Lecture #3: Principles of IoT Security

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

University of Twente | Friday May 9, 2025

UNIVERSITY OF TWENTE.

SIDN LABS

Your teachers today

Antonia Affinito
(teacher)

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

UNIVERSITY OF TWENTE.

SDN LABS

Today's agenda

- Admin
- Introduction to today's lecture
- IoT Overview
- Vulnerabilities, Threats, Risks
- Case Study and Discussion
- Common IoT Attacks

Admin

UNIVERSITY OF TWENTE.

SDN LABS

Lab Assignment

Have you joined a group for the lab assignment?

A. ✅ Yes? Make sure your group is registered in Canvas.

B. ❓ Still looking for a group?

   i. Use the discussion post on Canvas

   ii. Contact students who are not yet in a group

Deadline: May 12 2025

Lab Assignment: Devices

- Do you **need IoT devices** for your lab assignment?
  - Yes: Please reach out via email to our TAs (Pascal Huppert, Ting-Han Chen, Etienne Khan).

  - Can we use Raspberry Pis and ESP32s? **No**
    - They are user-defined, lack inherent cloud connectivity, and rely on installed software. As general-purpose devices, they cannot be studied like IoT things.
    - Just as you wouldn't study a desktop computer or smartphone.

Examples of suitable devices are light bulbs, audio speakers, doorbells, and light switches

Lab Assignment: Devices

Email addresses:

- pascal.huppert@utwente.nl
- e.khan@utwente.nl
- t.h.chen@utwente.nl

Important dates

- Two paper summaries per lecture: **before every lecture at 7 AM CEST**
- Lab assignment - required files, including presentations: **Wed Jun 25, 9 AM CEST**
- Written exam: **June 23, 15:45-17:30**
- Lab groups of 4 people: **May 12, EOB**

- Group Presentations: **June 27 (8:45 – 12:30), June 30 (8:45-12:30)**

UNIVERSITY OF TWENTE.

SDN LABS

Deliverable #1: 9 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 bring a single printed A4 with notes to the exam**

- 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

Schedule

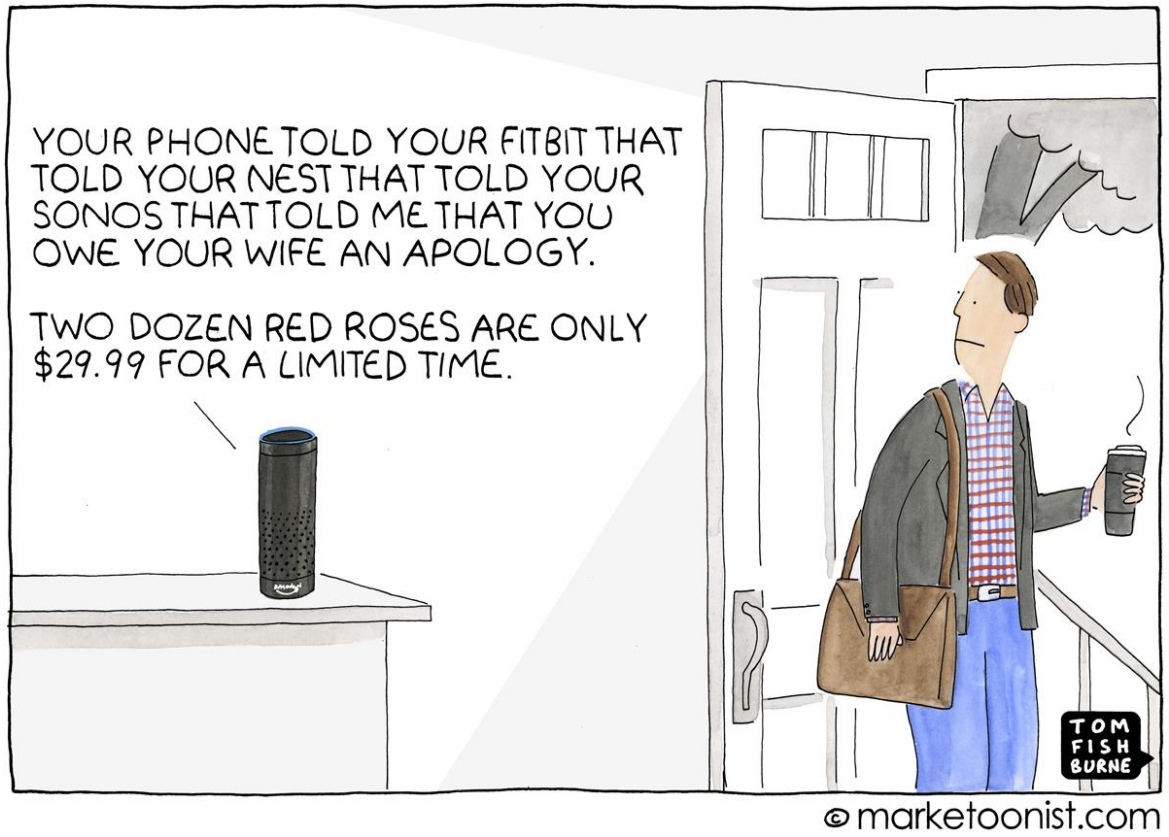
Lecture	Date	Contents
R1	Apr 25	Course introduction
G1	Apr 30	How the core of the Internet works (recorded)
R2	**May 9**	**Principles of IoT Security**
R3	May 16	Internet Core Protocols
R4	May 23	IoT Botnet Measurements
R5	May 27	IoTLS and Q&A Group Assignment
G2	Jun 6	Guest Lecture – PQC in IoT
R6	Jun 13	IoT Security Vulnerabilities
R7	Jun 20	IoT Forensic

Today's learning objective

- After the lecture, you will be able to explain and discuss the key concepts of IoT security.
- Contributes to SSI learning goal #1: "Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF"

Introduction to today's lecture

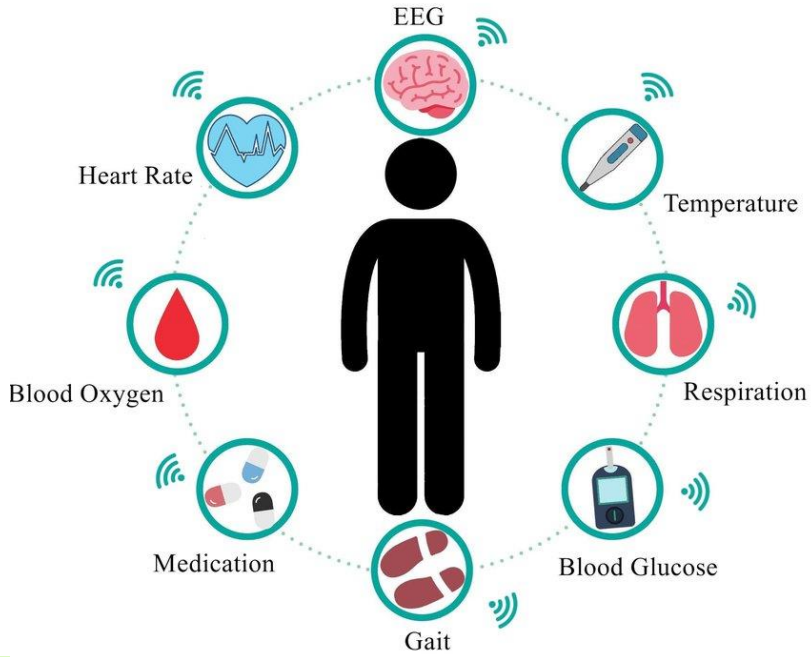
The Internet of Things



"An IoT is a network that connects uniquely identifiable "things" to the Internet. The "things" have sensing/actuation and potential programmability capabilities. Through the exploitation of the unique identification and sensing, information about the "thing" can be collected and the state of the "thing" can be changed from anywhere, anytime, by anything."
IEEE's description

UNIVERSITY OF TWENTE. SDN LABS

Examples of The Internet of Things



UNIVERSITY OF TWENTE.

SDN LABS

What is a “Thing”?

An object, either physical or virtual, which is capable of being identified and integrated into communication networks.

Physical

Smart Light Bulb (Device)

Virtual

AWS IoT Thing Shadow

The S in IoT stands for security

Tim Kadlec

UNIVERSITY OF TWENTE.
SIDN LABS

Why Secure The Internet of Things?

Any IoT Device Can Be Hacked, Even Grills

potential exploitation. For people who take grilling seriously, they now face the possibility of a ruined cookout — not because they picked the wrong cut of meat or didn't pay close enough attention to maintaining the ideal temperature, but because their grill was hacked.

UNIVERSITY OF TWENTE.

SDN LABS

Why Secure The Internet of Things?

Any IoT Device Can Be Hacked, Even Grills

potential exploitation. For people who take grilling seriously, they now face the possibility of a ruined cookout — not because they picked the wrong cut of meat or didn't pay close enough attention to maintaining the ideal temperature, but because their grill was hacked.

Hackers can Steal Your Identity and Bank Details from a Coffee Machine

Smart coffee machines that are connected to the internet using special apps could be targeted by hackers to steal their owner's bank or card details.

Vince Steckler, chief executive of security giant Avast, said, smart coffee machines allow owners to control them remotely using their phones. Users can even give the machines vocal commands if they are connected to virtual assistant software such as Amazon's Alexa.

"Coffee machines are not designed for security. They are additional vectors to get into your network. And you can't protect them," Steckler said in a media statement.

UNIVERSITY OF TWENTE.

SDN LABS

Why Secure The Internet of Things?

Any IoT Device Can Be Hacked, Even Grills

potential exploitation. For people who take grilling seriously, they now face the possibility of a ruined cookout — not because they picked the wrong cut of meat or didn't pay close enough attention to maintaining the ideal temperature, but because their grill was hacked.

Hackers can Steal Your Identity and Bank Details from a Coffee Machine

Smart coffee machines that are connected to the internet using special apps could be targeted by hackers to steal their owner's bank or card details.

Vince Steckler, chief executive of security giant Avast, said, smart coffee machines allow owners to control them remotely using their phones. Users can even give the machines vocal commands if they are connected to virtual assistant software such as Amazon's Alexa.

"Coffee machines are not designed for security. They are additional vectors to get into your network. And you can't protect them," Steckler said in a media statement.

Security News This Week: An IoT Teddy Bear Leaked Millions of Parent and Child Voice Recordings

UNIVERSITY OF TWENTE. SDN LABS

Key Components of IoT Hardware

- **Microcontroller Units (MCUs)**: Integrated circuits that contain a processor, ROM and RAM.
- **Sensors**: Devices that detect physical properties (temperature, humidity, motion)
- **Actuators**: Devices that take action based on commands (motors, relays)
- **Communication Modules**: Provide connectivity (Wi-Fi, Bluetooth, ZigBee, LoRa, Cellular)

Key Components of IoT Hardware

Memory Resources are frequently **limited** in the IoT devices

- **Mirai** botnet **exploited** the memory resource **limitations** of IoT devices as part of its **attack strategy**.

- Many IoT devices do not have enough memory to store detailed security logs, making it **difficult** for administrators to detect Mirai's presence or understand how it spread.

UNIVERSITY OF TWENTE.

SDN LABS

IoT Operating Systems

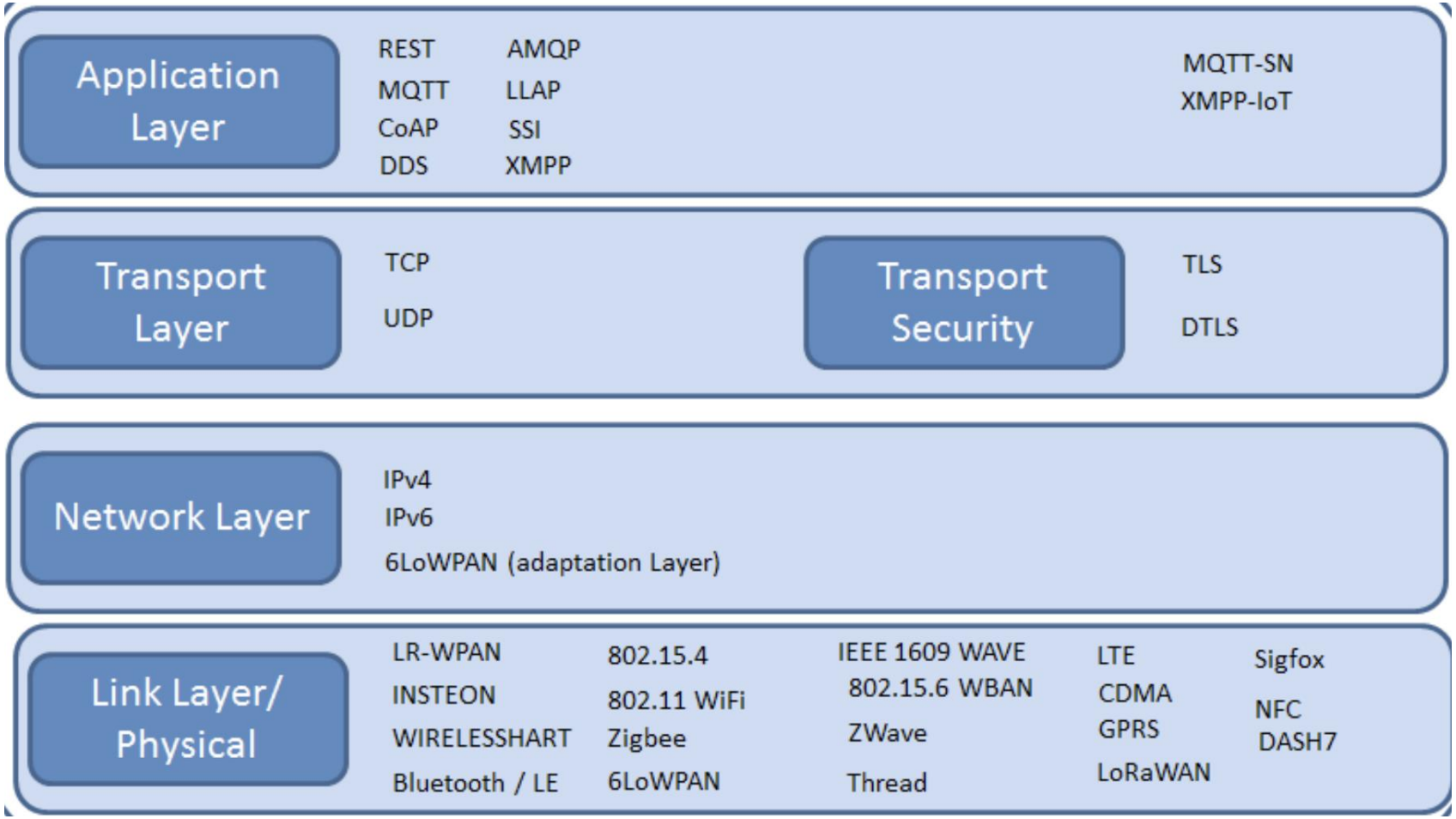
Types of IoT Operating Systems:

- **Real-Time Operating Systems (RTOS)**: Fast, predictable response for critical tasks (e.g., FreeRTOS, LynxOS).
- **Lightweight Embedded OS**: Optimized for low-power devices (e.g., TinyOS, Contiki).
- **General Purpose OS**: Full-featured, capable of complex tasks (e.g., Embedded Linux, Ubuntu Core).

Key Factors for Choosing an OS:

- Performance and resource efficiency.
- Security (process isolation, secure boot, cryptography).
- Hardware compatibility (CPU architecture, memory).

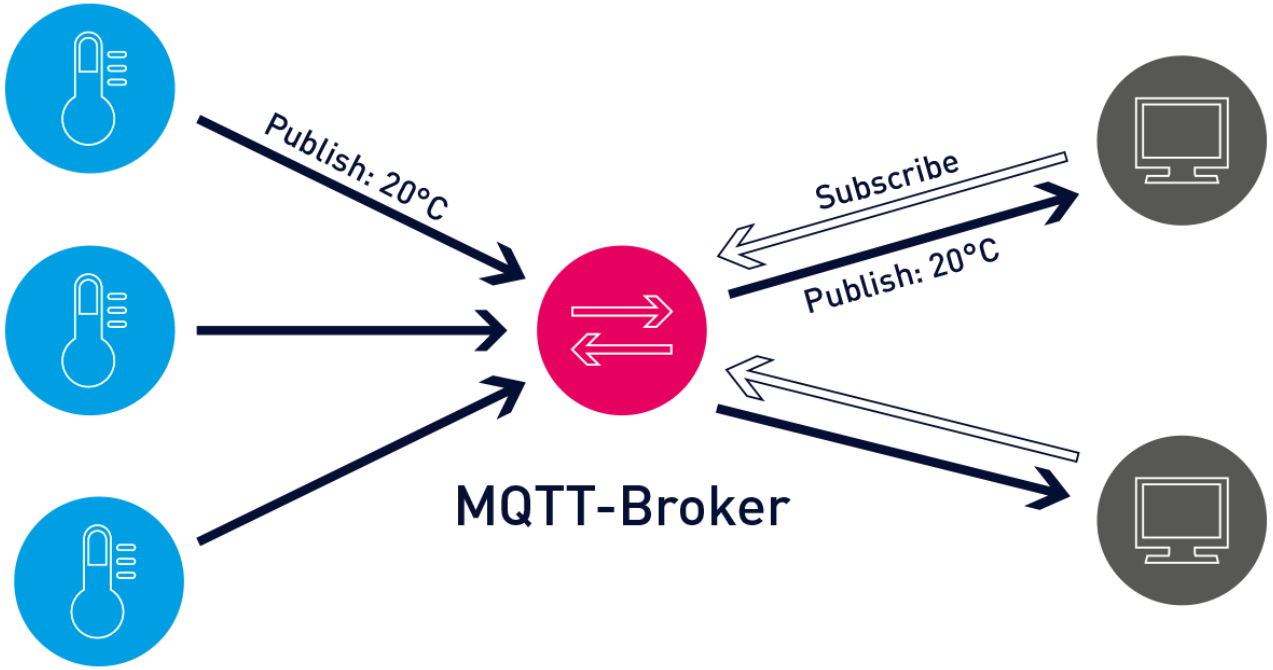
IoT Communications



UNIVERSITY OF TWENTE.

SDN LABS

MQTT (Message Queuing Telemetry Transport)



- One of the **most widely used** protocols for IoT
- Lightweight, **publish/subscribe** messaging protocol designed for efficient communication between devices in low-bandwidth, high-latency, or intermittently connected networks

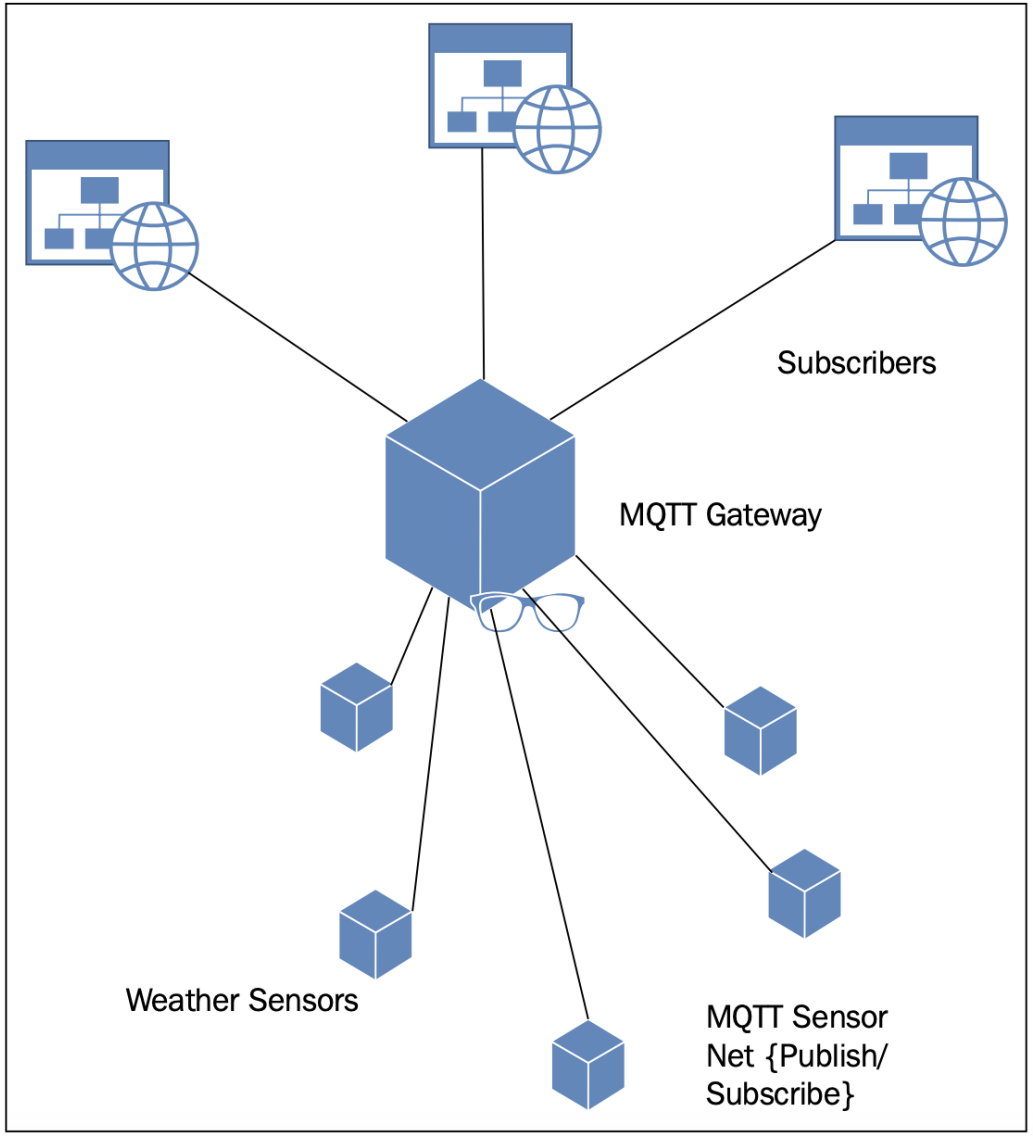
Source: https://www.paessler.com/it-explained/mqtt

UNIVERSITY OF TWENTE. SDN LABS

MQTT Publish/Subscribe Model

Publishers (Weather Sensors) send messages to a central **Broker** with a specific topic (e.g., weather/temperature). The Broker manages these messages.

Subscribers receive messages from the Broker if they have subscribed to the relevant topic.



UNIVERSITY OF TWENTE.

SDN LABS

MQTT Publish/Subscribe Model

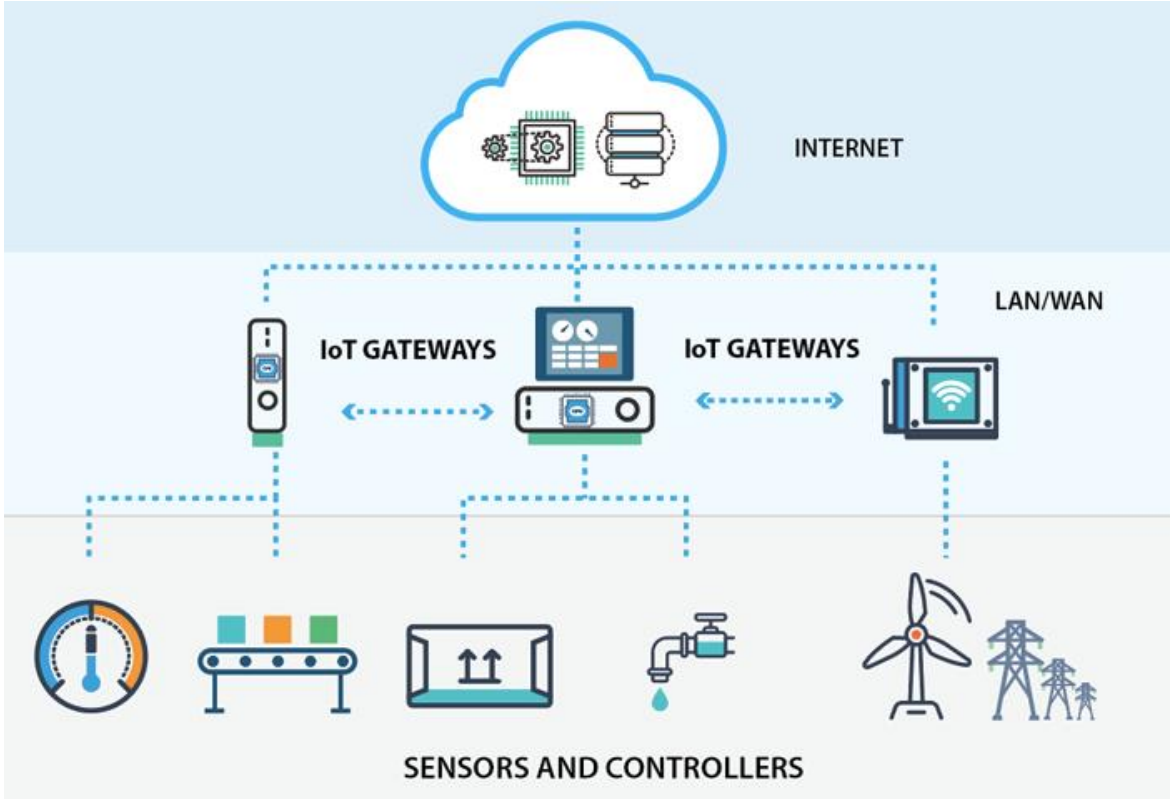
Advantages:

- Low Traffic and Latency
- Suitable for pushing and pulling application

Disadvantages:

- Can be blocked by firewall!
- Require an intermediate broker.

IoT Gateway



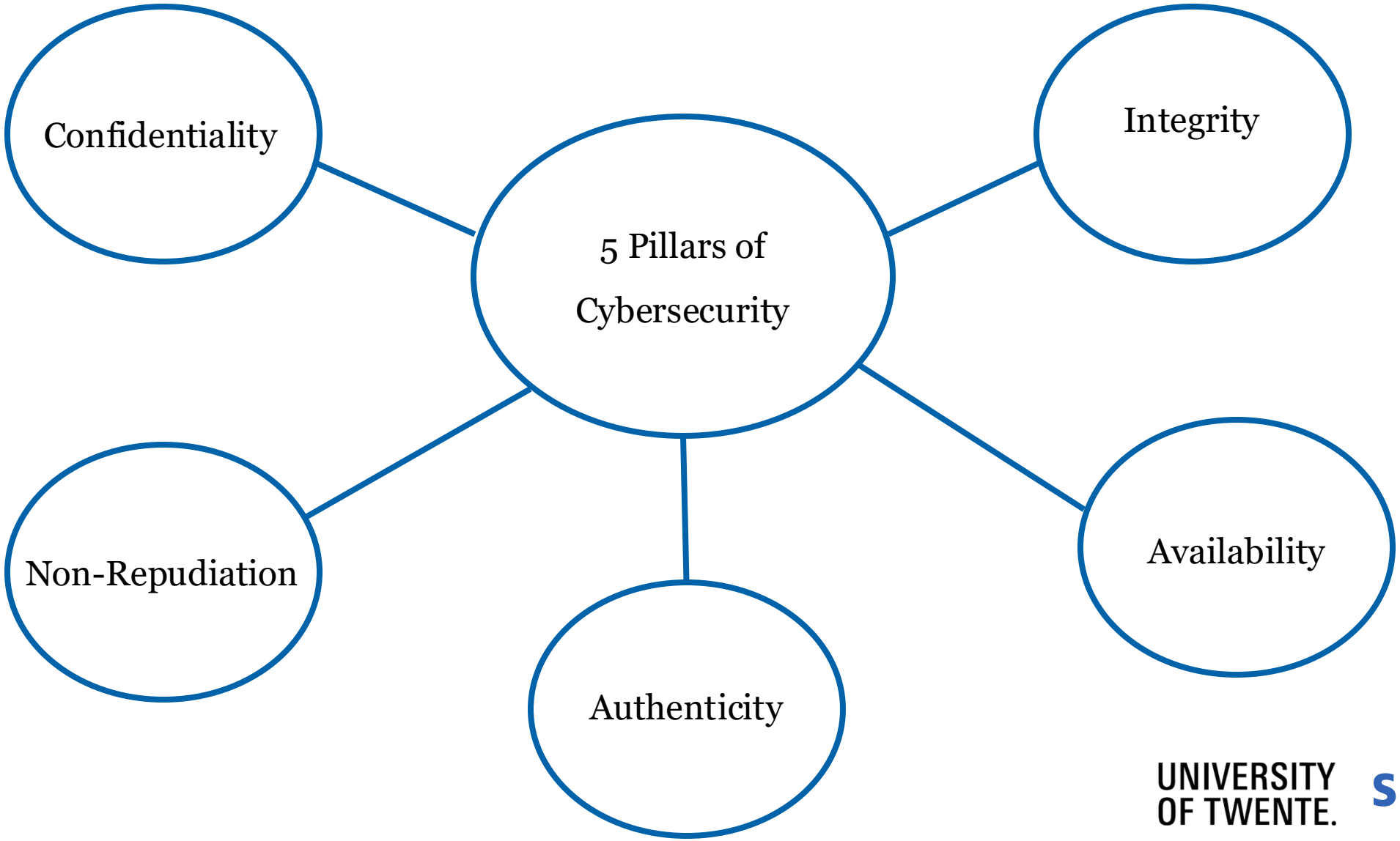
An IoT Gateway is a device that connects IoT devices to a network or cloud services.

It acts as an **intermediary**, **translating** communication protocols (e.g., MQTT, ZigBee) between IoT devices and the backend systems.

UNIVERSITY OF TWENTE.

SDN LABS

Pillars of Security



Threats, Vulnerabilities and Risks

Group Discussion

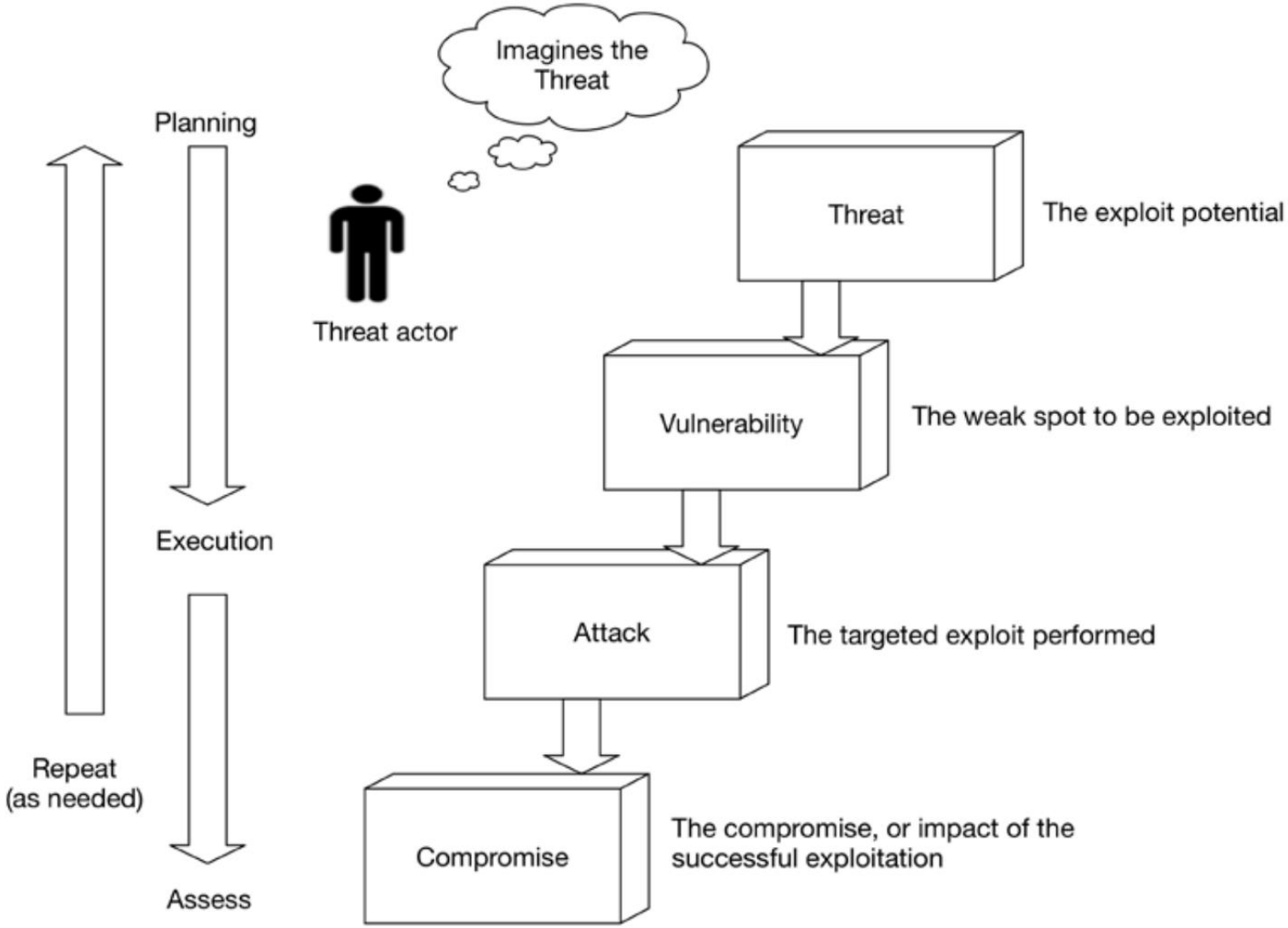
Group Discussion (8 minutes) in groups of four.

An IoT-enabled smart lock system is used in a residential building. An attacker uses a known vulnerability in the lock's firmware to remotely unlock doors, gaining access to private apartments

Your Tasks:

1. Identify threats, vulnerabilities and risks
2. Which scenario do you consider the most dangerous, and why?
3. If you're the manager/engineer, what would you do to prevent this?

Threat-Vulnerability-Risk. How does an IoT attack occur?



UNIVERSITY OF TWENTE.

SDN LABS

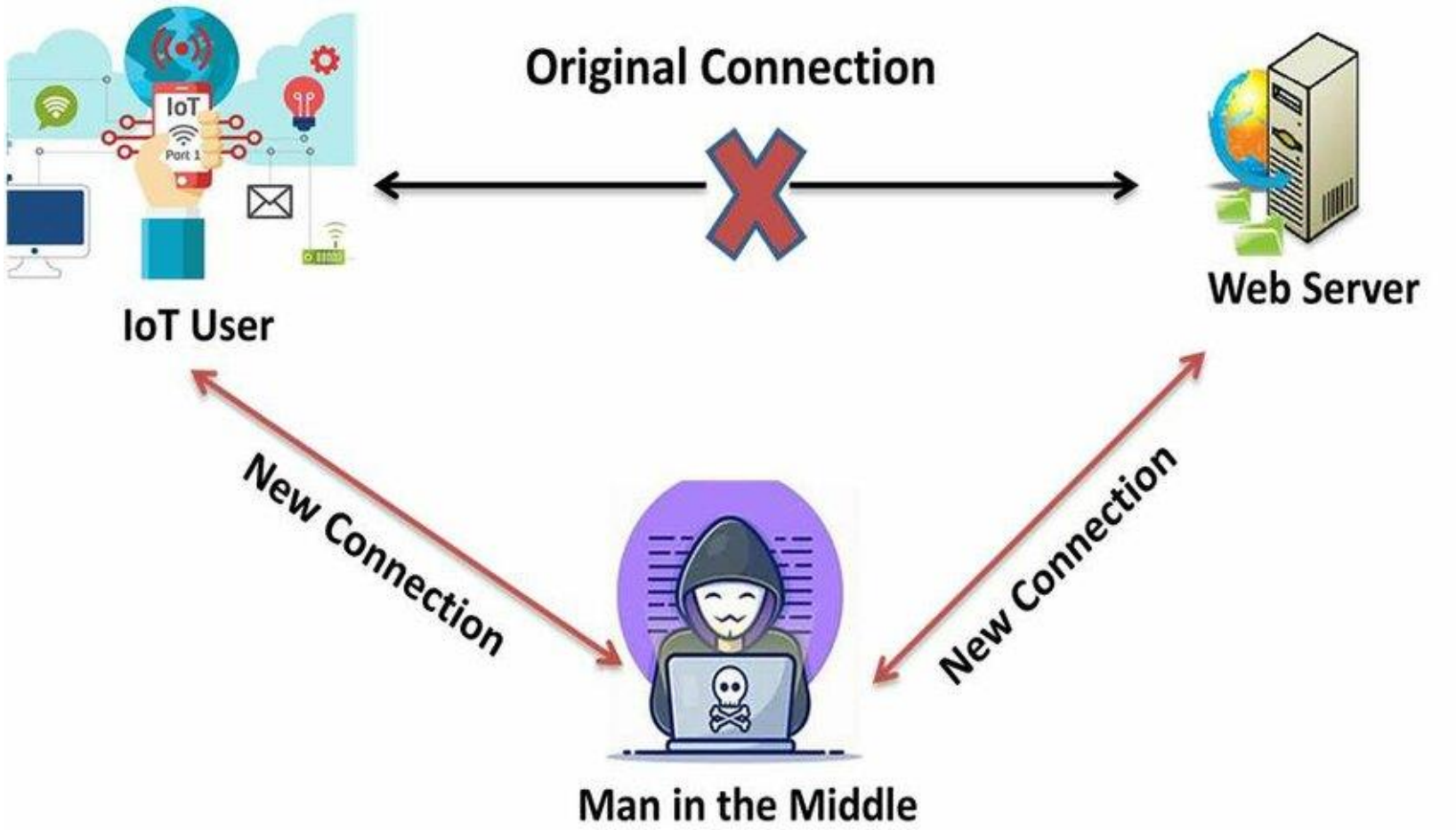
How an IoT Attack Occurs

1. **Discovery**: Attackers scan for exposed IoT devices (Shodan, Nmap).
2. **Access**: Exploit weak passwords, unpatched vulnerabilities, or unsecured interfaces.
3. **Control**: Deploy malware, hijack firmware, or manipulate device settings.
4. **Persistence**: Maintain control using backdoors or altered startup configurations.
5. **Execution**: Launch DDoS, steal data, or use the device for further attacks.

Common IoT Attack Types

- **Wireless scanning and mapping attacks**
  - Attacks that target the discovery and mapping of IoT devices through wireless protocols (Wi-Fi, Bluetooth, ZigBee).
- **Security Protocol Attacks**
  - Exploiting weaknesses in the security protocols used by IoT devices.
- **Physical Security Attacks**
  - Gaining unauthorized physical access to IoT devices.
- **Denial of Service (DoS) Attacks**
  - Overwhelming an IoT device or network with excessive requests, making it unavailable
- **Man-in-the-Middle (MITM) Attacks**
  - Intercepting and altering communication between IoT devices and their controllers.

Man-in-the-middle Attack



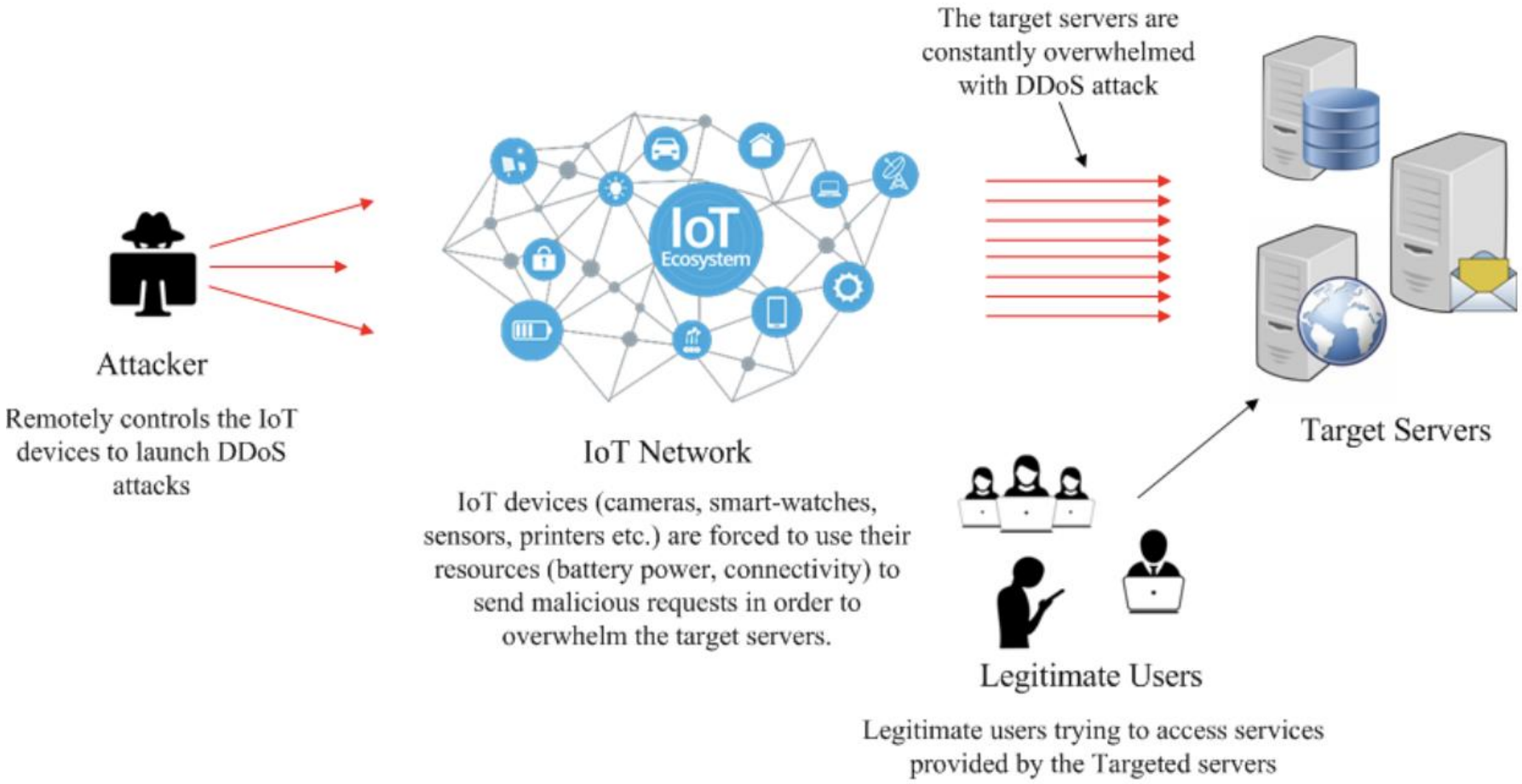
Source: https://www.researchgate.net/figure/Man-in-the-Middle-Attack_fig1_362068050

- ” Security Vulnerabilities in LoRaWAN”

UNIVERSITY OF TWENTE.

SDN LABS

A DDoS attack scenario in IoT networks



Source: https://www.mdpi.com/14248220/22/3/1094

- ” Understanding the Mirai Botnet”
- “Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet”

UNIVERSITY OF TWENTE.

SDN LABS

Today's learning objective revisited

- After the lecture, you will be able to explain and discuss key concepts of IoT security

- Limited technical depth, but important to "set the scene" for more technical papers later in the course

- Contributes to SSI learning goal #1: "Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF"

Next regular lecture:

Friday May 16, 08:45-10:30

Topic: Internet Core Protocols (DNSIoT, IPv6)

Dr. Antonia Affinito | a.affinito@utwente.nl
Prof. Cristian Hesselman | c.e.w.hesselman@utwente.nl

UNIVERSITY OF TWENTE.

SIDN LABS