Security Services for the Internet of Things: Introduction

Prof. Cristian Hesselman, dr. Antonia Affinito, dr. Savvas Kastanakis,
Etienne Khan, Ting-Han Chen, Pascal Huppert

Friday, 25 April, 2025

UNIVERSITY OF TWENTE. SIDN LABS

About me

- Postdoc @ University of Twente, DACS Group (2024 - now)
- PhD in Computer Science @ Lancaster University, SSG (2020 - 2024)
- BSc and MSc in Computer Science @ University of Crete and FORTH (2011 - 2018)

- Interested in:
  - Internet Measurement (with a preference on geopolitical and security concerns)
  - Internet Routing Attacks (but mostly defenses)
  - Trying to answer questions like: *how much of Europe's digital infrastructure relies on the US?,* or, *which paths on the Internet are more secure than the rest?* or, *what portion of the Internet's networks comply with best-current-practices?*

The *menu* for today…

- ❖ Welcome & Course Introduction
- ❖ Motivation: Why IoT Security?
- ❖ Course Objectives
- ❖ Course Format & Deliverables
- ❖ Common Pitfalls

UNIVERSITY OF TWENTE. SIDN LABS

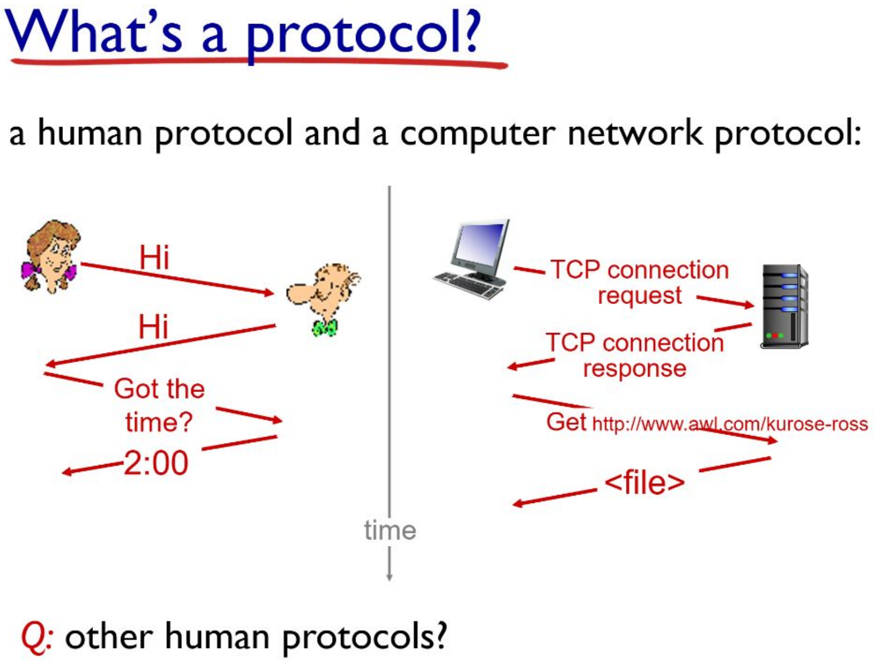
The *menu* for today…

- Welcome & Course Introduction
- Motivation: Why IoT Security?
- Course Objectives
- Course Format & Deliverables
- Common Pitfalls

UNIVERSITY
OF TWENTE.

SIDN LABS

Computer Networking 101



What’s a protocol?

a human protocol and a computer network protocol:

Q: other human protocols?

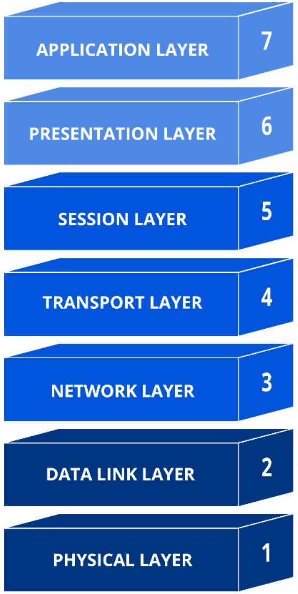
From the book: Computer Networking: A top-down approach

Computer Networking 101

A few (basic) networking concepts that we should know:

- ***Which are the nuts and bolts of communication networks?***
  a. Hosts: computing devices/end-systems (e.g., PC, server, laptop, smartphone, smartwatch)
  b. Links: medium which connect two endpoints (e.g., fiber, copper, radio, satellite)
  c. Switches: devices that connect multiple hosts within the same network
  d. Routers: devices that connect different networks, directing packets between them
  e. Protocols: the language spoken by hosts/links/switches/routers, i.e., rules that define how data is formatted/transmitted
  f. Standards: before using a protocol, the community first standardizes it (we all speak the same language)
- ***Which are some of the most important protocols?***
  a. IP: a fundamental protocol to identify devices and networks
  b. TCP: a reliable protocol to deliver data from one end to another
  c. DNS: a protocol which enables the translation of human-readable names into machine-readable IP addresses
  d. BGP: the Internet's routing protocol which determines the best paths to a destination
  e. HTTP(S): the cornerstone WWW protocol which enables communication between browsers/clients and servers
- ***What is the OSI model?***

Computer Networking 101



— Human-computer interaction layer, where applications can access the network services

— Ensures that data is in a usable format and is where data encryption occurs

— Maintains connections and is responsible for controlling ports and sessions

— Transmits data using transmission protocols including TCP and UDP

— Decides which physical path the data will take

— Defines the format of data on the network

— Transmits raw bit stream over the physical medium

How many of you are wearing/carrying a *thing* on them?

What is (or is not) an IoT device (aka a *thing*)?

These are **devices purpose-built to sense, transmit, or act autonomously**, often without direct user control.

- Smart thermostat
- Smart bulb
- Fitness tracker
- Smartwatch
- Smart speaker
- IP camera
- Motion sensor
- AirTag / Bluetooth tracker

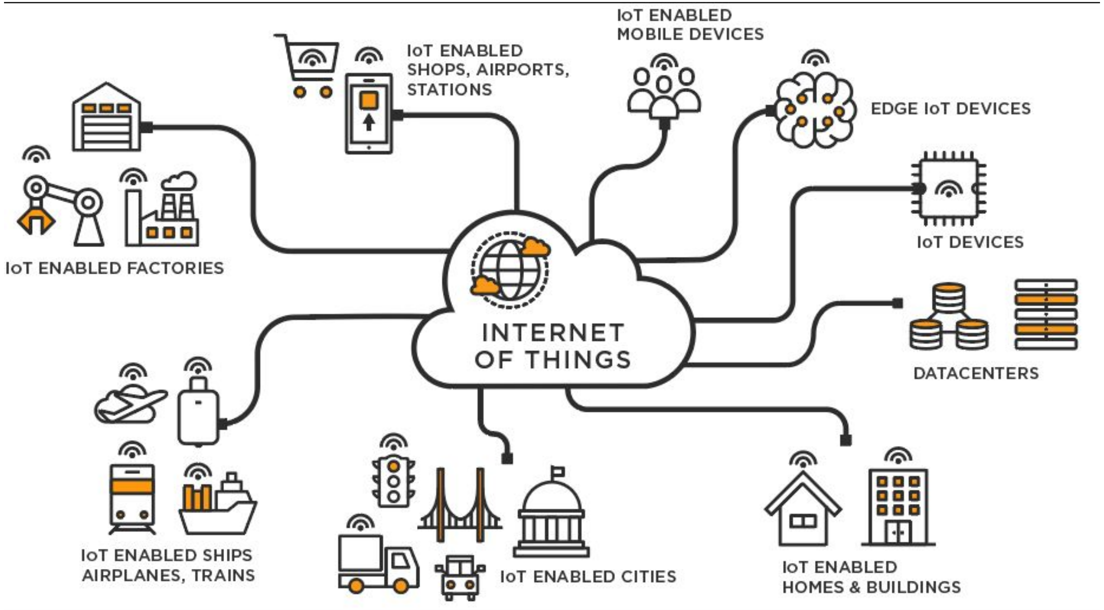
These are **general-purpose computing devices** or simply “connected” but not IoT in spirit.

- Smartphone
- Laptop
- Tablet
- Desktop PC
- Game console
- Smart TV*(This one is tricky — it's connected, but behaves more like a media platform than a sensing device.)

What is the definition of the Internet of Things?

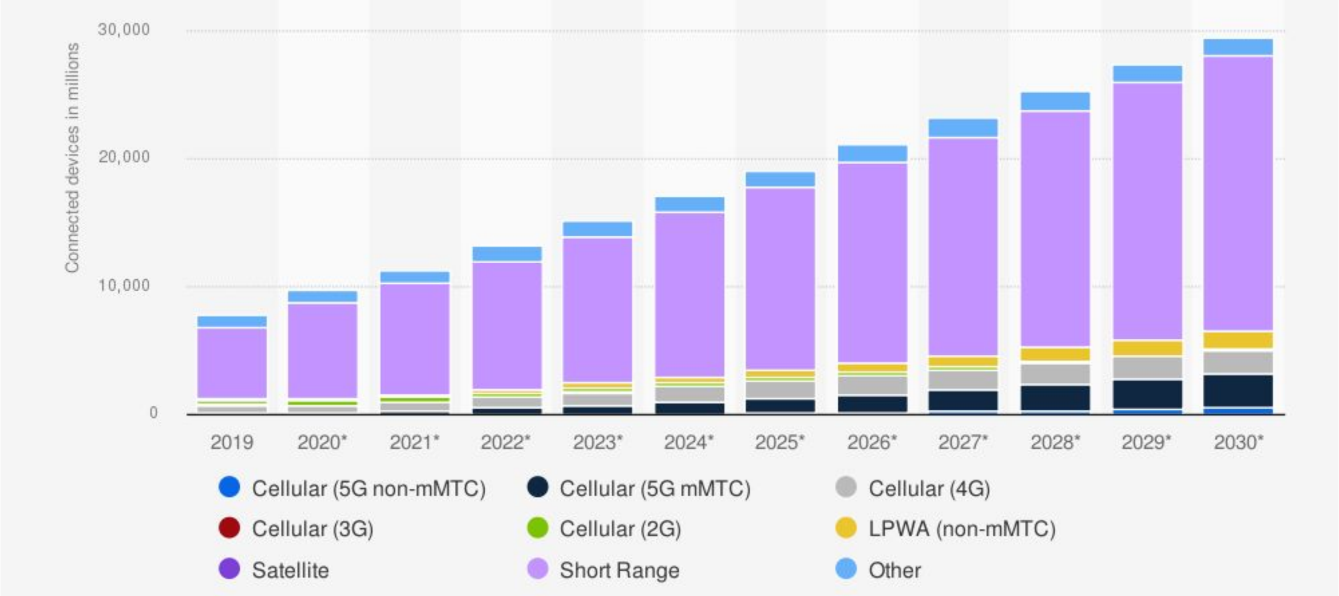
What is the definition of IoT?

A network of physical objects (“things”) embedded with sensors, software, and connectivity to exchange data.


IoT ENABLED SHOPS, AIRPORTS, STATIONS
IoT ENABLED MOBILE DEVICES
EDGE IoT DEVICES
IoT DEVICES
DATACENTERS
IoT ENABLED FACTORIES
INTERNET OF THINGS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

The (explosive) growth of connected IoT!

This unprecedented growth underscores IoT's transition from a tech trend to a foundational pillar of digital infrastructure.



https://www.statista.com/statistics/1194688/iot-connected-devices-communications-technology/

What is the definition of IoT?

A network of physical objects (“things”) embedded with sensors, software, and connectivity to exchange data.

- **Applications:** Used in smart homes, healthcare, industrial systems, agriculture, and more to enhance efficiency and decision-making.
- **Real-Time Data Collection:** Continuously gathers data from the environment or user interactions to provide timely insights.
- **Edge & Cloud Integration:** Devices often process data locally (edge computing) or send it to the cloud for analysis and storage.
- **Scalability:** Can range from a single device in a home to millions of sensors across a smart city or industrial operation.
- **Security & Privacy Challenges:** Introduces new vulnerabilities due to large attack surfaces and sensitive data handling.
- **Energy & Resource Constraints:** Many IoT devices are low-power and resource-limited, influencing design and security considerations.

What is the definition of IoT?

A network of physical objects (“things”) embedded with sensors, software, and connectivity to exchange data.

- **Applications:** Used in smart homes, healthcare, industrial systems, agriculture, and more to enhance efficiency and decision-making.
- **Real-Time Data Collection:** Continuously gathers data from the environment or user interactions to provide timely insights.
- **Edge & Cloud Integration:** Devices often process data locally (edge computing) or send it to the cloud for analysis and storage.
- **Scalability:** Can range from a single device in a home to millions of sensors across a smart city or industrial operation.
- **Security & Privacy Challenges:** Introduces new vulnerabilities due to large attack surfaces and sensitive data handling.
- **Energy & Resource Constraints:** Many IoT devices are low-power and resource-limited, influencing design and security considerations.

The *menu* for today…

- ❖ Welcome & Course Introduction
- ❖ Motivation: Why IoT Security?
- ❖ Course Objectives
- ❖ Course Format & Deliverables
- ❖ Common Pitfalls

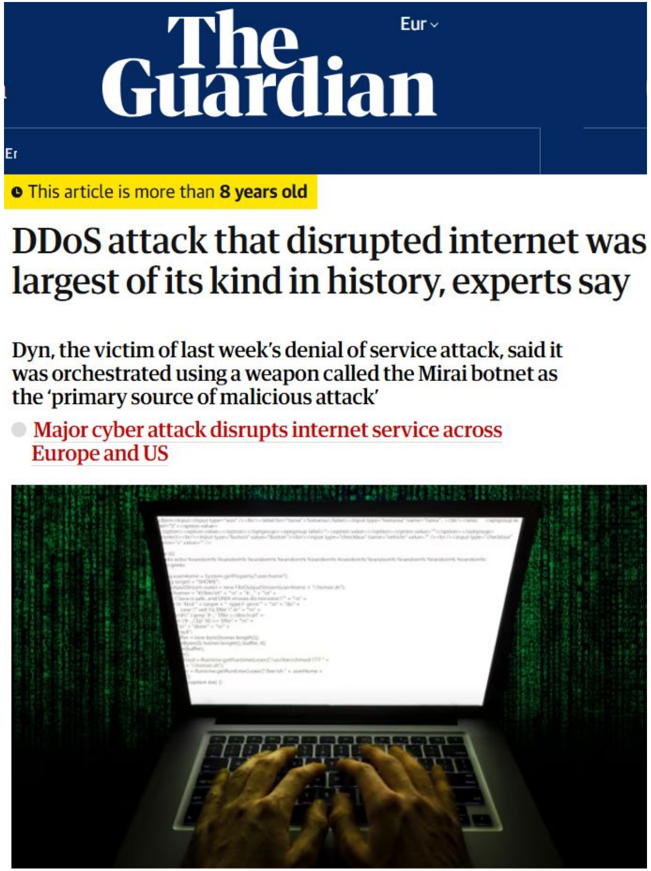
The IoT wakeup call: Mirai-powered DDoS attacks (2016)

What Happened?

- In October 2016, the **Mirai botnet** launched one of the largest DDoS attacks in history.
- It targeted **Dyn**, a major DNS provider, bringing down sites like **Twitter, Netflix, Reddit, and Spotify**.

The Role of IoT

- Mirai infected **hundreds of thousands of insecure IoT devices** (e.g., IP cameras, routers).
- Devices were hijacked using **default usernames and passwords**.
- Formed a massive botnet used to flood targets with traffic.



This article is more than **8 years old**

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Major cyber attack disrupts internet service across Europe and US

UNIVERSITY OF TWENTE.

SIDN LABS

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

Impact

- **1.2 Tbps** of traffic — largest attack ever at the time.
- Exposed the fragility of the Internet’s infrastructure.
- Sparked global concern about **IoT security standards** and device regulation.

Why It Matters?

- Mirai showed that **"dumb" devices** can cause **smart problems**.
- Shifted IoT security from a niche topic to a **global priority**.
- Inspired standards like **MUD* (RFC 8520)** and government attention.

*The **Manufacturer Usage Description (MUD)** is a standard developed by the IETF (Internet Engineering Task Force) to help secure IoT devices by defining and enforcing their **expected network behavior**.

Key Challenges in IoT Security

1. Device Diversity & Scale:
   a. Billions of devices, countless vendors, varying software/hardware stacks
   b. Hard to apply one-size-fits-all solutions
2. Lack of Standards:
   a. Many IoT devices are inconsistent to security protocol implementations and update mechanisms.
3. Limited Resources:
   a. Many IoT devices are low-power, minimal memory/CPU
   b. Can’t run traditional security tools (antivirus, heavy encryption, etc.)
4. Security vs Usability:
   a. Secure configs mean harder setup or limited functionality
   b. Manufacturers often prioritize time-to-market and ease of use

UNIVERSITY OF TWENTE.

SIDN LABS

Key Challenges discussed in SSI’25

1. Device Diversity & Scale:
    a. Discussed in lecture topics on IoT ecosystems and threat modelling
    b. Explored through lab work analyzing IoT devices
2. Lack of Standards:
    a. Analyzed via readings on MUD (RFC8520) and security frameworks
    b. Hands-on use of MUD profiles in lab assignment
3. Limited Resources:
    a. Topic in lectures on lightweight security protocols
    b. Use of efficient tools (wireshark and tcpdump) for constrained devices
4. Security vs Usability:
    a. Guest lectures and papers on the trade-offs of real-world IoT deployments.
    b. Class discussions around usability testing and secure configs

UNIVERSITY OF TWENTE. SIDN LABS

The *menu* for today…

- ❖ Welcome & Course Introduction
- ❖ Motivation: Why IoT Security?
- ❖ Course Objectives
- ❖ Course Format & Deliverables
- ❖ Common Pitfalls

UNIVERSITY OF TWENTE. SIDN LABS

Learning Objectives

By the end of this course, students will be able to:

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

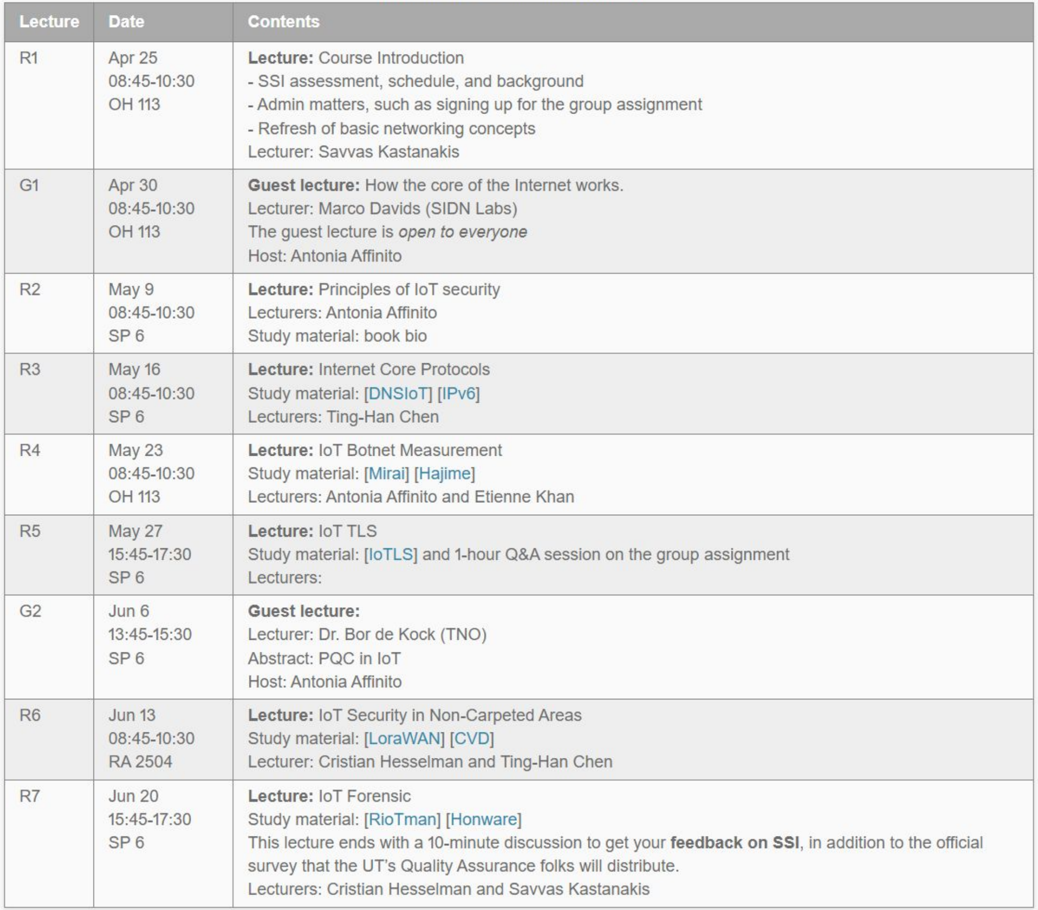
- Be able to analyze network traffic of IoT devices and create device profiles that describe this behavior

SSI also contributes to your skills to independently carry out research projects and to develop new services and systems.

The *menu* for today…

- ❖ Welcome & Course Introduction
- ❖ Motivation: Why IoT Security?
- ❖ Course Objectives
- ❖ Course Format & Deliverables
- ❖ Common Pitfalls

Schedule



Lecture	Date	Contents
R1	Apr 25 08:45-10:30 OH 113	**Lecture:** Course Introduction - SSI assessment, schedule, and background - Admin matters, such as signing up for the group assignment - Refresh of basic networking concepts Lecturer: Savvas Kastanakis
G1	Apr 30 08:45-10:30 OH 113	**Guest lecture:** How the core of the Internet works. Lecturer: Marco Davids (SIDN Labs) The guest lecture is *open to everyone* Host: Antonia Affinito
R2	May 9 08:45-10:30 SP 6	**Lecture:** Principles of IoT security Lecturers: Antonia Affinito Study material: book bio
R3	May 16 08:45-10:30 SP 6	**Lecture:** Internet Core Protocols Study material: [DNSIoT] [IPv6] Lecturers: Ting-Han Chen
R4	May 23 08:45-10:30 OH 113	**Lecture:** IoT Botnet Measurement Study material: [Mirai] [Hajime] Lecturers: Antonia Affinito and Etienne Khan
R5	May 27 15:45-17:30 SP 6	**Lecture:** IoT TLS Study material: [IoTLS] and 1-hour Q&A session on the group assignment Lecturers:
G2	Jun 6 13:45-15:30 SP 6	**Guest lecture:** Lecturer: Dr. Bor de Kock (TNO) Abstract: PQC in IoT Host: Antonia Affinito
R6	Jun 13 08:45-10:30 RA 2504	**Lecture:** IoT Security in Non-Carpeted Areas Study material: [LoraWAN] [CVD] Lecturer: Cristian Hesselman and Ting-Han Chen
R7	Jun 20 15:45-17:30 SP 6	**Lecture:** IoT Forensic Study material: [RioTman] [Honware] This lecture ends with a 10-minute discussion to get your **feedback on SSI**, in addition to the official survey that the UT's Quality Assurance folks will distribute. Lecturers: Cristian Hesselman and Savvas Kastanakis

Course Format

- **Lectures:** 9 sessions (7 regular, 2 guest lectures) focusing on IoT security topics.
  - **Paper Discussions:** Each lecture discusses two academic papers; students submit summaries beforehand (max 250 words each).
  - **Guest Lectures:** Industry experts provide real-world perspectives on IoT security challenges.

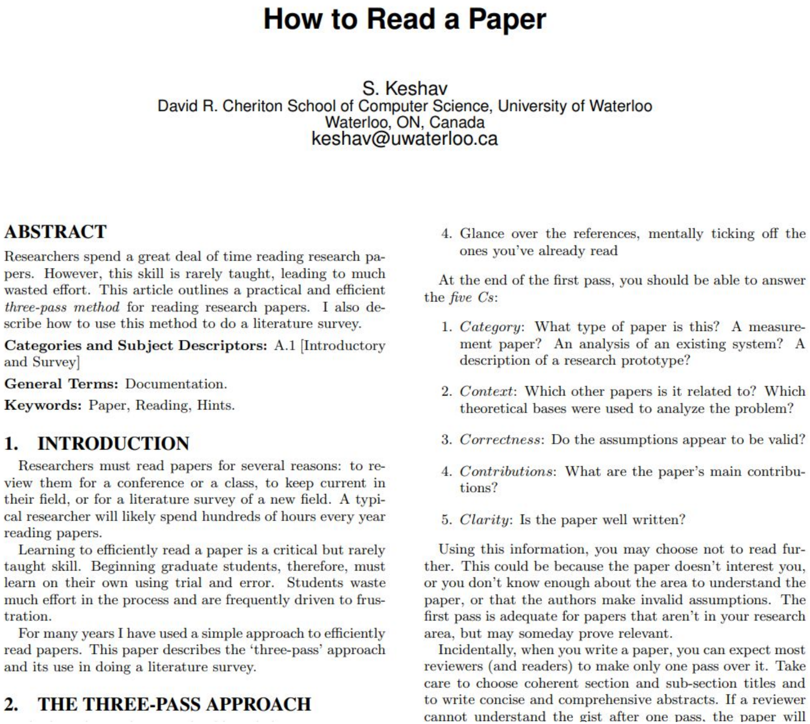
- **Lab Assignment:** Hands-on group project analyzing IoT device behavior using tools like Wireshark and tcpdump.

- **Assessment:** Combination of a written exam + group project evaluation + summaries.

Deliverable #1: Paper Summaries

- **Requirement:** Submit summaries (max 250 words each) before every lecture.
- **Purpose:** Facilitates understanding and prepares students for in-depth discussions.
- **Submission:** Via Canvas by 7 AM on lecture days.
- **Assessment:** Not graded but mandatory for course completion.

How to read a paper?



How to Read a Paper

S. Keshav
David R. Cheriton School of Computer Science, University of Waterloo
Waterloo, ON, Canada
keshav@uwaterloo.ca

ABSTRACT

Researchers spend a great deal of time reading research papers. However, this skill is rarely taught, leading to much wasted effort. This article outlines a practical and efficient *three-pass method* for reading research papers. I also describe how to use this method to do a literature survey.

Categories and Subject Descriptors: A.1 [Introductory and Survey]

General Terms: Documentation.

Keywords: Paper, Reading, Hints.

1. INTRODUCTION

Researchers must read papers for several reasons: to review them for a conference or a class, to keep current in their field, or for a literature survey of a new field. A typical researcher will likely spend hundreds of hours every year reading papers.

Learning to efficiently read a paper is a critical but rarely taught skill. Beginning graduate students, therefore, must learn on their own using trial and error. Students waste much effort in the process and are frequently driven to frustration.

For many years I have used a simple approach to efficiently read papers. This paper describes the 'three-pass' approach and its use in doing a literature survey.

2. THE THREE-PASS APPROACH

4. Glance over the references, mentally ticking off the ones you've already read

At the end of the first pass, you should be able to answer the *five Cs*:

1. *Category*: What type of paper is this? A measurement paper? An analysis of an existing system? A description of a research prototype?

2. *Context*: Which other papers is it related to? Which theoretical bases were used to analyze the problem?

3. *Correctness*: Do the assumptions appear to be valid?

4. *Contributions*: What are the paper's main contributions?

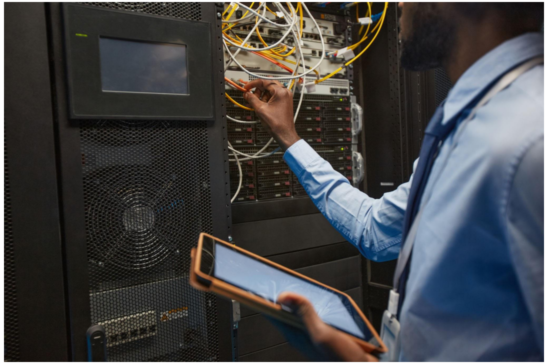
5. *Clarity*: Is the paper well written?

Using this information, you may choose not to read further. This could be because the paper doesn't interest you, or you don't know enough about the area to understand the paper, or that the authors make invalid assumptions. The first pass is adequate for papers that aren't in your research area, but may someday prove relevant.

Incidentally, when you write a paper, you can expect most reviewers (and readers) to make only one pass over it. Take care to choose coherent section and sub-section titles and to write concise and comprehensive abstracts. If a reviewer cannot understand the gist after one pass, the paper will

Deliverable #2: Lab Assignment

- **Group work (4 students)**
- **Objective:** Analyze network traffic of IoT devices and create Manufacturer Usage Descriptions (MUD) profiles
  - Capture and inspect device network behavior
  - Identify unusual or insecure traffic patterns
  - Create device profiles
- **Tools:** Wireshark, tcpdump, MUD specification
- **Output:** Measurement Results + Presentation
- **Deadline:** 19th of June (measurements) + Probably after the exam



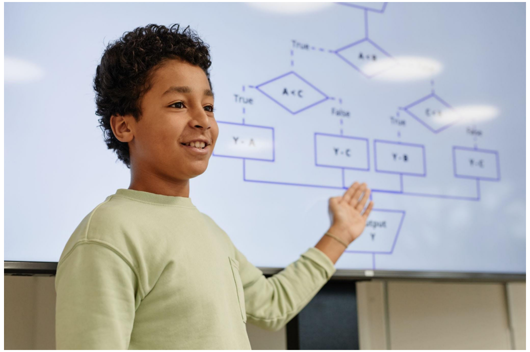
Deliverable #2.1: Measurement Results

- Measure network traffic of 2 IoT devices in groups of 4

- Use IoT devices without a browser-like interface
    a. Examples: camera, audio speaker, light bulb, thermostat
    b. Do not use multi-purpose devices like tablets, phones, laptops

- Use WireShark, TCPdump for capturing traffic.

Deliverable #2.2: Presentation



Content must include:

- **Methodology** used for measurements and analysis
- **Results** from network traffic measurements
- **Observations & Analysis** of measurements and the MUD specification
- **Proposal** for:

  a. Novel uses of MUD for IoT security, **or**

  b. Extensions to the MUD spec to better capture device behavior

Visuals are allowed: Text, graphs, tables, etc.

Forming Groups

You can create the groups on Canvas after the first lecture.

To ensure that everyone in the group can contribute effectively and that the workload is distributed evenly, we suggest that you form groups with members who have similar skills.

We suggest making a brief summary of each group meeting:

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

Deliverable #3: Written Exam

Date: June 23 (in-person, single A4 cheat sheet allowed)

- Multiple-choice and open questions on Remindo platform
- Covers the 9 papers you studied
- You can bring at most 1 A4 page summary of the papers
- Takes about 2 hours
- The written exams will take place on campus, room to be announced.

Assessment

Passing Criteria:

- Your final grade (**G**) must be **5.5 or higher**.
- Calculated as: G=(Written Exam Score×50%)+(Group Project Score×50%)

Additional Constraints:

- **Both** written exam and lab assignment scores **must individually be 5.5 or higher**.
- Submission of summaries for **all 9 papers** is mandatory.
    a. Summaries are **not graded**, but timely submission is essential to pass.

Rounding

As per the UT’s grading policy, we will round your grade G as follows:

If $G \geq 5{,}00$ and $G < 5{,}50$ then $G := 5{,}00$
If $G \geq 5{,}50$ and $G < 6{,}00$ then $G := 6{,}00$
For $n \neq 5$:

- If $G \geq n{,}00$ and $G < n{,}25$ then $G := n{,}00$
- If $G \geq n{,}25$ and $G < n{,}75$ then $G := n{,}50$
- If $G \geq n{,}75$ and $G < (n+1){,}00$ then $G := (n+1){,}00$

Changes from last year’s edition

Increased team size (from 3 to 4)

Removed lab report and introduced presentation talks

The *menu* for today…

- ❖ Welcome & Course Introduction
- ❖ Motivation: Why IoT Security?
- ❖ Course Objectives
- ❖ Course Format & Deliverables
- ❖ Common Pitfalls

Common Pitfalls

- Forgetting to submit summaries or submitting the wrong ones.
- Starting too late with the lab assignment.
- Not testing your measurement setup early on in the process.

Plagiarism and GenAI

- As per the university’s policy on academic misconduct:
  a. No form of plagiarism is tolerated (copy word-to-word, paraphrase, self-plagiarism, accidental plagiarism)
     i. Instead, cite and quote
  b. You may use ChaptGPT, Grammarly or other tools to help you improve the language of your group presentation. The original content MUST however be written by you and your lab group.
     a. As per the same policy, we will consider suspicion of unpermitted or unreported use of AI as potential academic misconduct.

QnA

UNIVERSITY OF TWENTE.

SIDN LABS

QnA

In your lab assignment, you’re expected to interact with MUD profiles in one or more of the following ways:

1. Measure Actual Network Behavior

- Observe and log the traffic of an IoT device under normal operation.
- Analyze:
  - Which protocols/ports are used?
  - Who does the device talk to?
  - Is traffic one-way or bi-directional?

2. Compare with Existing MUD Profile (if any)

- If the device already has a published MUD file, compare its behavior with what's in the profile.
- Look for:
  - Unexpected behavior
  - Deviations from the spec
  - Security implications

QnA

In your lab assignment, you're expected to interact with MUD profiles in one or more of the following ways:

3. Write Your Own MUD Profile

- If no official MUD exists, you can **create one** based on your measurement and analysis.
- Your goal: describe the device's legitimate behavior in MUD format.

4. Propose Extensions or Novel Uses

- Suggest ways the MUD framework could be extended to:
  - Support new device types
  - Improve IoT security
  - Capture more complex behaviors