Security Services for the IoT: Introduction

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

UNIVERSITY OF TWENTE.

SIDN LABS

Teaching team

Cristian Hesselman
(teacher)

Elmer Lastdrager
(teacher)

Ramin Yazdani
(teaching assistant)

Etienne Khan
(teaching assistant)

UNIVERSITY OF TWENTE.

SIDN LABS

Online house rules

- Mute your mic!
- Put a “?” in the chat if you’d like to ask a question and we’ll give you the floor (*or write your question directly in the chat*)
- Unmute your mic (and optionally turn on your cam) if you want to speak :-)
- Roles: chair (Cristian), moderator (Elmer), attendees (you guys)

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

- Five-slide high-level introduction to IoT security
- Course overview
- (Brief introduction of SIDN Labs)
- Guest lecture by Marco Davids (SIDN Labs) on “How the core of the Internet is organized”

Security issues in the IoT?

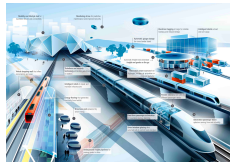
UNIVERSITY OF TWENTE.

SDN LABS

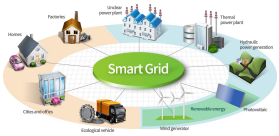
Internet of Things (IoT)

- 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



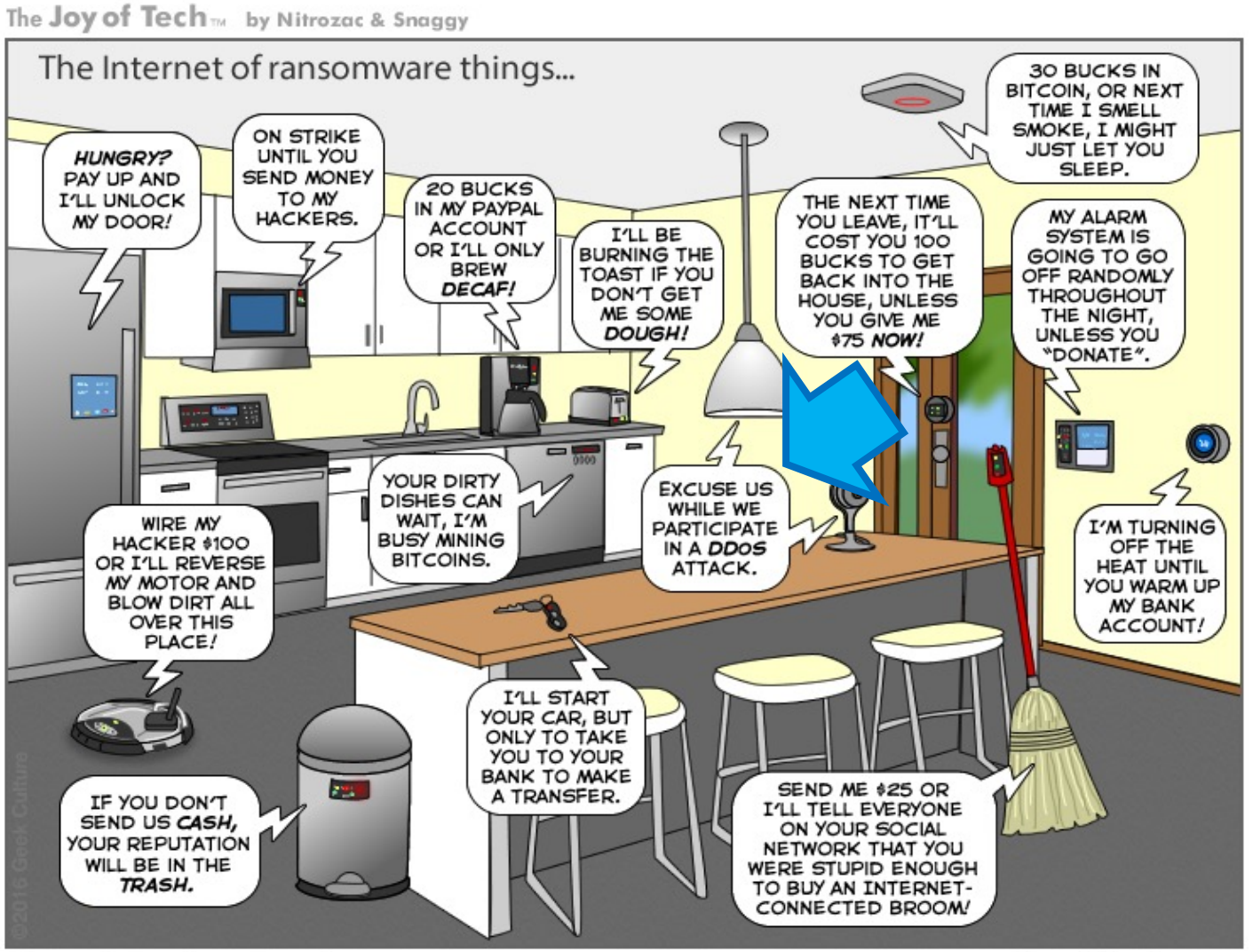
Smart energy grids

Smart homes and cities

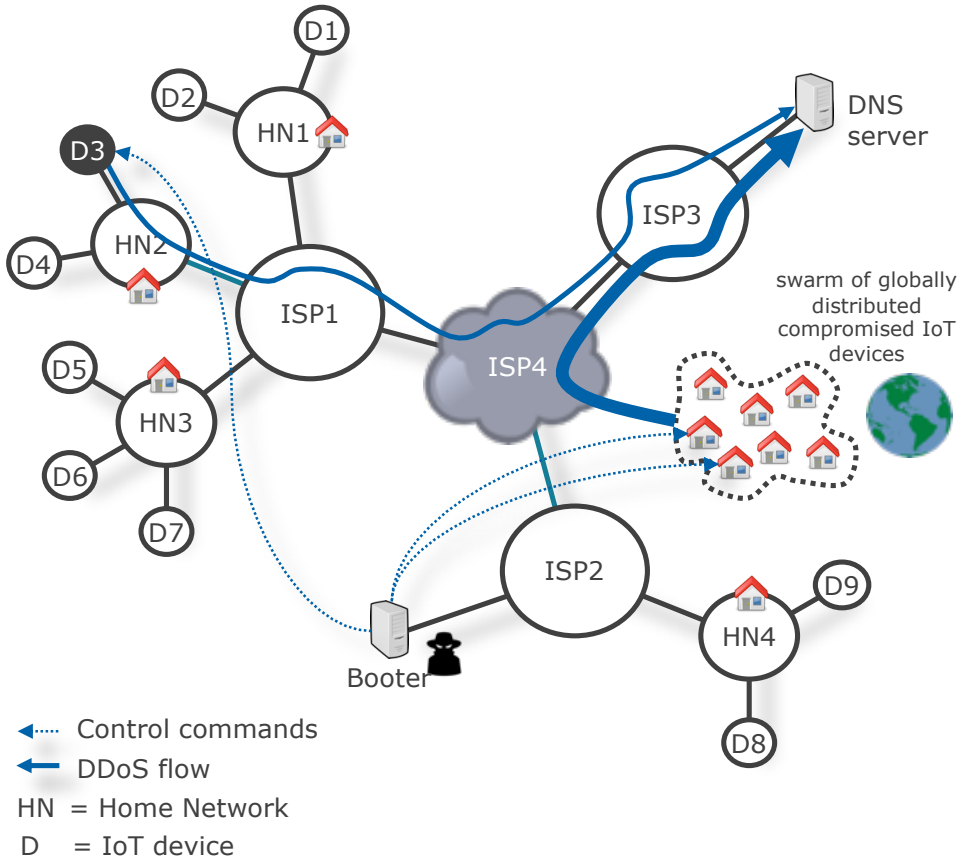
- Promises safer, smarter, more sustainable society, **but IoT security is a major challenge**

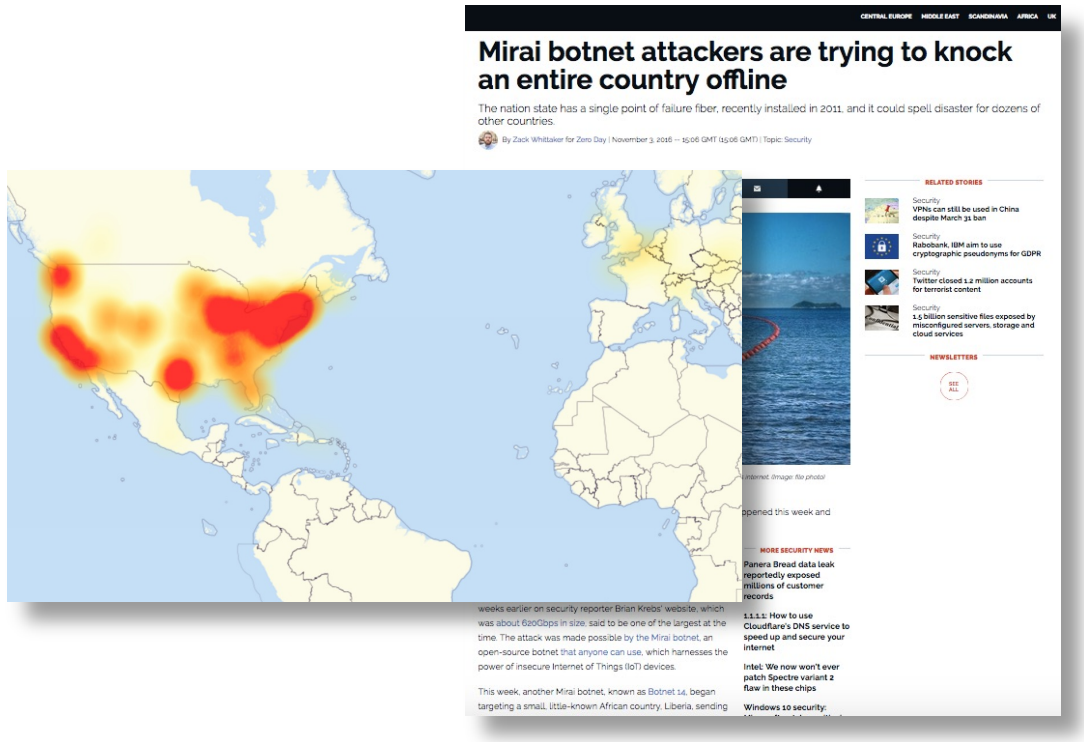
Further reading: [WEIS] [DNSIoT]

“The Internet of Insure Things”



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





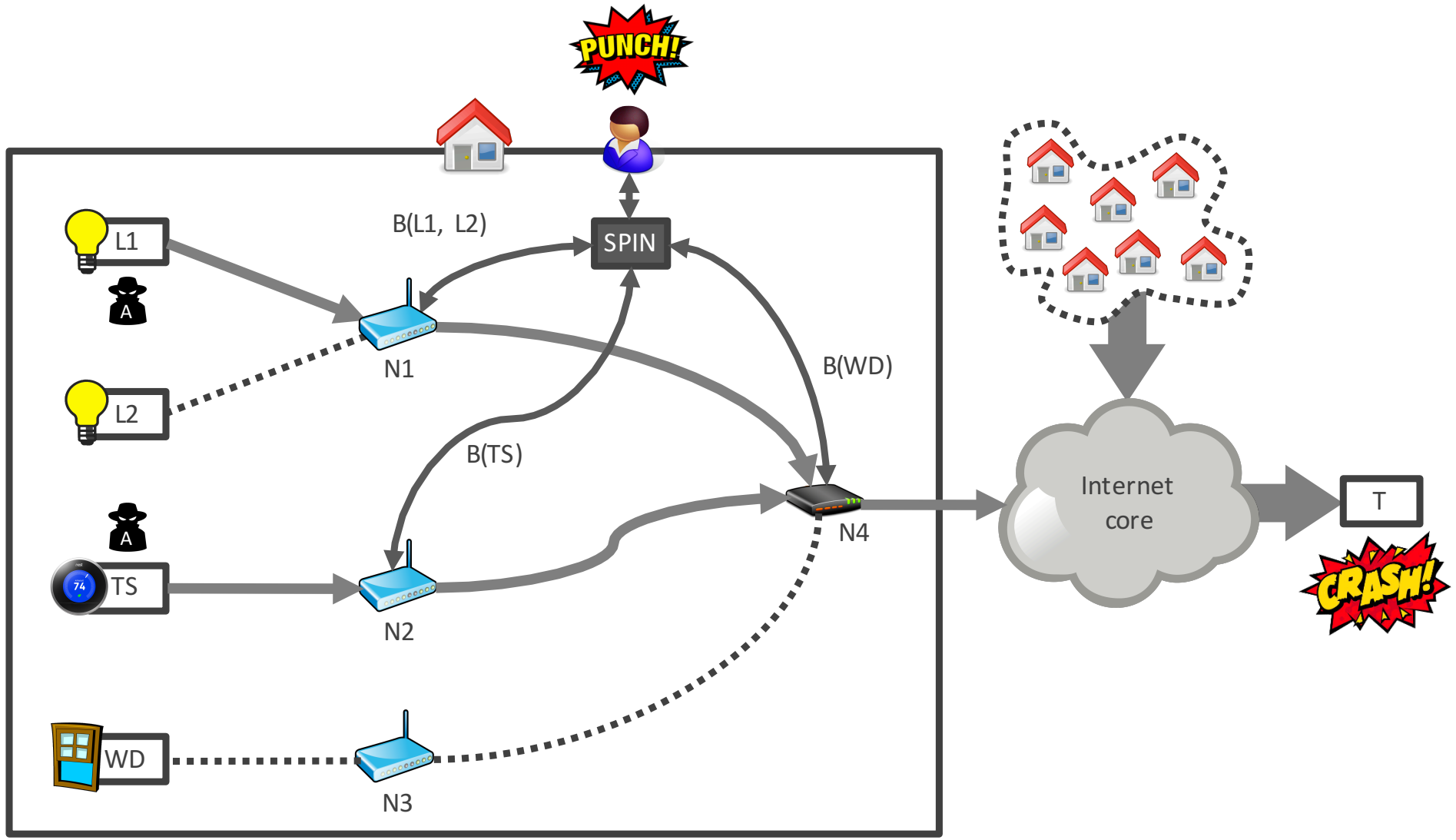
Other targets: OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

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

UNIVERSITY OF TWENTE.

SDN LABS

Example of an IoT security system: SPIN



Further reading: [NOMS] and https://spin.sidnlabs.nl/en/

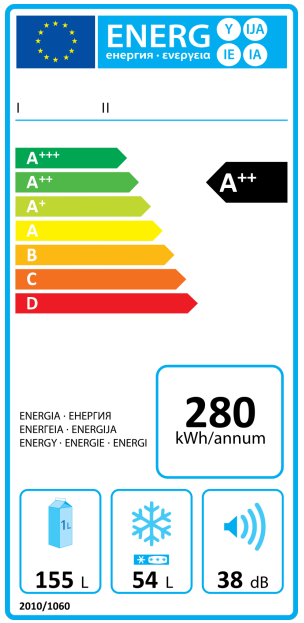
UNIVERSITY OF TWENTE.

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)

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

- 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)
- Firm deadline: **Sunday June 20, 2021, 23:59 CEST**

Lab experiment

- Measure network traffic of **2+** IoT devices in groups of **two or 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 Khan 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?

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 2
- You can pick a timeslot in the week before the oral exams
- We'll take your oral exam through a video call using Canvas (instructions on the SSI site)

Important dates

- Two summaries per lecture: before the lecture in which the papers will be discussed
- Lab report (PDF) and required files: **Sun June 20, 2021, 23:59 CEST**
- All to be submitted through CANVAS

Lectures

- Three **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 21	Course introduction Guest lecture #1: how the core of the internet is organized, Marco Davids (SIDN Labs)
2	Apr 28	Guest lecture #2: the relationship between regulation & IoT security, Eelco Vriezekolk, Agentschap Telecom (Dutch telecoms regulator)
3	May 6*	Lecture: IoT Concepts and Applications
4	May 12	Lecture: IoT Botnet Measurements
5	May 18	Lecture: IoT Honeypots
6	May 25*	Guest lecture #3: The Life Of An IoT Device, Eliot Lear, Cisco Systems
7	May 26	Lecture: IoT Edge Security Systems
8	Jun 2	Lecture: IoT Device Behavior
9	Jun 9	Lecture: IoT in Non-Carpeted Areas
10	Jun 16	Lecture: IoT Edge Security Systems (re-sit)

* Different lecture times/days. Default slot: Wednesdays 11:00 - 12:45

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 reproducability early on.

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

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	dr. Elmer Lastdrager (SIDN Labs) dr. Cristian Hesselman (SIDN Labs)
Fourth quartile	April 19 – July 4, 2021
Academic year	2020/2021

UNIVERSITY OF TWENTE.

SIDN LABS

SIDN Labs?

UNIVERSITY OF TWENTE.

SIDN LABS

Operator of the .nl TLD

- *Stichting Internet Domeinregistratie Nederland* (SIDN)

- Critical infrastructure services
  - Lookup IP address of a domain name (almost every interaction)
  - Registration of all .nl domain names
  - Manage fault-tolerant and distributed infrastructure

- Increase the value of the Internet in the Netherlands and elsewhere
  - Enable safe and novel use of the Internet
  - Improve the security and resilience of the Internet itself

.nl = the Netherlands
17M inhabitants
6.2M domain names
3.4M DNSSEC-signed
2.5B DNS queries/day
8.6B NTP queries/day

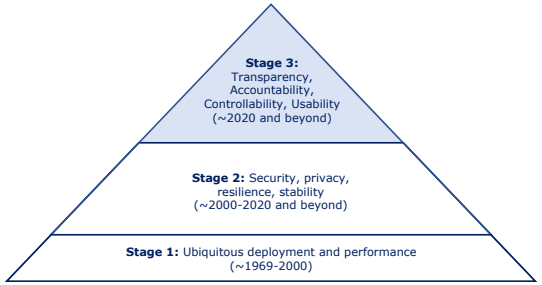
SIDNfonds

UNIVERSITY OF TWENTE.

SIDN LABS

SIDN Labs = research team

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



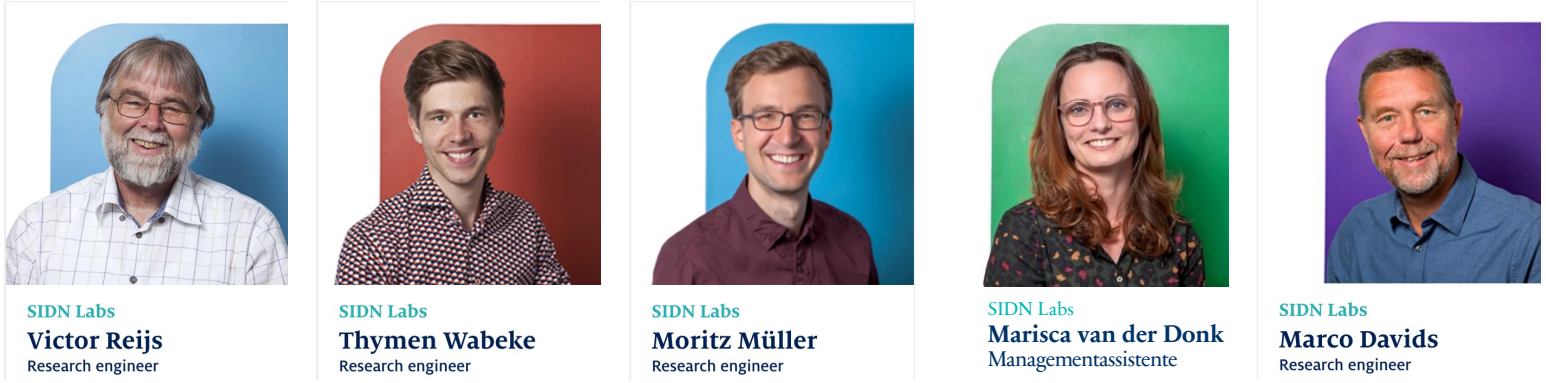
- Strategies:
  - Applied research (measurements, prototyping, evaluation)
  - Make results publicly available and useful for various target groups
  - Work with universities, infrastructure operators, and other labs

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

UNIVERSITY OF TWENTE.

SIDN LABS

SIDN Labs team



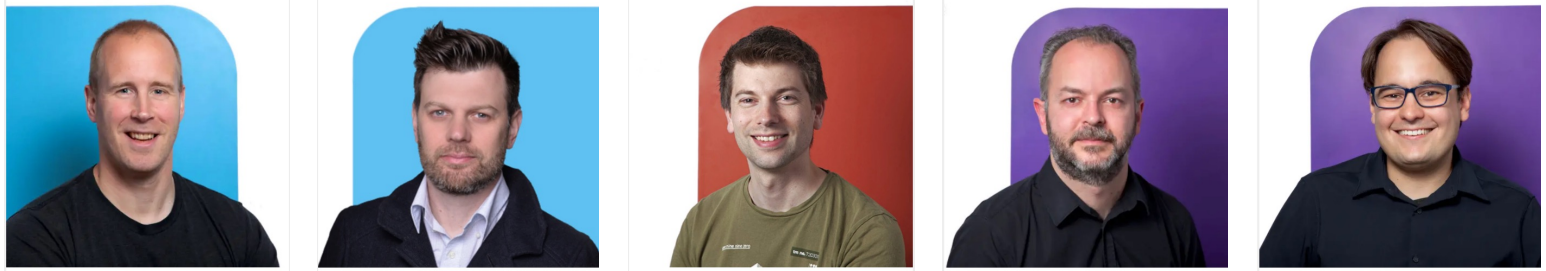
SIDN Labs
Victor Reijs
Research engineer

SIDN Labs
Thymen Wabeke
Research engineer

SIDN Labs
Moritz Müller
Research engineer

SIDN Labs
Marisca van der Donk
Managementassistente

SIDN Labs
Marco Davids
Research engineer



SIDN Labs
Maarten Wullink
Research engineer

SIDN Labs
João Ceron
Research engineer

SIDN Labs
Joeri de Ruiter
Research engineer

SIDN Labs
Jelte Jansen
Research engineer

SIDN Labs
Giovane Moura
Data Scientist

SIDN Labs
Elmer Lastdrager
Research engineer

SIDN Labs
Dennis Eijkel
Afstudeerder (UT)

SIDN Labs
Caspar Schutijser
Research engineer

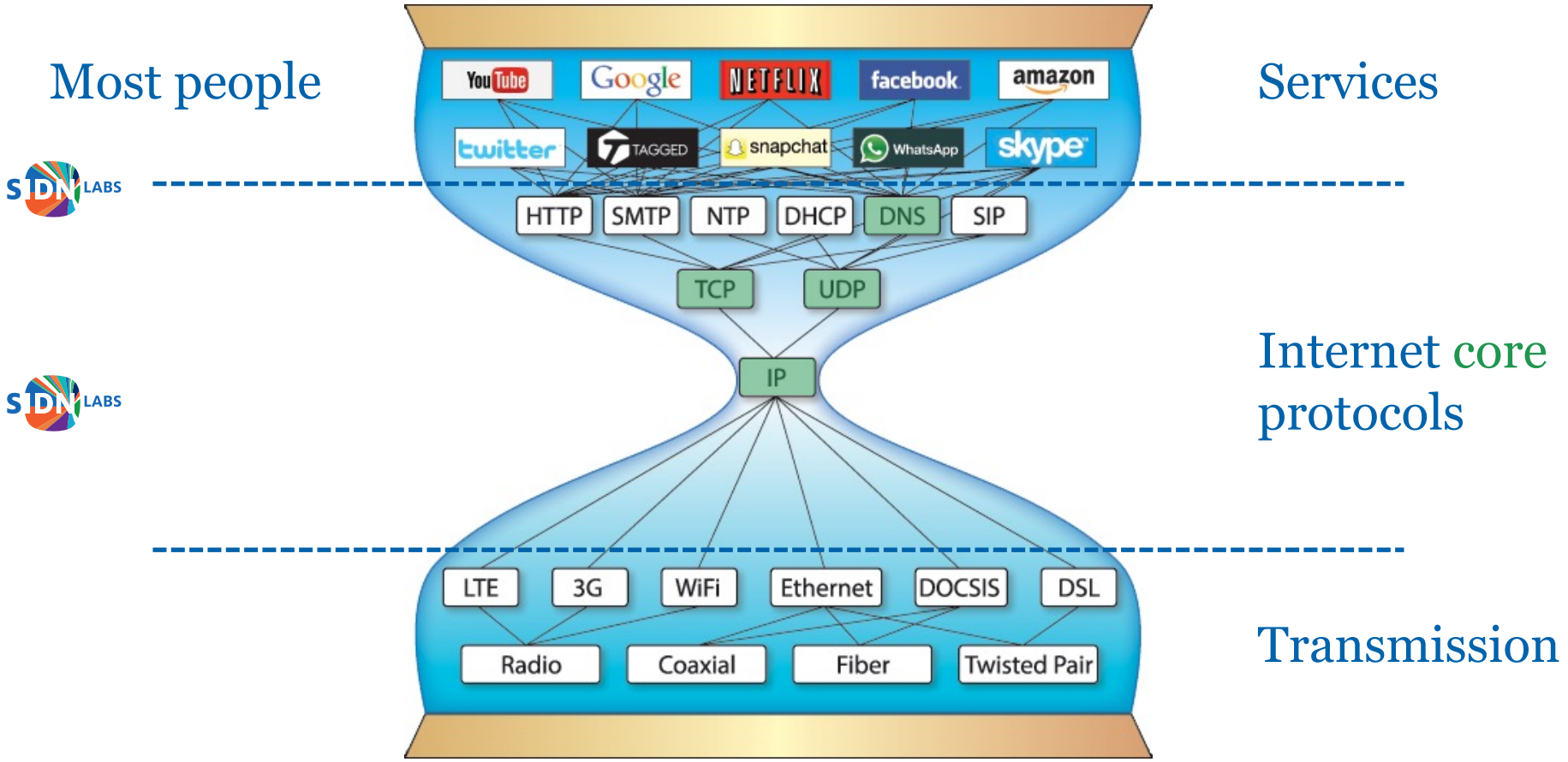
SIDN Labs
Cristian Hesselman
Directeur SIDN Labs

- 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.

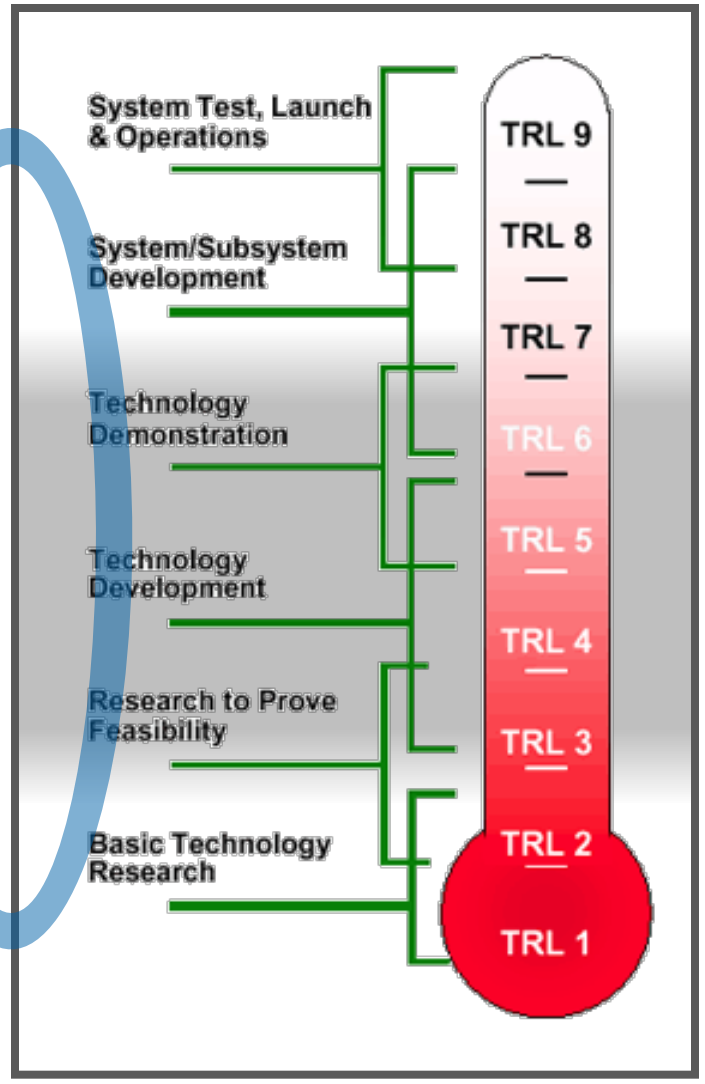
SIDN LABS

The Internet under the hood



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

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

Guest lecture

Marco Davids (SIDN Labs)

UNIVERSITY OF TWENTE.

SIDN LABS

Volg ons

.nl SIDN.nl

@SIDN

SIDN

Q&A

Next lecture: **Wed Apr 28, 11:00-12:45**

Cristian Hesselman
Director of SIDN Labs
+31 6 25 07 87 33
c.e.w.hesselman@utwente.nl
@hesselma

Elmer Lastdrager
Research Engineer
+31 6 12 47 84 88
elmer.lastdrager@sidn.nl
@ElmerLastdrager

UNIVERSITY OF TWENTE.

SIDN LABS