Security Services for the IoT: Introduction

Cristian Hesselman, Antonia Affinito, Etienne Khan, and Ting-Han Chen

UNIVERSITY OF TWENTE.

SIDN LABS

Teaching team

Cristian Hesselman
(teacher)

Antonia Affinito
(teacher)

Etienne Khan
(teaching assistant)

Ting-Han Chen
(teaching assistant)

Teaching team

Antonia Affinito
(teacher)

- Assistant Professor at Design and Analysis at Communication Systems (DACS) - EEMCS Faculty
- Research Interests:
  - DNS Security
  - Cyber Threats Detection
  - Network Measurements
  - IoT Security

Learning Objectives

- Provide an overview of Security Services for the IoT (SSI)

- Understand the basic concepts of the IoT security

- Develop an understanding of the assessment, deliverables, etc.

- Result: understanding of SSI, the work you'll need to carry out, and some IoT inspiration

Agenda

- High-level introduction to IoT security
- Course overview
- Group Assignment: Assessing risks of IoT devices

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?

Security issues in the IoT?

Poll: How you define the Internet of Things (IoT)?

https://www.bsitsoftware.com/iot

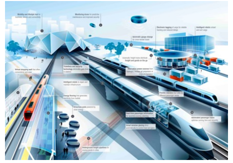
UNIVERSITY OF TWENTE.

SIDN LABS

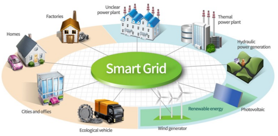
Internet of Things (IoT)

- 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



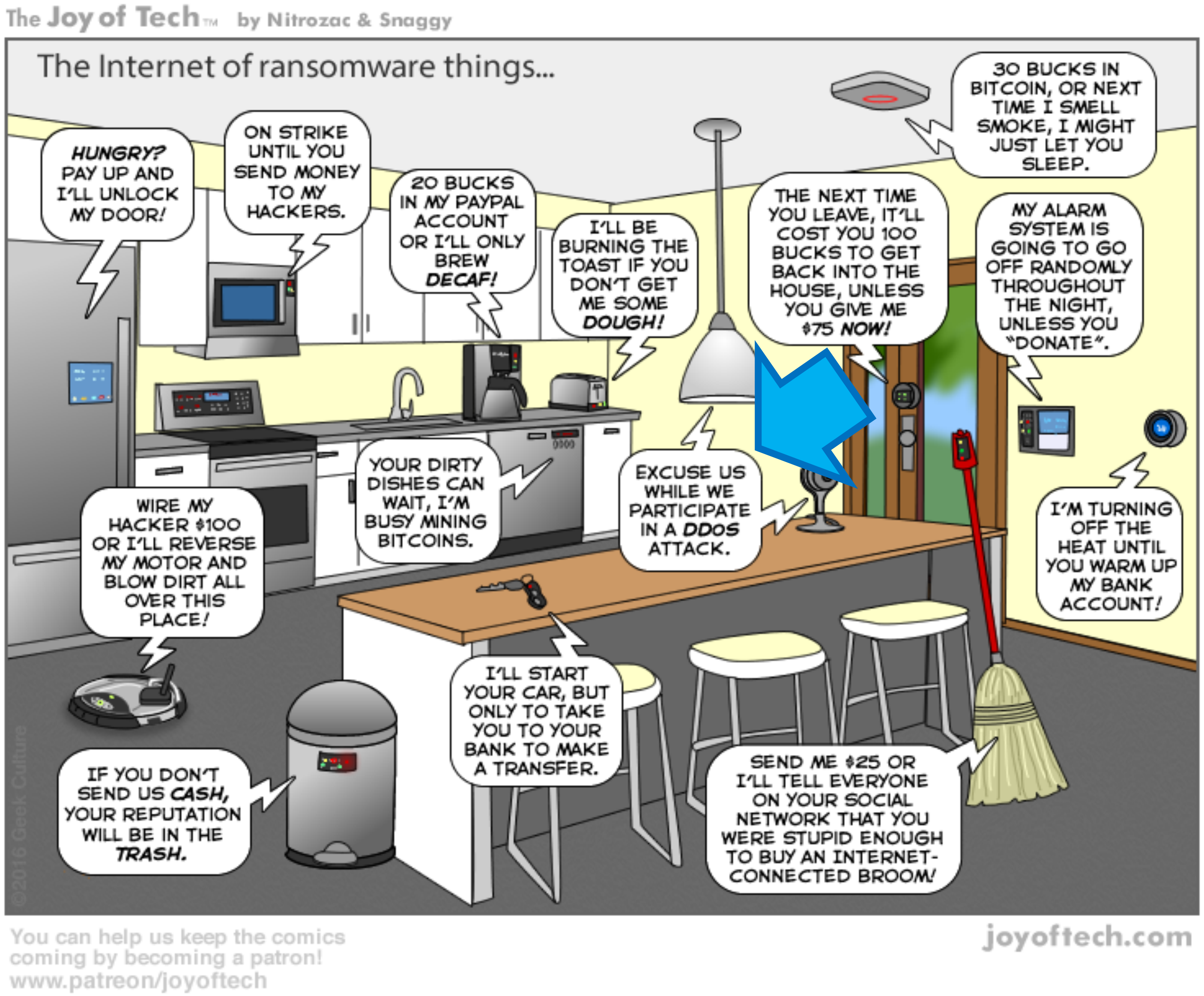
Smart energy grids

Smart homes and cities

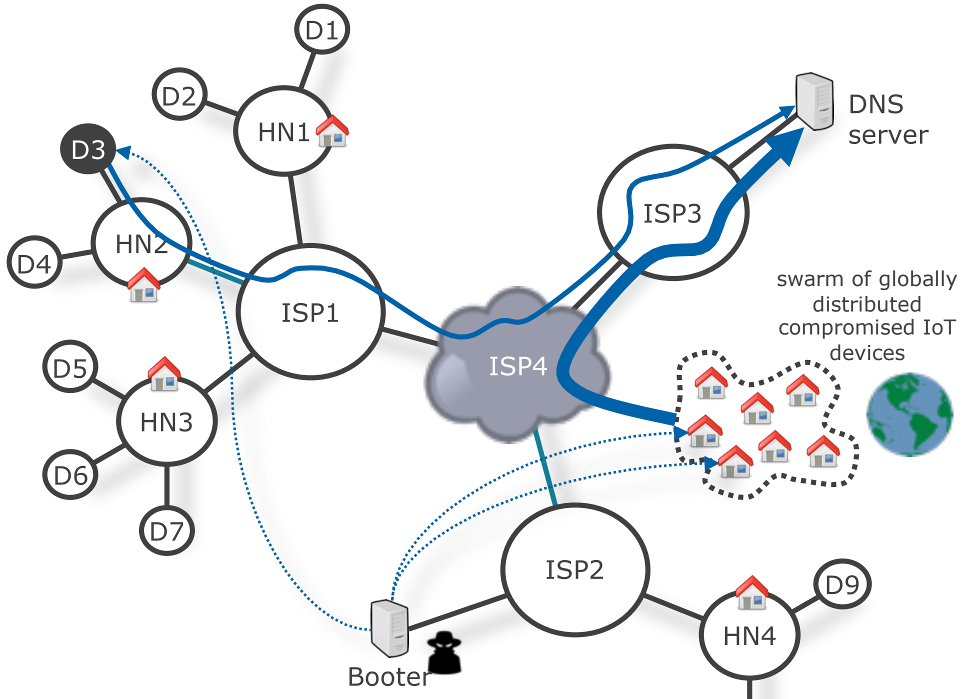
- Promises safer, smarter, more sustainable society, **but IoT security is a major challenge**

Further reading: [WEIS] [DNSIoT]

“The Internet of Insecure Things”


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

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

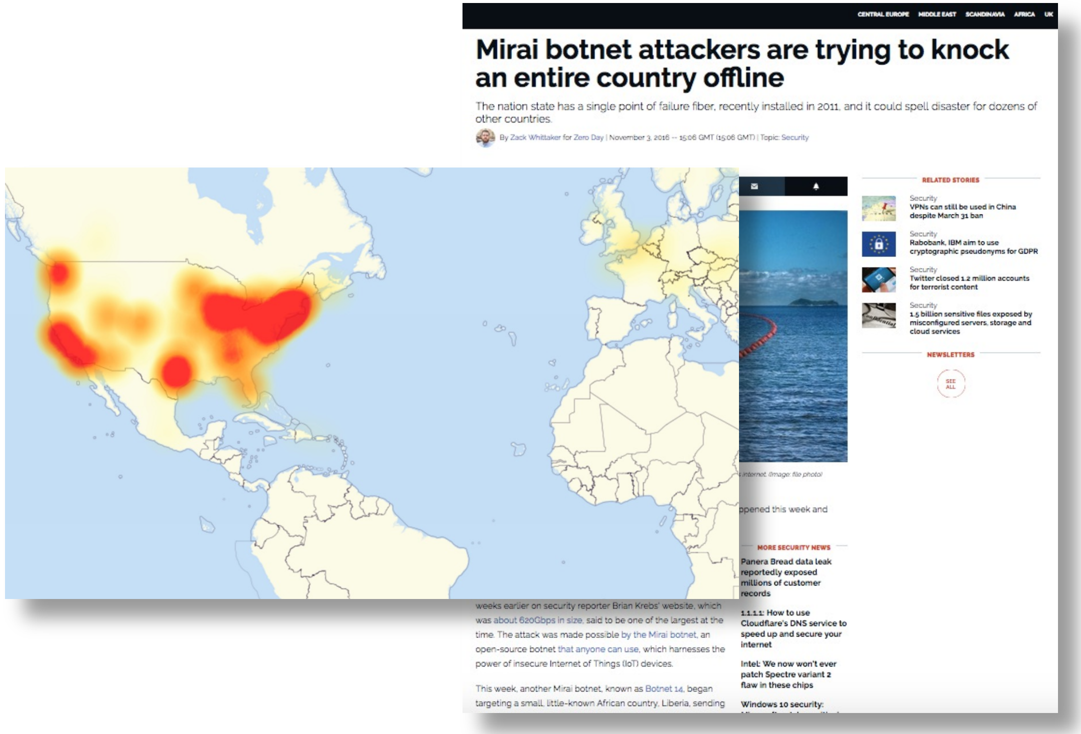


◂····· Control commands

◂━━ DDoS flow

HN = Home Network

D = IoT device



Mirai botnet attackers are trying to knock an entire country offline

The nation state has a single point of failure fiber, recently installed in 2011, and it could spell disaster for dozens of other countries.

By Zack Whittaker for Zero Day | November 3, 2016 -- 15:06 GMT (15:06 GMT) | Topic: Security

RELATED STORIES

Security
VPNs can still be used in China despite March 31 ban

Security
Rabobank, IBM aim to use cryptographic pseudonyms for GDPR

Security
Twitter closed 1.2 million accounts for terrorist content

Security
1.5 billion sensitive files exposed by misconfigured servers, storage and cloud services

NEWSLETTERS

SEE ALL

internet. (Image: file photo)

ppened this week and

weeks earlier on security reporter Brian Krebs' website, which was about 620Gbps in size, said to be one of the largest at the time. The attack was made possible by the Mirai botnet, an open-source botnet that anyone can use, which harnesses the power of insecure Internet of Things (IoT) devices.

This week, another Mirai botnet, known as Botnet 14, began targeting a small, little-known African country, Liberia, sending

MORE SECURITY NEWS

Panera Bread data leak reportedly exposed millions of customer records

1.1.1.1: How to use Cloudflare's DNS service to speed up and secure your internet

Intel: We now won't ever patch Spectre variant 2 flaw in these chips

Windows 10 security:

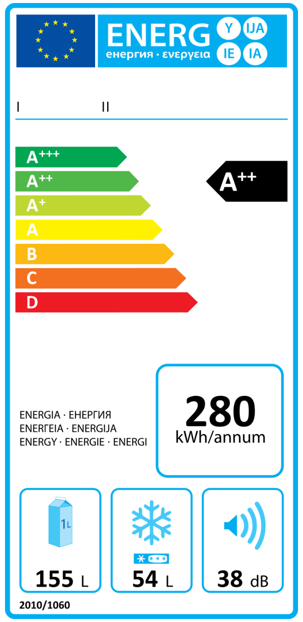
Other targets: OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

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

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

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

SSI is an ‘overview’ course

Assessment

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

- Total score = [(score of written 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 written 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

Deliverable #2: lab report

Group-based project:
a measurement-based study

Group signups open later today

Firm deadline: Wednesday 19 June 2024, 09:00 CEST

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

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?

Use of ChatGPT and other tools

- You may use ChaptGPT, Grammarly or other tools to help you **improve the language** of your lab report.
  - The **original content** MUST however be written by you and your lab group.
- Your report MUST include either of these **two statements** or otherwise we will **not** take it into consideration.
  - "AUTHOR DECLARATION: During the preparation of this work the authors used [NAME TOOL / SERVICE] ONLY to improve the language of their report. The authors confirm that they alone wrote the original text in full and that they then reviewed and edited the content using [NAME TOOL / SERVICE]. The authors jointly take full responsibility for the content of the work.
  - "AUTHOR DECLARATION: During the preparation of this work the authors used no artificial intelligence tools."

Lab groups: selection & management

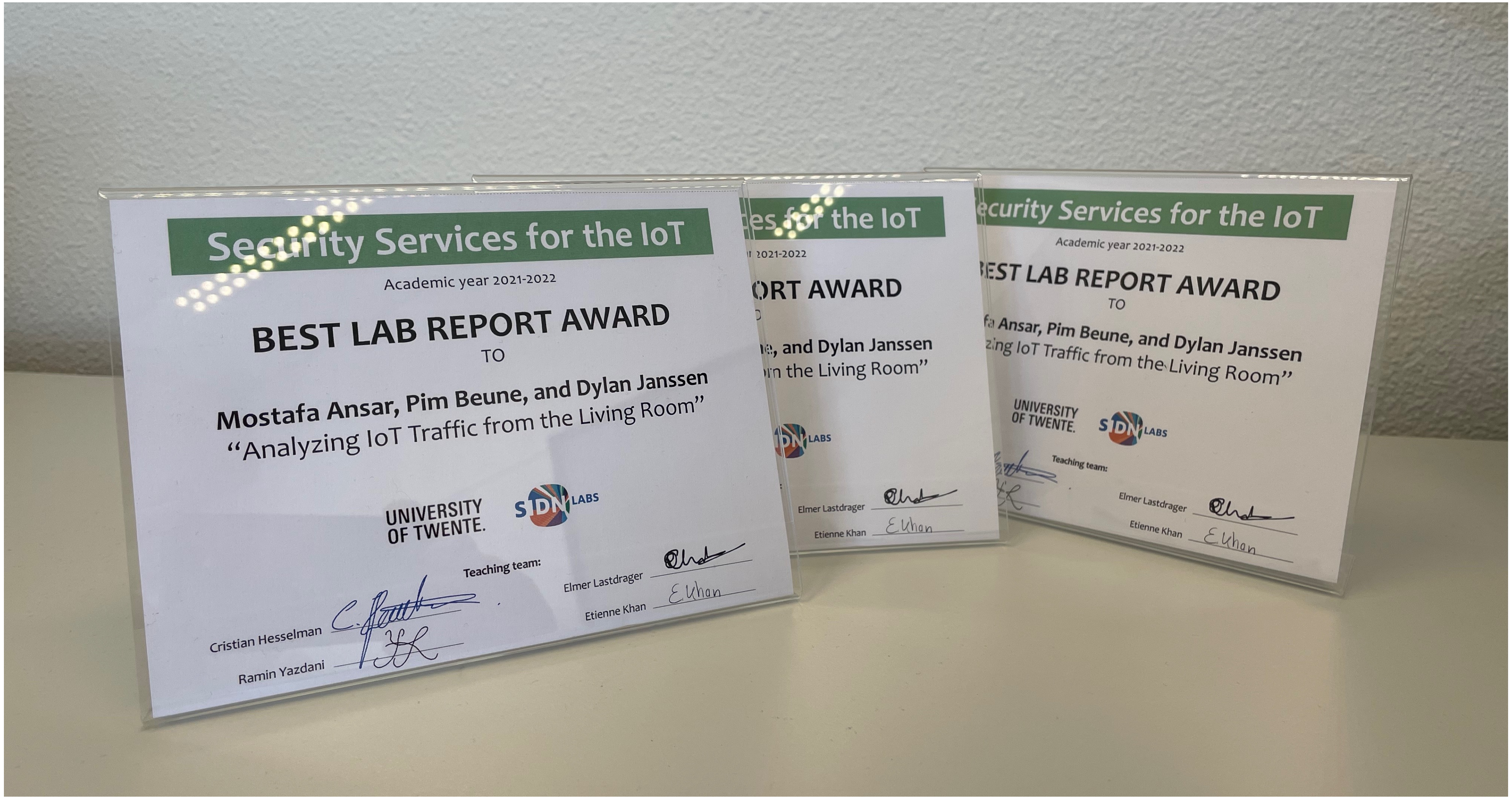
Form groups with members having **similar skills/background**.

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.

Best paper award



Security Services for the IoT

Academic year 2021-2022

BEST LAB REPORT AWARD

TO

Mostafa Ansar, Pim Beune, and Dylan Janssen

"Analyzing IoT Traffic from the Living Room"

Teaching team:

Cristian Hesselman

Ramin Yazdani

Elmer Lastdrager

Etienne Khan E.Khan

es for the IoT
r 2021-2022
ORT AWARD
e, and Dylan Janssen
rn the Living Room"
Elmer Lastdrager
Etienne Khan E.Khan

ecurity Services for the IoT
Academic year 2021-2022
EST LAB REPORT AWARD
TO
a Ansar, Pim Beune, and Dylan Janssen
zing IoT Traffic from the Living Room"
Teaching team:
Elmer Lastdrager
Etienne Khan E.Khan

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

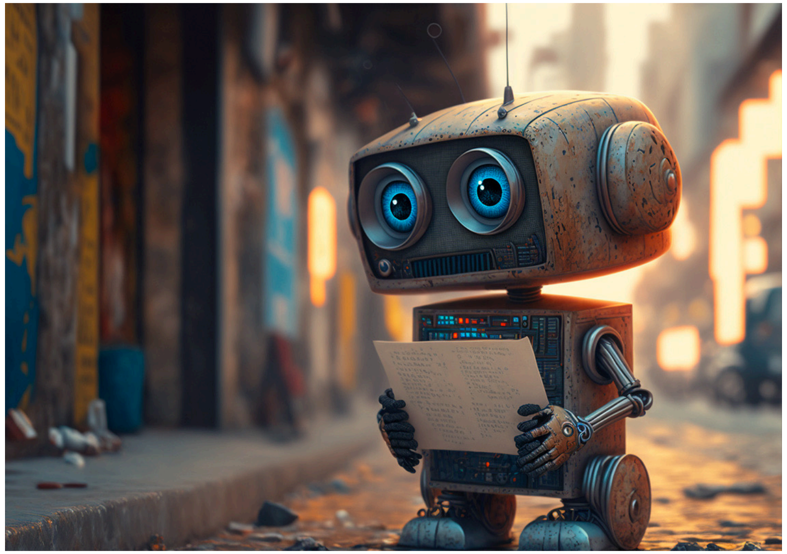
Written exam

- Multiple-choice and open questions on Remindo platform
- Covers the 12 papers you studied
- You can bring at most 1 A4 page summary of the papers
- Takes about 2 hours and will take place on July 3
- The written exams will take place on campus, room to be announced.

LLM’s (ChatGPT and others)

- 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: Wednesday 19 June 2024, 09:00 CEST
- All to be submitted through CANVAS

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

Schedule

No.	Date	Contents
1	May 1	Course introduction
2	May 7	Guest lecture #1: How the core of the Internet works. Lecturer: Marco Davids (SIDN Labs)
3	May 8	Lecture: IoT and Internet Core Protocols
4	May 15	Lecture: IoT Edge Security Systems
5	May 29	Lecture: IoT Botnet Measurements 1
6	Jun 5	Lecture: IoT Botnet Measurements 2
7	Jun 12	Lecture: IoT Security in Non-Carpeted Areas
8	Jun 19	Lecture: IoT Device Security
9	???	Guest lecture #2: t.b.d

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

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

- Replaced 2 papers
- Written exam
- 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. Antonia Affinito (University of Twente)
Teaching Assistents	Etienne Khan (University of Twente) Ting-Han Chen (University of Twente)
Fourth quartile	April 29 to July 5, 2024
Academic year	2023/2024

Group Assignment

How concerned are you about the security of your IoT devices?

- **Open discussion** in groups of 5 students
  - Choose 5 students who are sitting close to you
  - If there are no enough students, smaller groups are also acceptable
- **Select** an IoT device and **identify** all the potential **security risks** associated with it
  - You may use sources online to assist you
- At the end of the exercise (15 min), each group will be expected to give a **1-minute pitch**.

1-Minute Pitch

UNIVERSITY OF TWENTE.

SIDN LABS

Today’s learning objective

- To what extent you think you will be able to **address** all the course requirements for the SSI course?
- To what extent you think you will be able to **discuss** the basic IoT concepts?

😃 😐 🙁

Feedback

- **Please share your feedback on today's lecture**
- How **well** did the lecture cover the course requirements?
- How **helpful** was the practical session?

😀 😐 🙁

- We **value** your input and feedback
  - At the end of the second lecture, we will have a **10-minute round** of feedback.

Q&A

Next guest lecture: **Tue May 7**
Next lecture: **Wed May 8**

Cristian Hesselman Director of SIDN Labs	+31 6 25 07 87 33 c.e.w.hesselman@utwente.nl @hesselma
Antonia Affinito Assistant Professor	a.affinito@utwente.nl

UNIVERSITY OF TWENTE. SIDN LABS