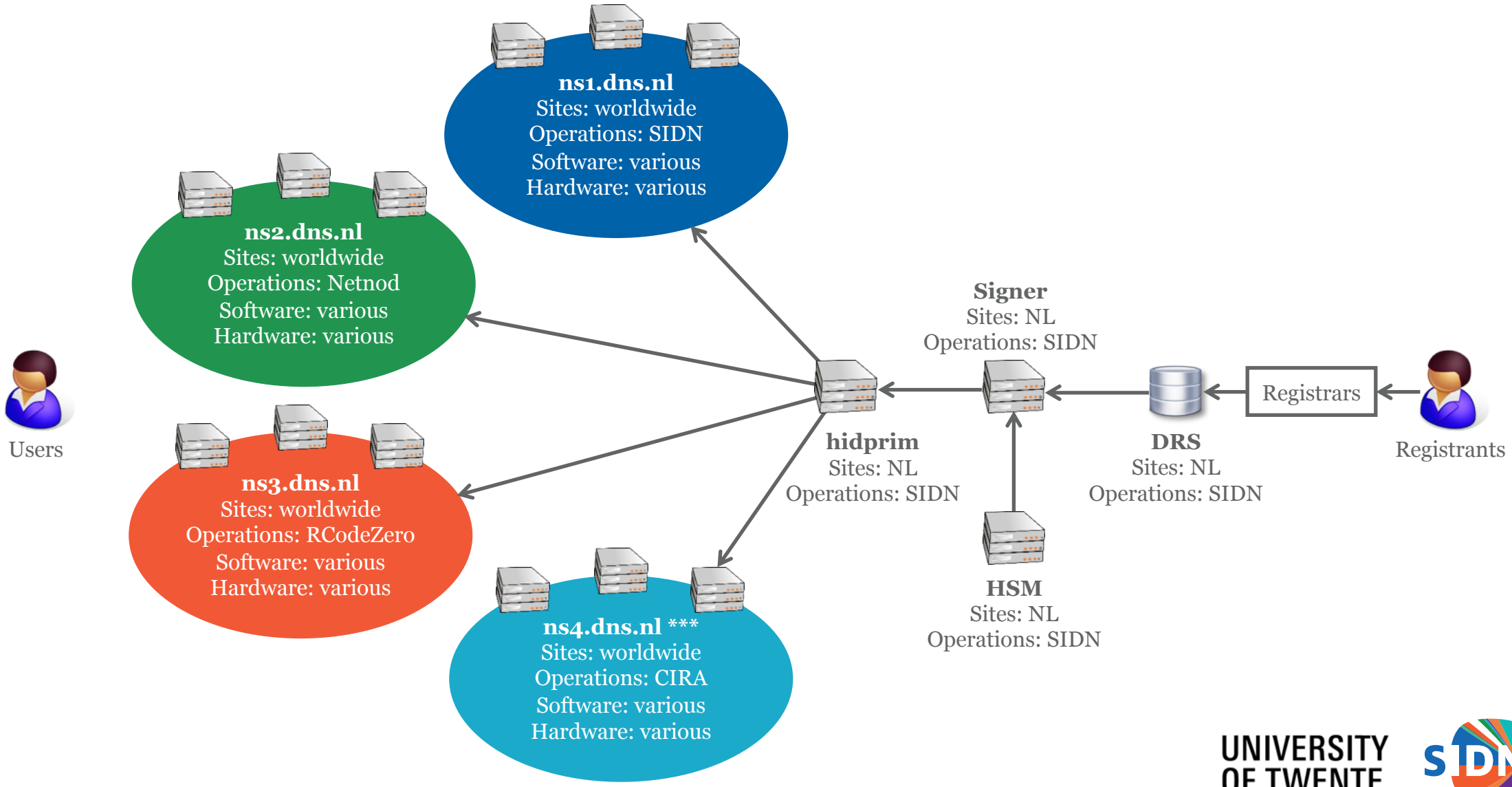
- Increase the value of the Internet in the Netherlands and elsewhere
  - Enable safe and novel uses (SIDN Fonds, IRMA)
  - Increase security and trustworthiness of the infrastructure (SIDN Labs)

- Not-for-profit organization of ~100 FTE, based in Arnhem

.nl = the Netherlands
17M inhabitants
6.3M domain names
3.6M DNSSEC-signed
2.5B DNS queries/day
8.6B NTP queries/day

UNIVERSITY OF TWENTE.
SIDN LABS

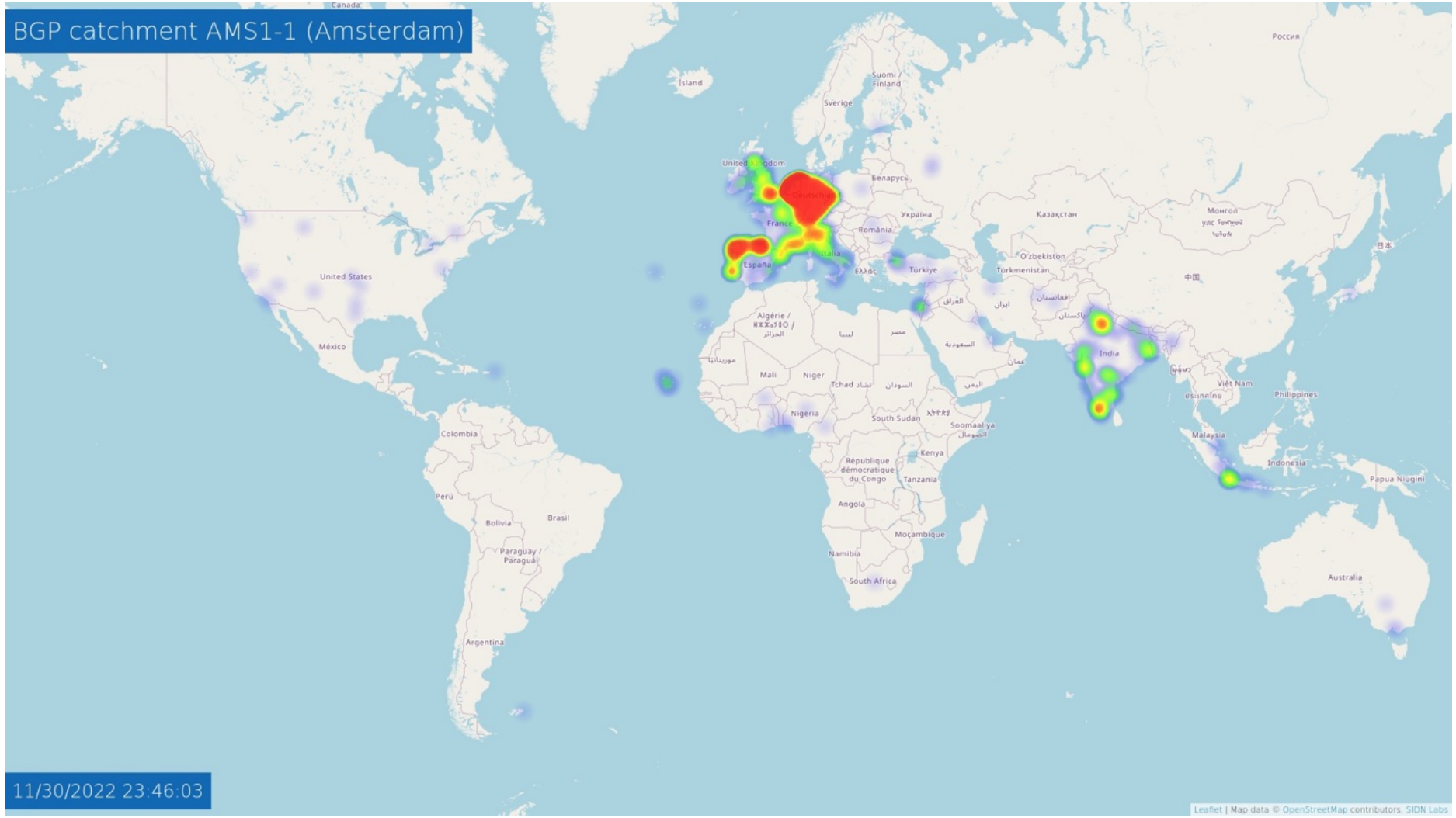
Heterogeneous and fault-tolerant DNS infrastructure



UNIVERSITY OF TWENTE.

SIDN LABS

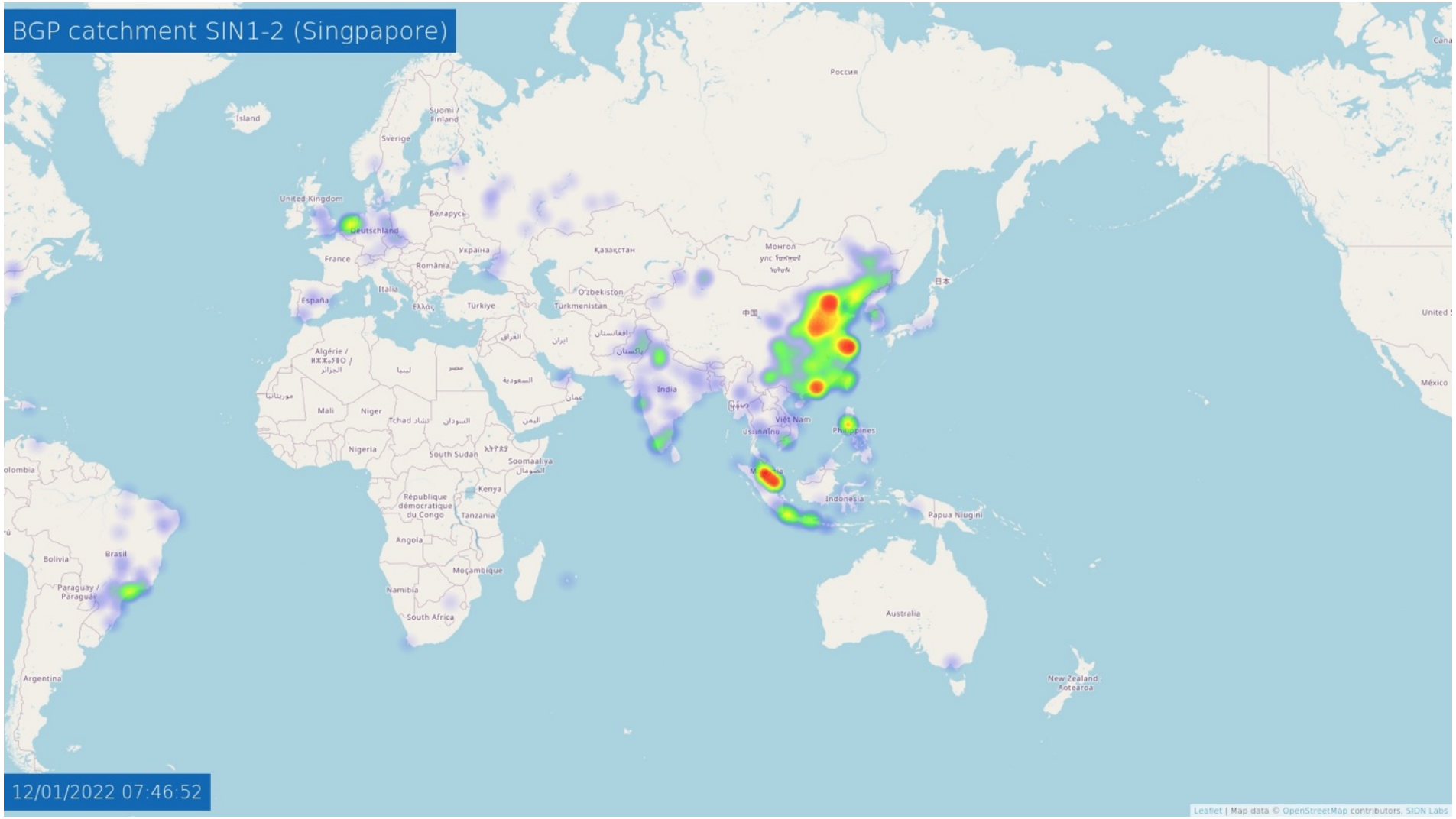
Anycast infrastructure (1)



UNIVERSITY OF TWENTE.

SIDN LABS

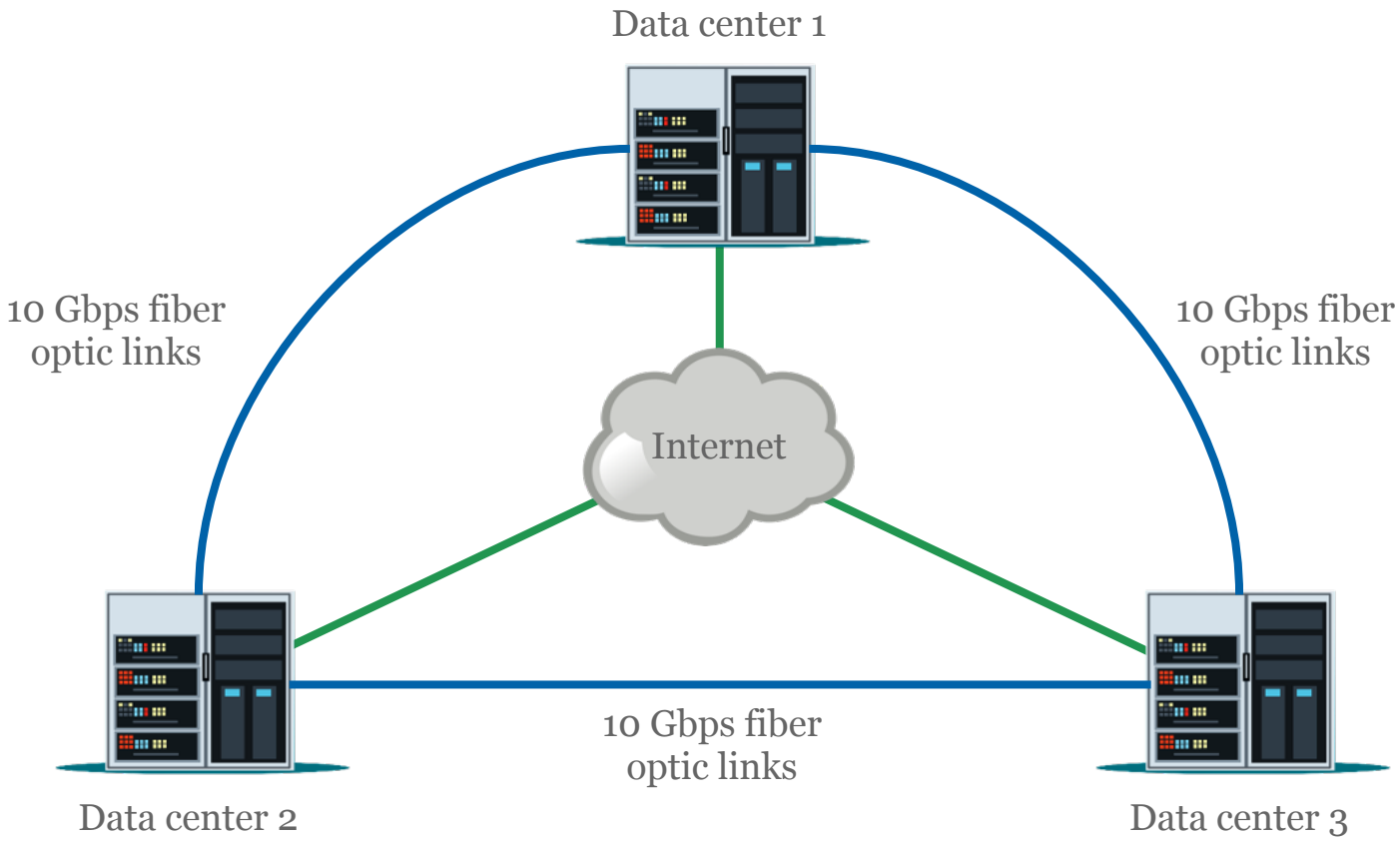
Anycast infrastructure (2)



UNIVERSITY OF TWENTE.

SIDN LABS

Registration infrastructure (DRS, RDAP, WHOIS, …)



99.96% availability
Full-automatic failover

UNIVERSITY OF TWENTE.

SDN LABS

Other security areas

- System monitoring and patching (with NCSC-NL and others)
- Secure software development
- Infrastructure penetration testing
- Large-scale and collaborative DDoS mitigation drills (Dutch Anti-DDoS Coalition)
- Security Operations Center (ISO 27001)
- Proactive and collaborative abuse mitigation (phishing, malware, fake shops, etc.)

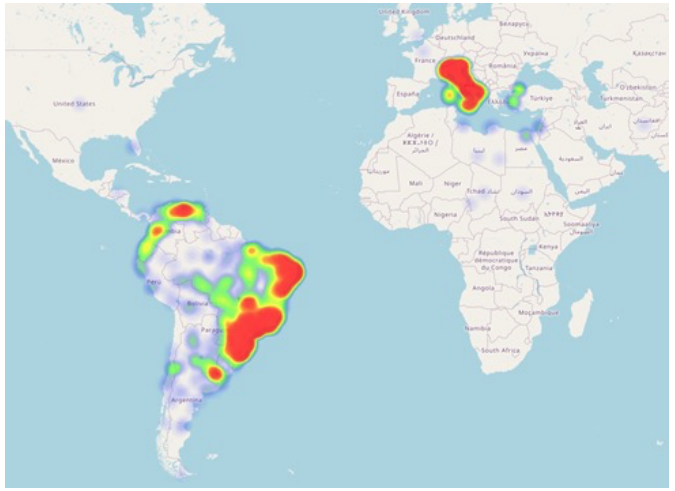
UNIVERSITY OF TWENTE.

SIDN LABS

A more flexible DNS infrastructure (in progress)

- Virtual machines at cloud providers
- Vultr, Packet (Equinix), Heficed
- Control over VMs and operating systems
- Complements “as a service” and owned infra
- BIRD-based BGP sessions to cloud providers
  - Path pre-pending
  - BGP communities

Anycast2020 sites



BGP tuning based on catchments

UNIVERSITY OF TWENTE.

SIDN LABS

SIDN Labs = research team

- Goal: increase trustworthiness (security, stability, resilience, and transparency) of our society's internet infrastructure, for .nl and the Netherlands in particular.

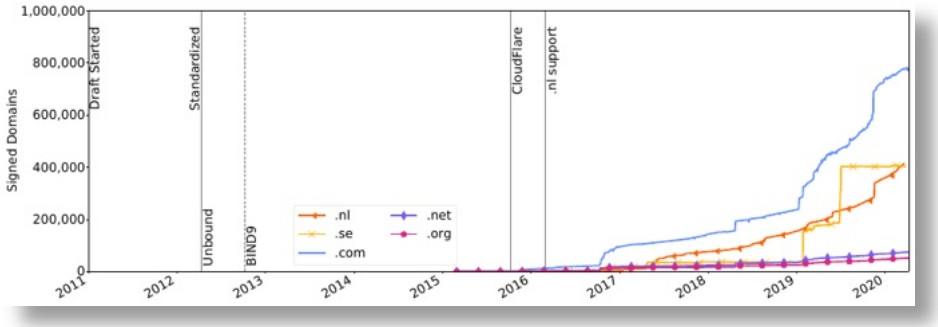
- Strategies:
  - Applied technical research (measurements, design, prototyping, evaluation)
  - Make results publicly available and useful for various target groups
  - Work with universities, infrastructure operators, and other labs

- Three research areas: network security (DNS, NTP, BGP), domain name & IoT security, trusted future internet infrastructures.

UNIVERSITY OF TWENTE.

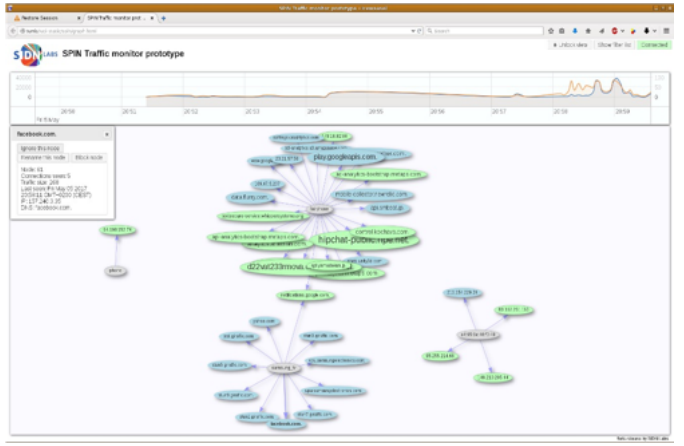
SIDN LABS

Example projects

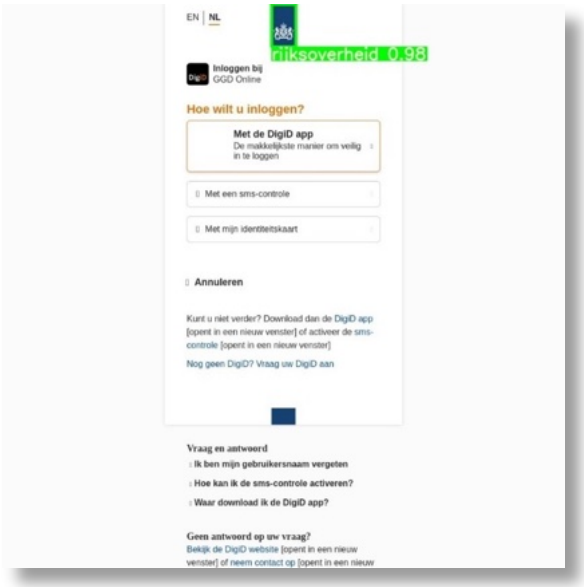


Measuring the deployment of newly standardized DNSSEC algorithms

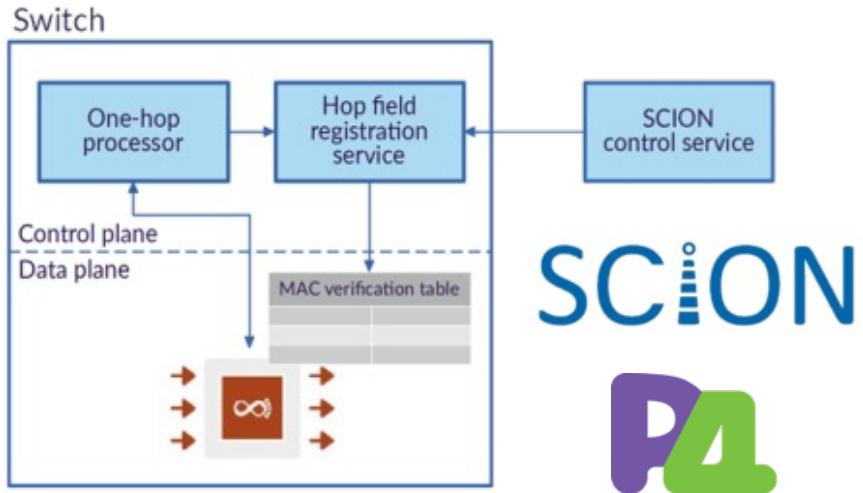
Provide well-managed and secure time services



Making the IoT more secure and transparent and measure its evolution



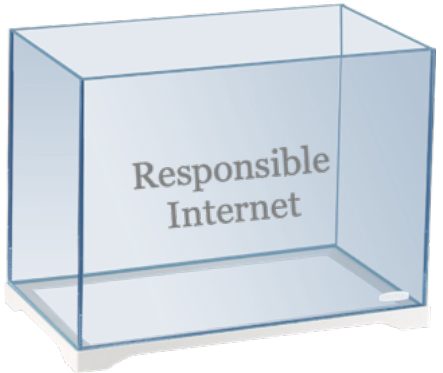
Logo detection technology to identify malicious .nl websites



SCION

P4

Experimenting with secure future networks and programmable networks



2STiC

NWO

€1.9M

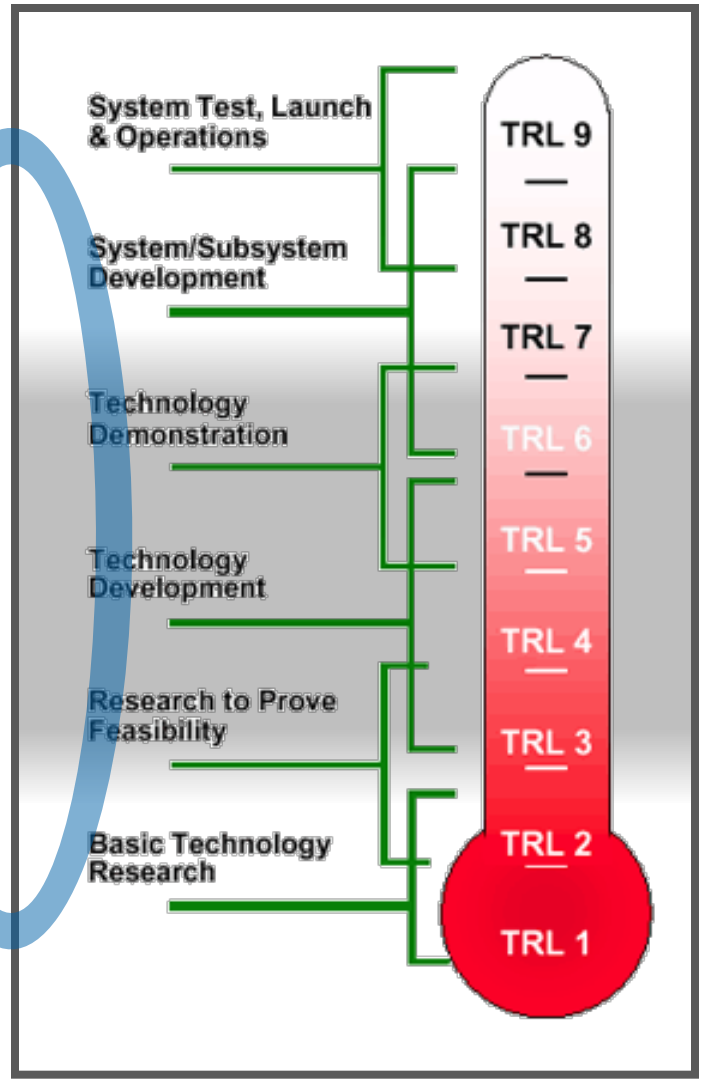
Developing a new Internet security and autonomy paradigm

UNIVERSITY OF TWENTE.

SIDN LABS

SIDN Labs and Technology Readiness Levels

SIDN Labs focuses on the **R** in R&D



Operations

Experimental

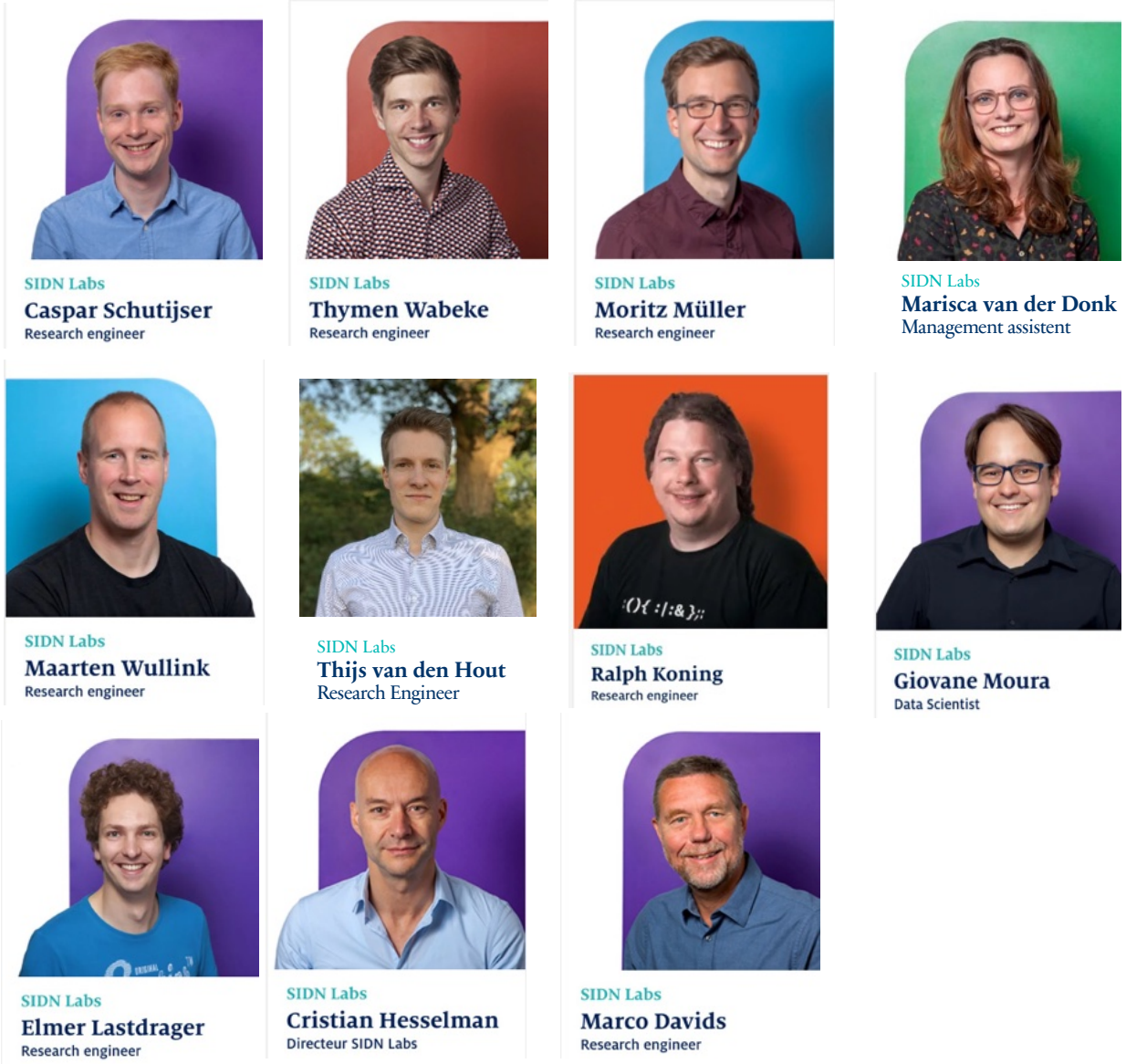
Fundamental research

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

O'Reilly, C. A., & Tushman, M. L. (2013). Organizational ambidexterity: Past, present, and future. Academy of Management Perspectives, 27(4), 324-338

Examples of our research partners

SIDN Labs team



- Technical experts, divers in seniority and nationality
- Help SIDN teams, write open-source software, analyze large amounts of data, conduct experiments, write articles, collaborate with universities
- M.Sc students help us advance specific areas

UNIVERSITY OF TWENTE.

SIDN LABS

SSI is a collaborative course

- Motivation for SIDN Labs
  - Help educating the next generation of Internet security engineers and researchers
  - Highlight societal impact of the Internet (e.g., concentration, interaction w/ physical world)
  - Aligns with our work on IoT security (SPIN project, RAPID project, and others)
  - Perhaps interest some of you to check out our work for an M.Sc. Project :-)

- Extends ongoing academic-industry research collaboration
  - SIDN Labs: improve security and resilience of SIDN's services and wider Internet using university's latest academic insights, methodologies, network, and creative thinking
  - University: further improved research and education using SIDN's operational experience, unique datasets, and industry network

UNIVERSITY OF TWENTE.

SIDN LABS

Volg ons

SIDN.nl

@SIDN

SIDN

Q&A

Next lecture: **Wed May 3, 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