Security Services for the IoT: Introduction

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

University of Twente | April 22, 2020

UNIVERSITY OF TWENTE.

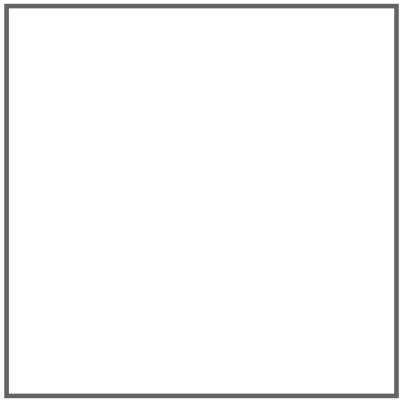
SIDN LABS

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 want to ask a question and we’ll give you the floor
- Unmute your mic (and optionally turn on your cam) if you want to speak :-)
- Roles: chair (Cristian), moderator (Elmer), attendees (you guys)

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

UNIVERSITY OF TWENTE. SIDN LABS

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”

UNIVERSITY OF TWENTE.

SIDN LABS

Security issues in the IoT?

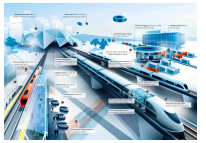
UNIVERSITY OF TWENTE.

SDN LABS

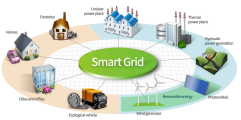
Internet of Things (IoT)

- 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

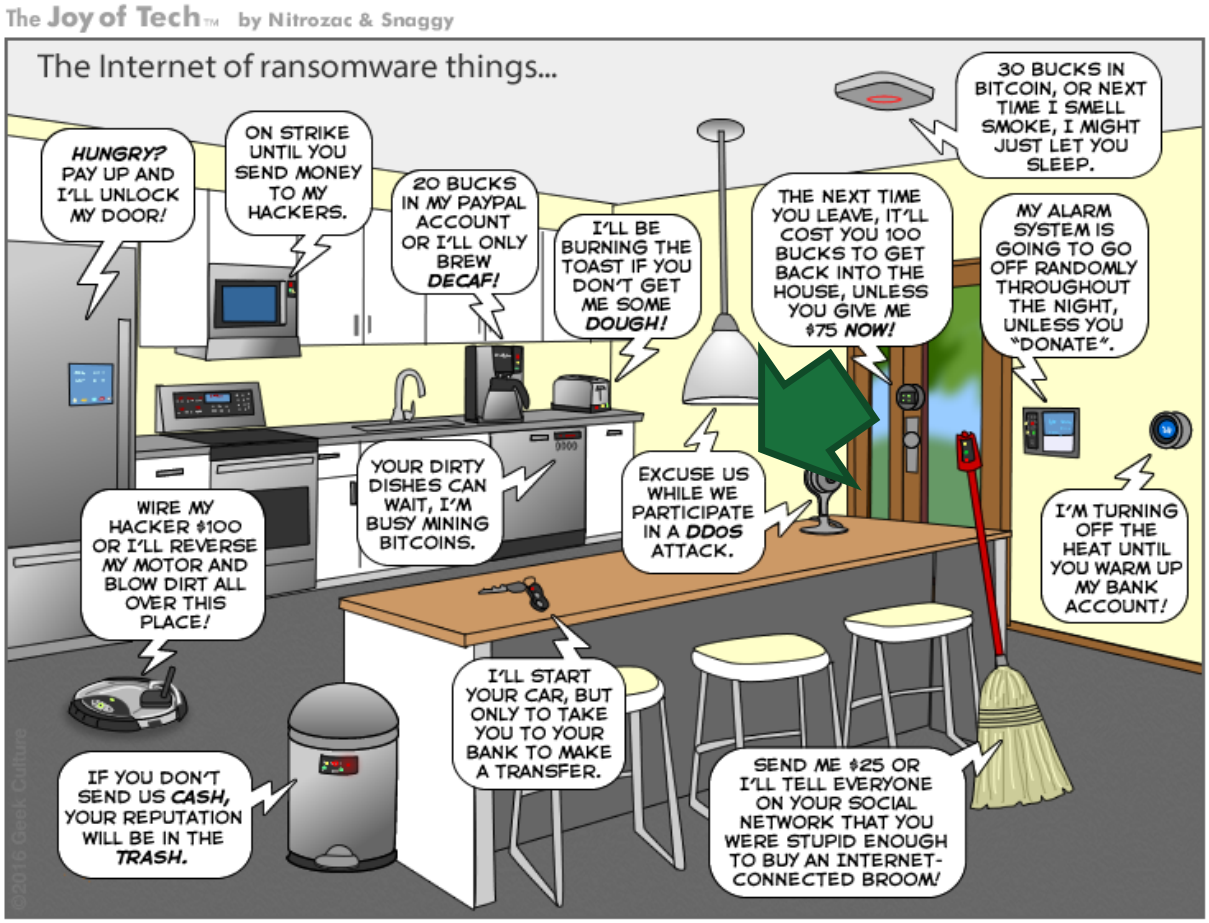
- IoT promises a safer, smarter, and more sustainable society, but IoT security is a major challenge

[SAC105] T. April, L. Chapin, kc claffy, C. Hesselman, M. Kaeo, J. Latour, D. McPherson, D. Piscitello, R. Rasmussen, and M. Seiden, “The DNS and the Internet of Things: Opportunities, Risks, and Challenges”, SSAC report SAC105, June 2019

UNIVERSITY OF TWENTE.

SIDN LABS

“Nightmare on connected home street”



MAT HONAN GEAR 06.13.14 06:30 AM

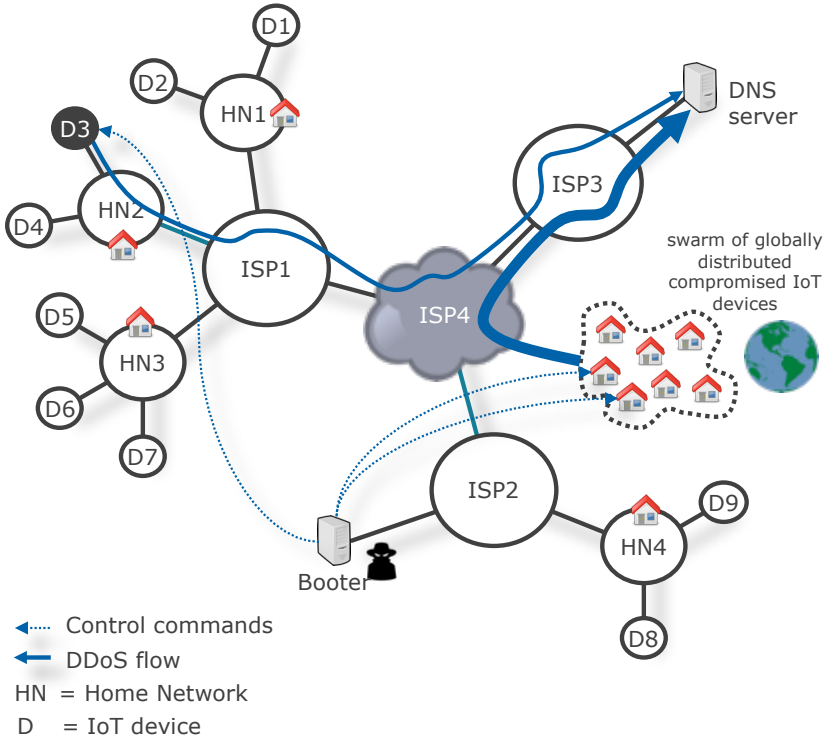
THE NIGHTMARE ON CONNECTED HOME STREET

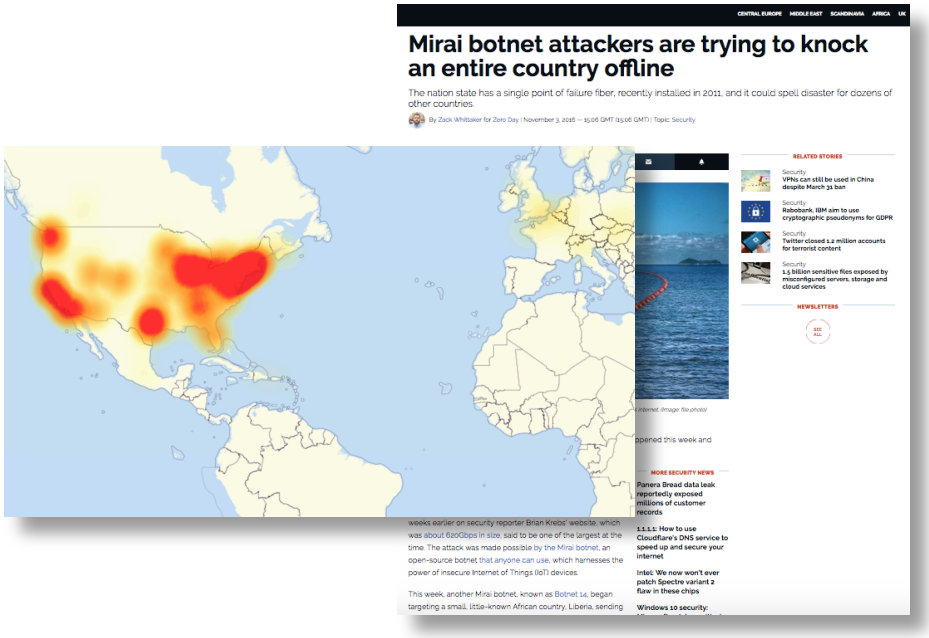
https://www.wired.com/2014/06/the-nightmare-on-connected-home-street/

UNIVERSITY OF TWENTE.

SDN LABS

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





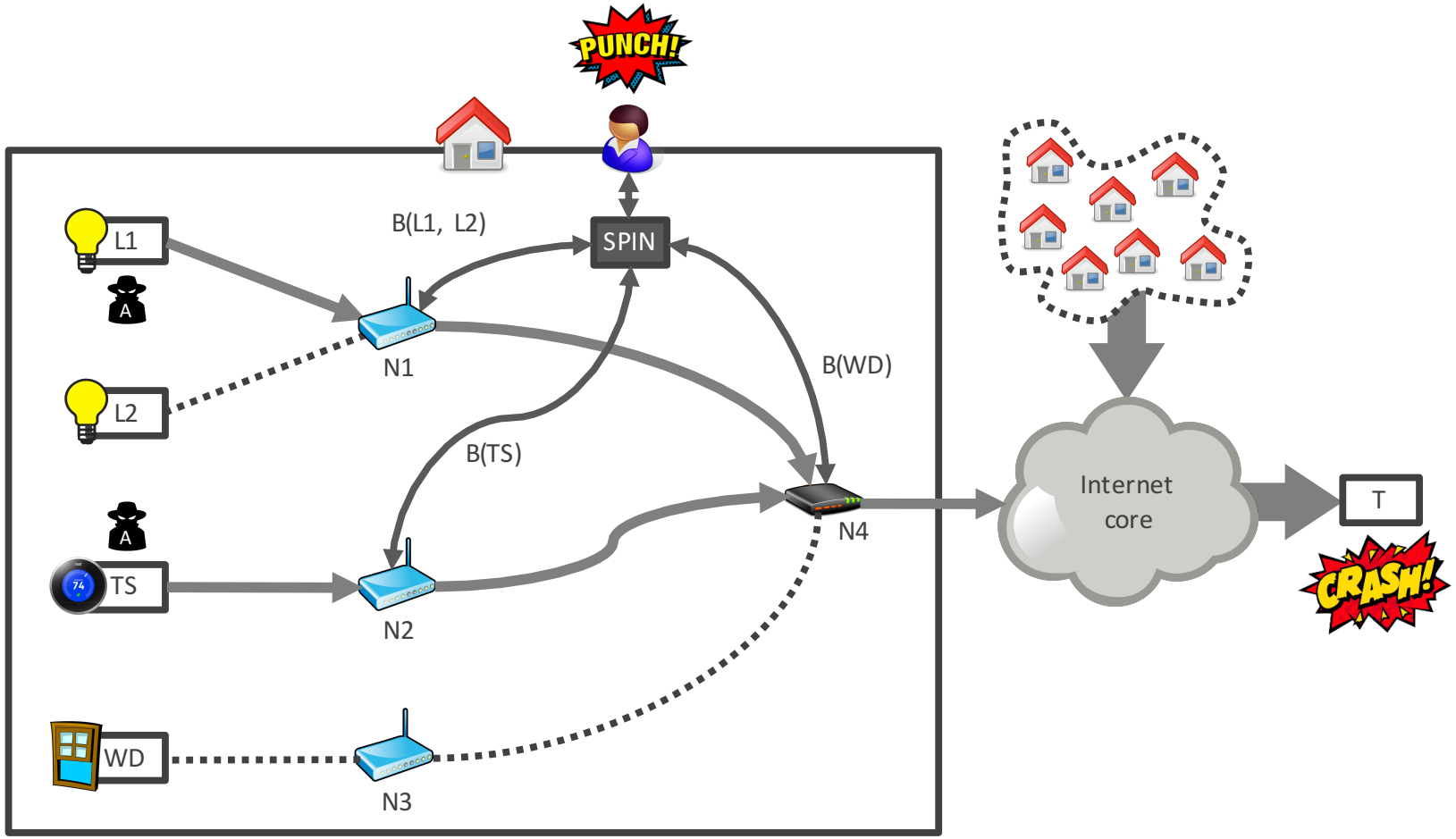
Other targets: OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

[Mirai], [Hajime], [SAC105]
https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

UNIVERSITY OF TWENTE.

SDN LABS

Example of an IoT security system: SPIN



https://spin.sidnlabs.nl/en/

UNIVERSITY OF TWENTE.

SIDN LABS

Key challenges

- Enable safer, smarter, and more sustainable society through the IoT
- Protect the Internet and its users (at home and elsewhere)
- Deployment of IoT security solutions
- Interoperability between IoT devices and security services
- We'll be discussing papers that address these issues

UNIVERSITY OF TWENTE. SIDN LABS

Course overview

UNIVERSITY OF TWENTE.

SDN 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%

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

- We'll announce the papers that will be discussed in the oral exam one week beforehand

UNIVERSITY OF TWENTE.

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 A4 page
- You can add figures and graphs from the paper or add your own if you like
- Submit through CANVAS on the **Tuesday** before the lecture in which the papers will be discussed

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

UNIVERSITY OF TWENTE. SIDN 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 the MUD specification
- Five-page lab report in two-column IEEE format, MUD spec, PCAP file, README file
- Evaluation: clarity and soundness of the methodology, analysis, writing, quality of PCAPs/MUDs
- Firm deadline: **Sunday June 21, 2020, 23:59 CEST**

UNIVERSITY OF TWENTE.

SIDN LABS

Lab assignment

- 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
- Do not use multi-purpose devices like tablets, phones, laptops
- No SPIN devices this year: use WireShark, TCPdump, or other
- Etienne Khan available for assistance

UNIVERSITY OF TWENTE.

SDN LABS

Oral exam

- Q&A with an SSI teacher and a teaching assistant
- Covers a **subset** of the 12 papers you studied, use the summaries you wrote
- We'll announce your subset of papers in the week before the exams
- Takes about 30 minutes and will take place from June 22 through July 3
- We'll likely need take your oral exam through a video call (instructions on the SSI site)

UNIVERSITY OF TWENTE.

SIDN LABS

Important dates

- Two summaries per lecture: before the lecture in which the papers will be discussed
- Lab report, PCAPs, MUD files, README file: Sun June 21, 2020, 23:59 CEST
- All to be submitted through CANVAS

Schedule

No.	Date	Contents
1	Apr 22	Course introduction Guest lecture #1: how the core of the internet is organized
2	Apr 29	Guest lecture #2: Security in The Things Network
3	May 6	Lecture: IoT Concepts and Applications
4	May 13	Lecture: IoT Botnet Measurements
5	May 20	Lecture: IoT Honeypots
6	May 27	Lecture: IoT Edge Security Systems
7	Jun 3	Lecture: IoT Device Behavior
8	Jun 10	Lecture: IoT Network Security
9	Jun 17	Lecture: IoT Edge Security Systems (re-sit)

UNIVERSITY OF TWENTE.

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

Learning outcomes

- 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)

UNIVERSITY OF TWENTE.

SIDN LABS

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 20 – July 5, 2020
Academic year	2019/2020

UNIVERSITY OF TWENTE.

SIDN LABS

SIDN Labs?

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 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 DACS' latest academic insights, methodologies, network, and creative thinking
  - DACS group: further improved research and education using SIDN's operational experience, unique datasets, and industry network

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
5.9M domain names
3.2M DNSSEC-signed
1.3B DNS queries/day

SIDN fonds

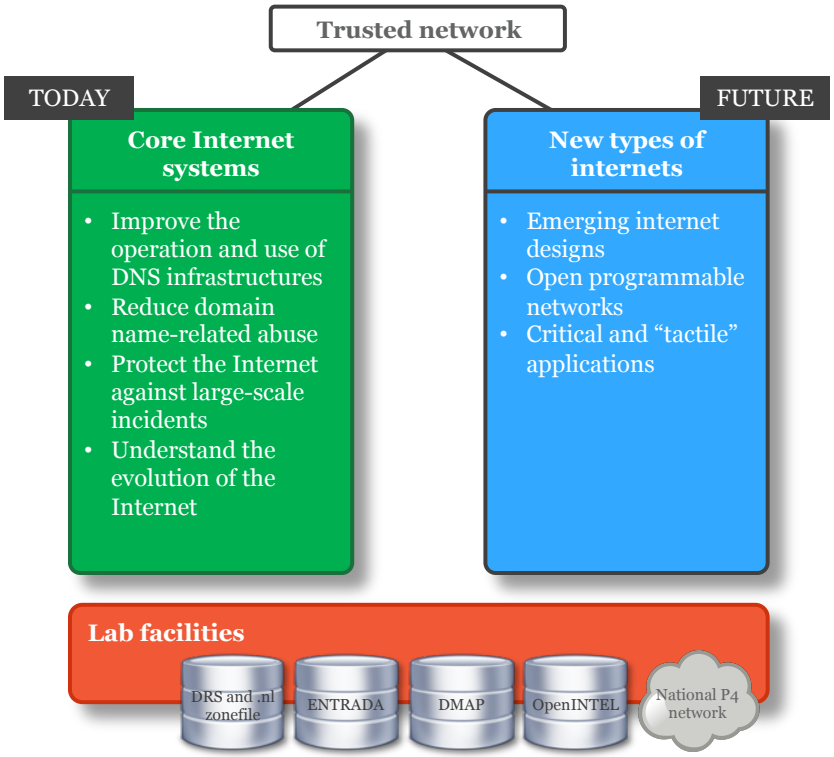
UNIVERSITY OF TWENTE.

SIDN LABS

SIDN Labs objective: to increase the trustworthiness of our society's internet infrastructure

- Trusted = secure, stable, resilient, and transparent, for .nl and NL in particular

- Strategies to get there
  - Measure, prototype, evaluate mechanisms that increase the trustworthiness of the Internet
  - The same, but for new internet infrastructures that complement the Internet
  - Reinforce the Dutch, European, and global research and operational communities

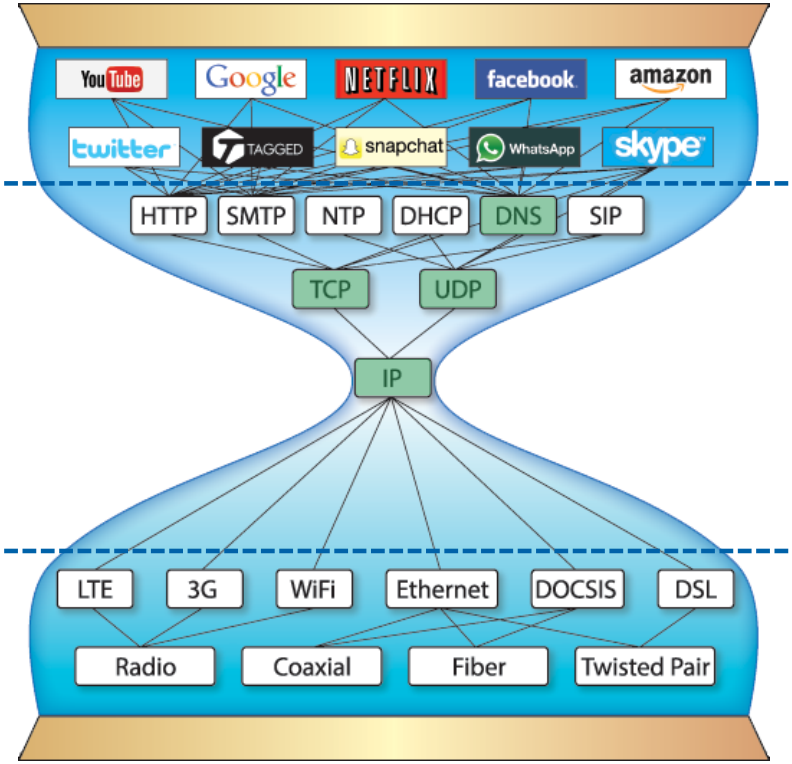


UNIVERSITY OF TWENTE.

SIDN LABS

The Internet under the hood

Most people



Services

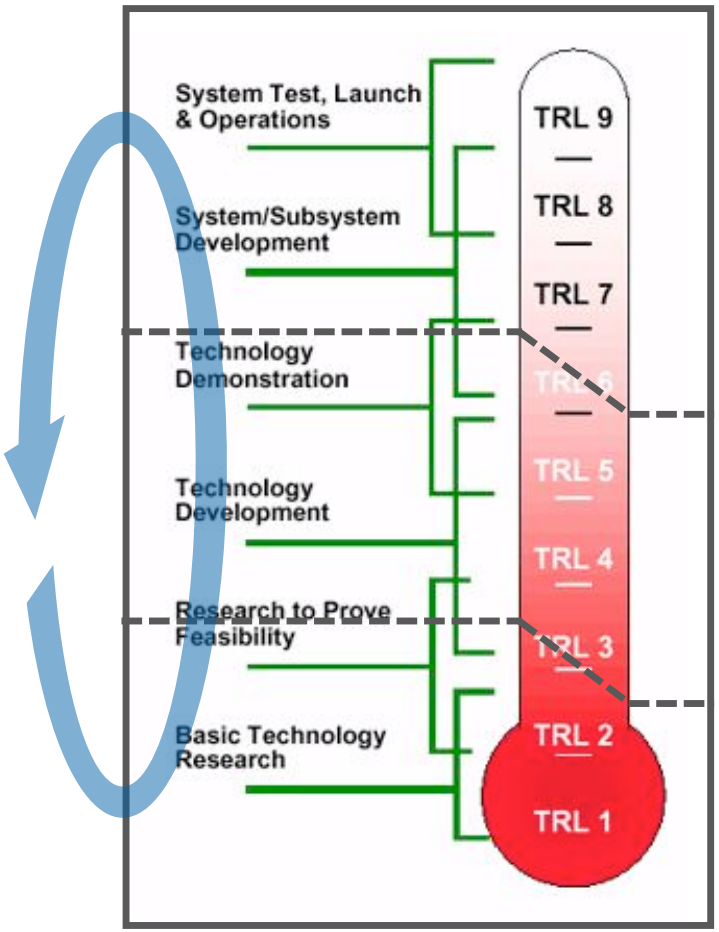
Internet core protocols

Transmission

UNIVERSITY OF TWENTE.

Technology Readiness Levels

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



Operations

Experimental

Basic research

UNIVERSITY OF TWENTE.

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

Daily work

- Help operational teams
- Write open source software
- Analyze vast amounts of data
- Run experiments
- Write academic papers and tech reports
- Work with universities

UNIVERSITY OF TWENTE.

SIDN LABS

Examples of research partners

Guest lecture

Marco Davids (SIDN Labs)

UNIVERSITY OF TWENTE.

SIDN LABS

Volg ons

SIDN.nl

@SIDN

SIDN

Q&A

Next lecture: **Wed Apr 29, 10:45-12:30**

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

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

UNIVERSITY OF TWENTE.

SIDN LABS