OTH REGENSBURG

SEPP 4.0 - Evaluation of Hands-On IoT-Security Exercises

Louis Ebneth, Sebastian Fischer

Ostbayerische Technische Hochschule Regensburg

CROSS-SEC 2026 - April 19 to April 23, 2026 - Lisbon, Portugal

Prof. Dr. Sebastian Fischer

since 2023	Professor for "Computer Science and System Security" at OTH Regensburg, Germany
2021 - 2023	Lecturer at OTH Regensburg, Germany
2022	Dr. rer. nat. at Freie Universität Berlin, Germany
2018 - 2021	Research Associate at Fraunhofer AISEC, Germany
2015 - 2018	Research Associate at OTH Regensburg, Germany
2015	M. Sc. Applied Research in Computer Science, OTH Regensburg
2013	B. Sc. Computer Science, OTH Regensburg

sebastian.fischer@oth-regensburg.de

Contents

- Background
- SEPP Platform
- Example Exercise
- Evaluation Results
- Conclusion and Outlook

Background

- A lot of insecure IoT devices (like Smart Home devices)
- IoT Security Lecture at the Technical University of Regensburg
  - Basics of IoT Security
  - Security analysis of IoT device -> students “hack” their own device
  - Hands-on learning experience
- Problem: every device is different, but they should try all the “hacking” methods

SEPP Platform

SEPP Platform

- Weekly exercise session of 90 minutes that accompanies the IoT Security lecture
- Multiple groups of 2-3 students work on the same exercise sheet
- Evaluation of the exercises through observations and student questionnaires

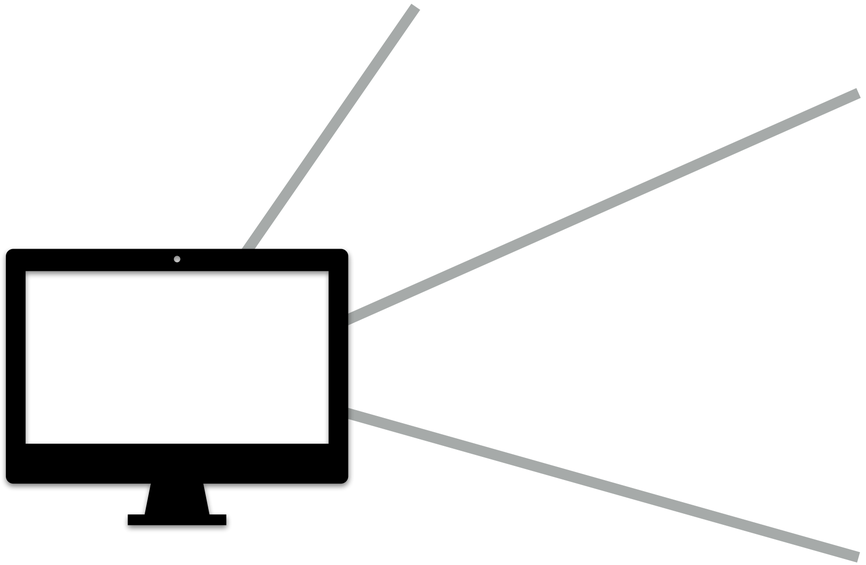
SEPP Platform: Exemplary Attacks

- Identifying devices on the network using Nmap
- Replay attack
- Address Resolution Protocol (ARP) spoofing based Man-in-the-Middle attack
- Denial of Service / Distributed Denial of Service
- Brute Force attack
- Session Hijacking attack
- Bluetooth Low Energy Sniffing

OTH REGENSBURG

Example Exercise

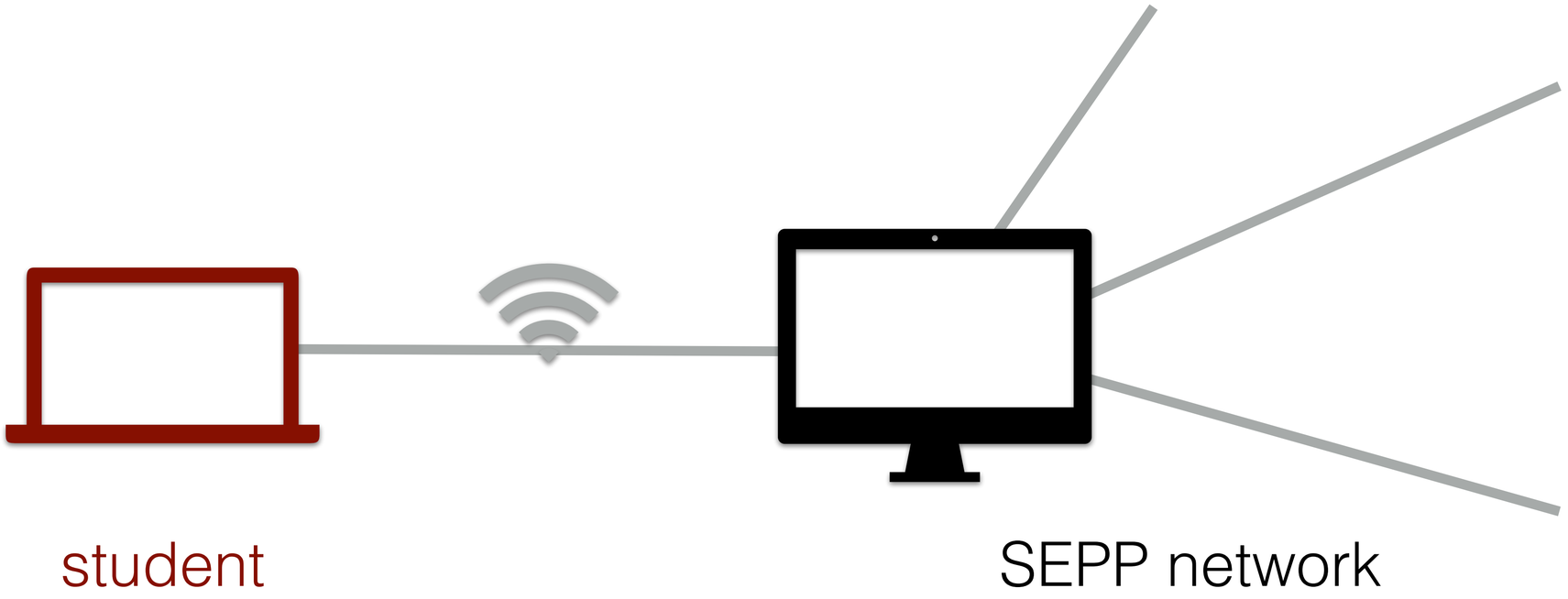
student



SEPP network

OTH REGENSBURG

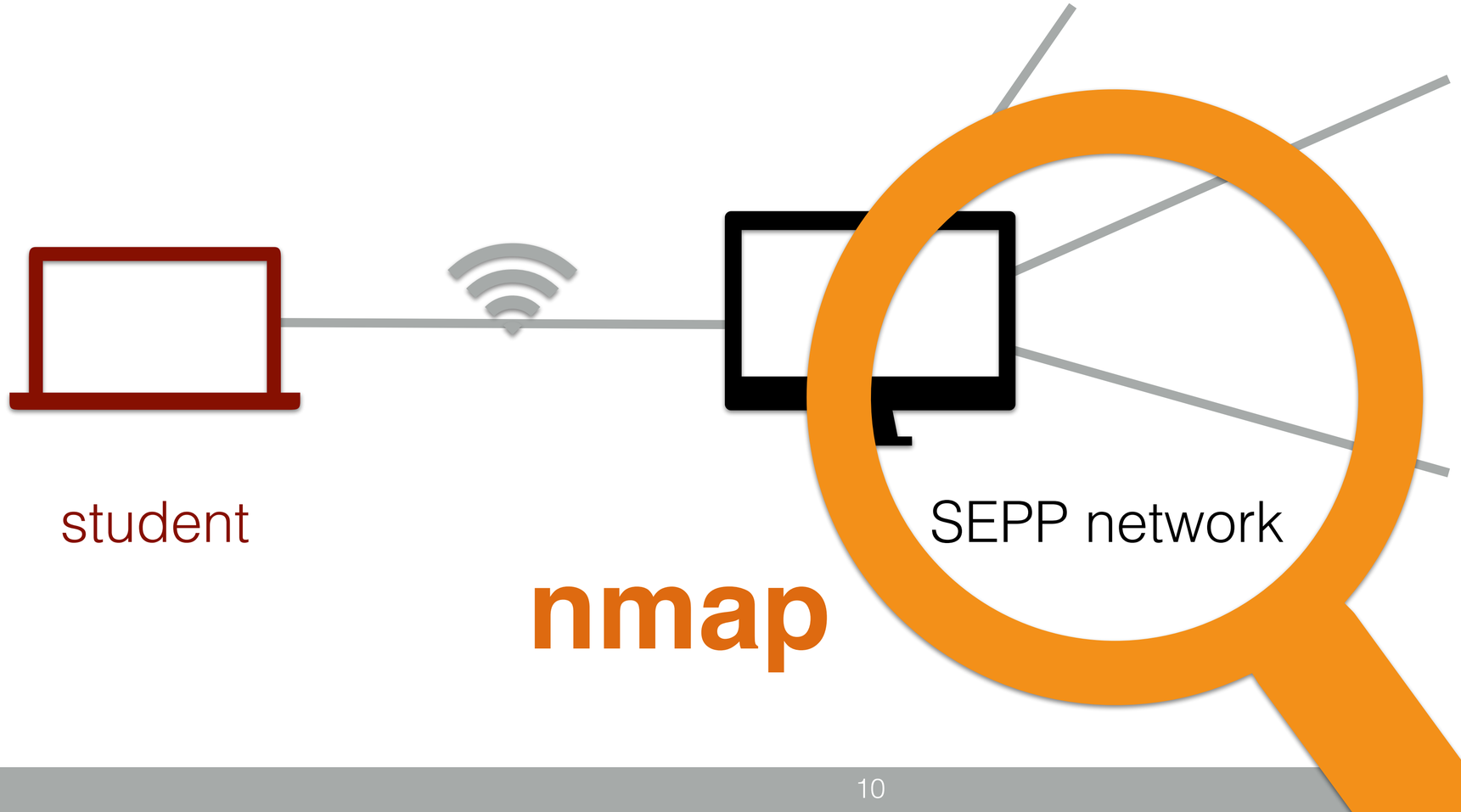
Connect to network



OTH REGENSBURG

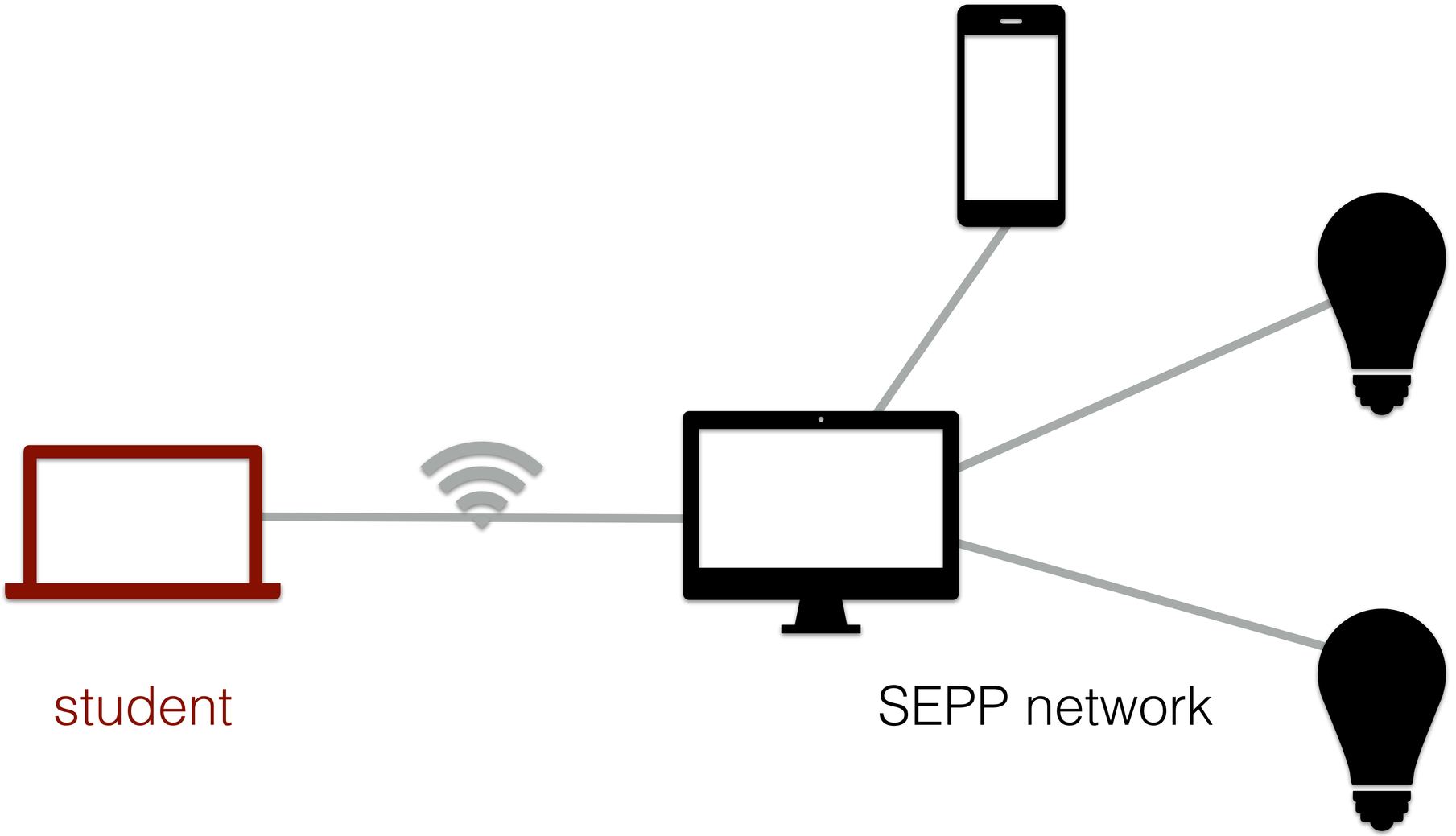
Network scan with nmap

```
nmap -sn <IP adress range>
```



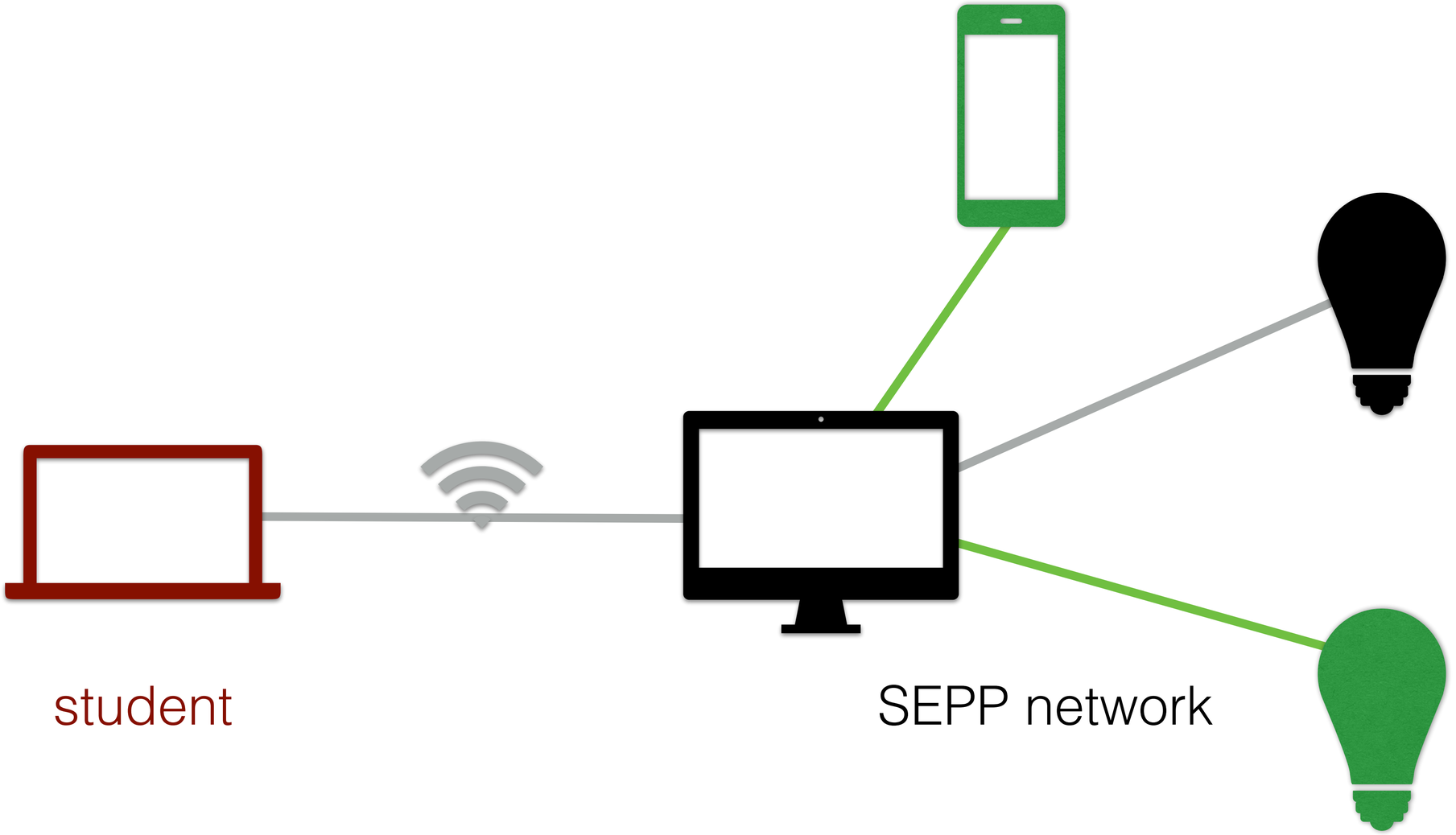
OTH REGENSBURG

SEPP network



OTH REGENSBURG

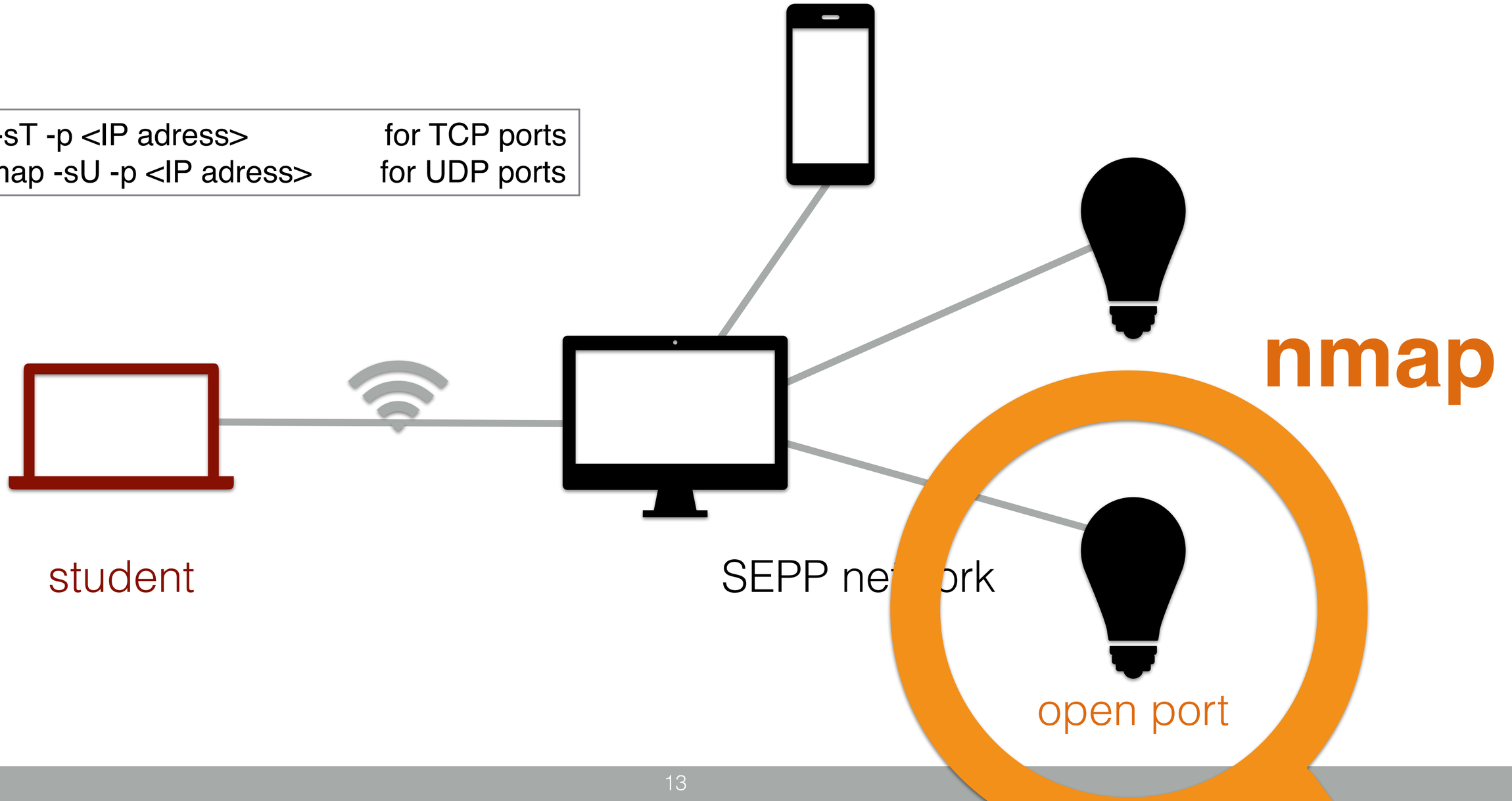
Normal communication with device



OTH REGENSBURG

Device scan for open ports (TCP / UPD)

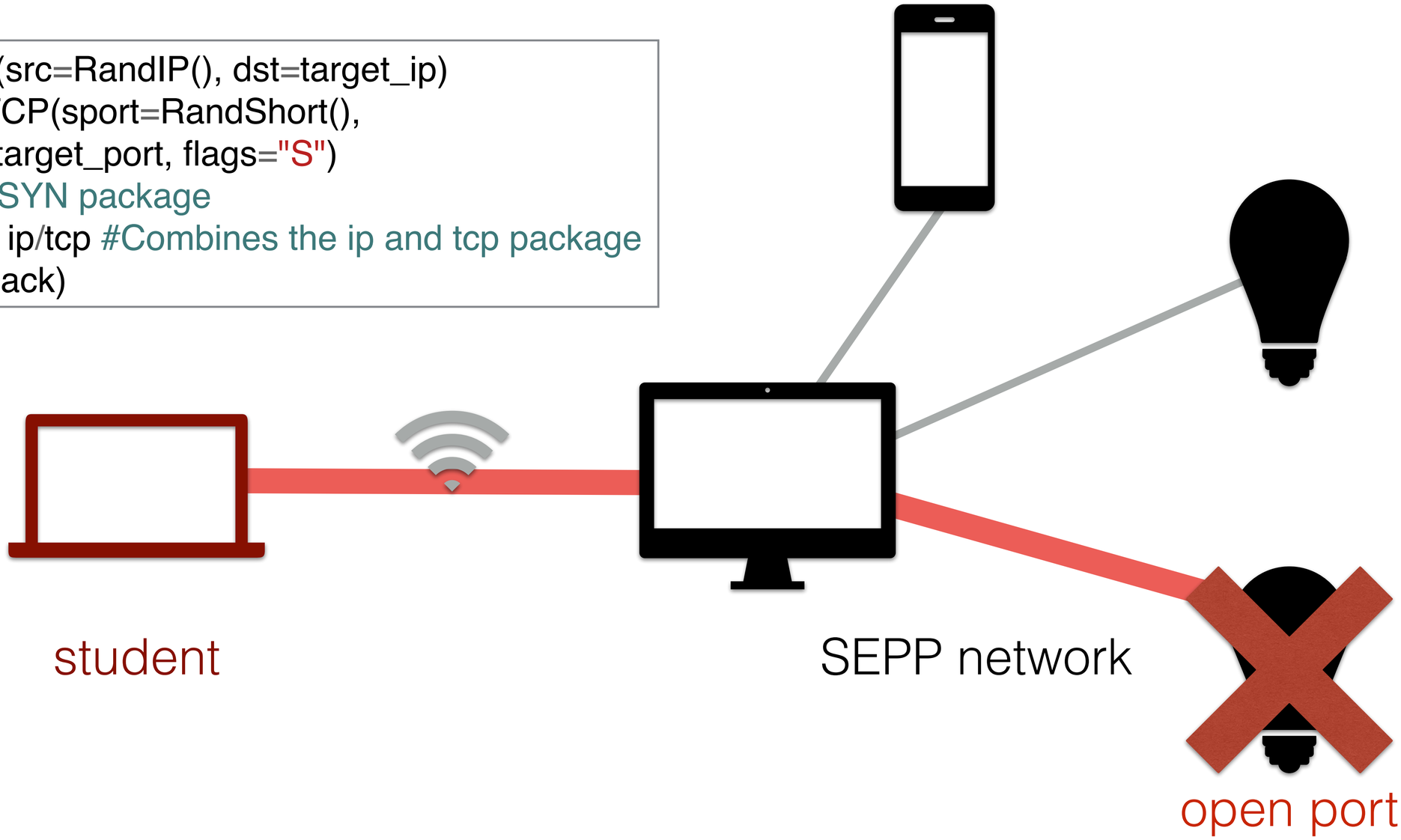
nmap -sT -p <IP adress>	for TCP ports
and nmap -sU -p <IP adress>	for UDP ports



OTH REGENSBURG

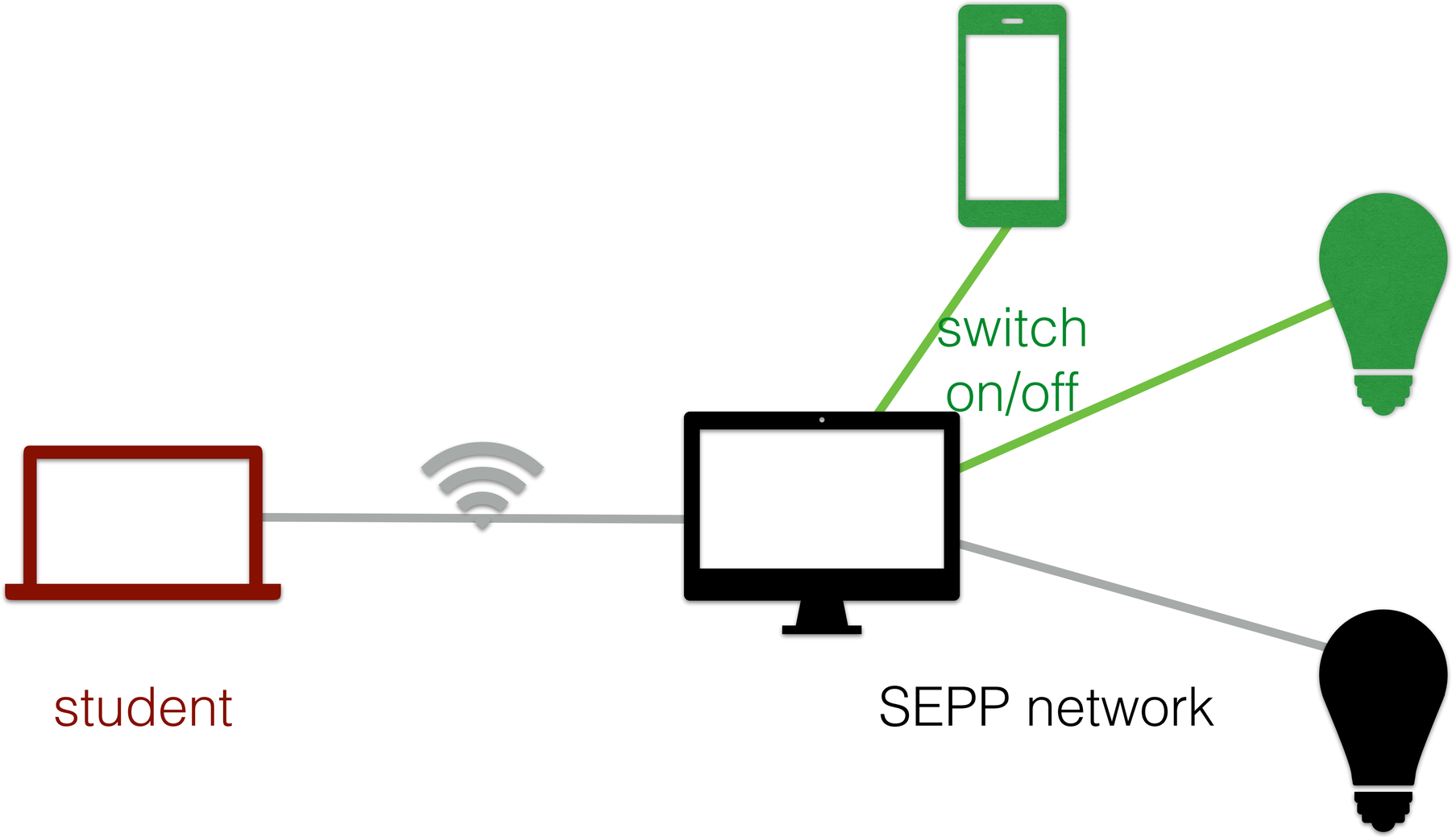
DoS attack with Scapy (Python)

```
ip = IP(src=RandIP(), dst=target_ip)
tcp = TCP(sport=RandShort(),
dport=target_port, flags="S")
#S for SYN package
pack = ip/tcp #Combines the ip and tcp package
send(pack)
```



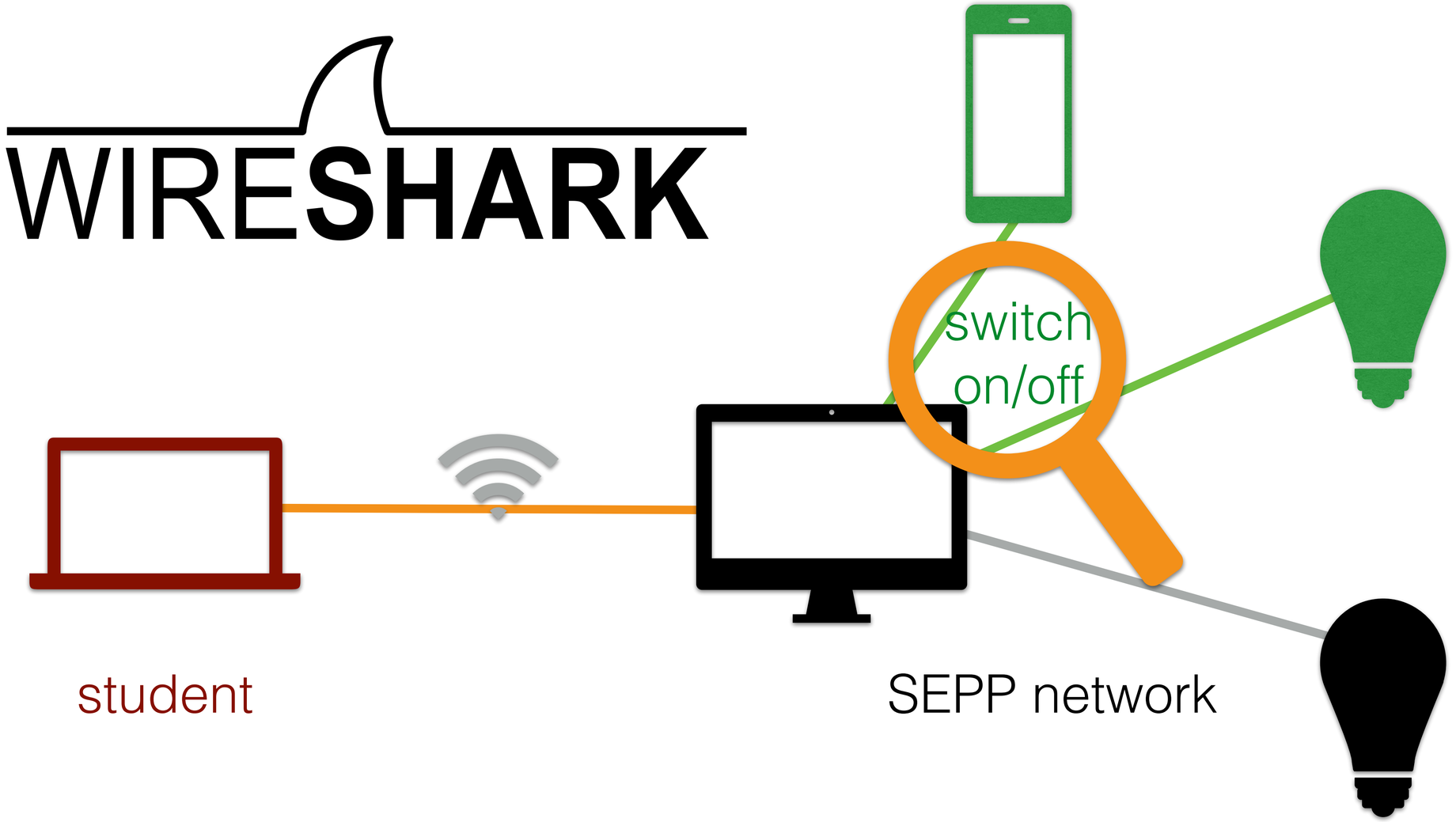
OTH REGENSBURG

Normal communication with device



OTH REGENSBURG

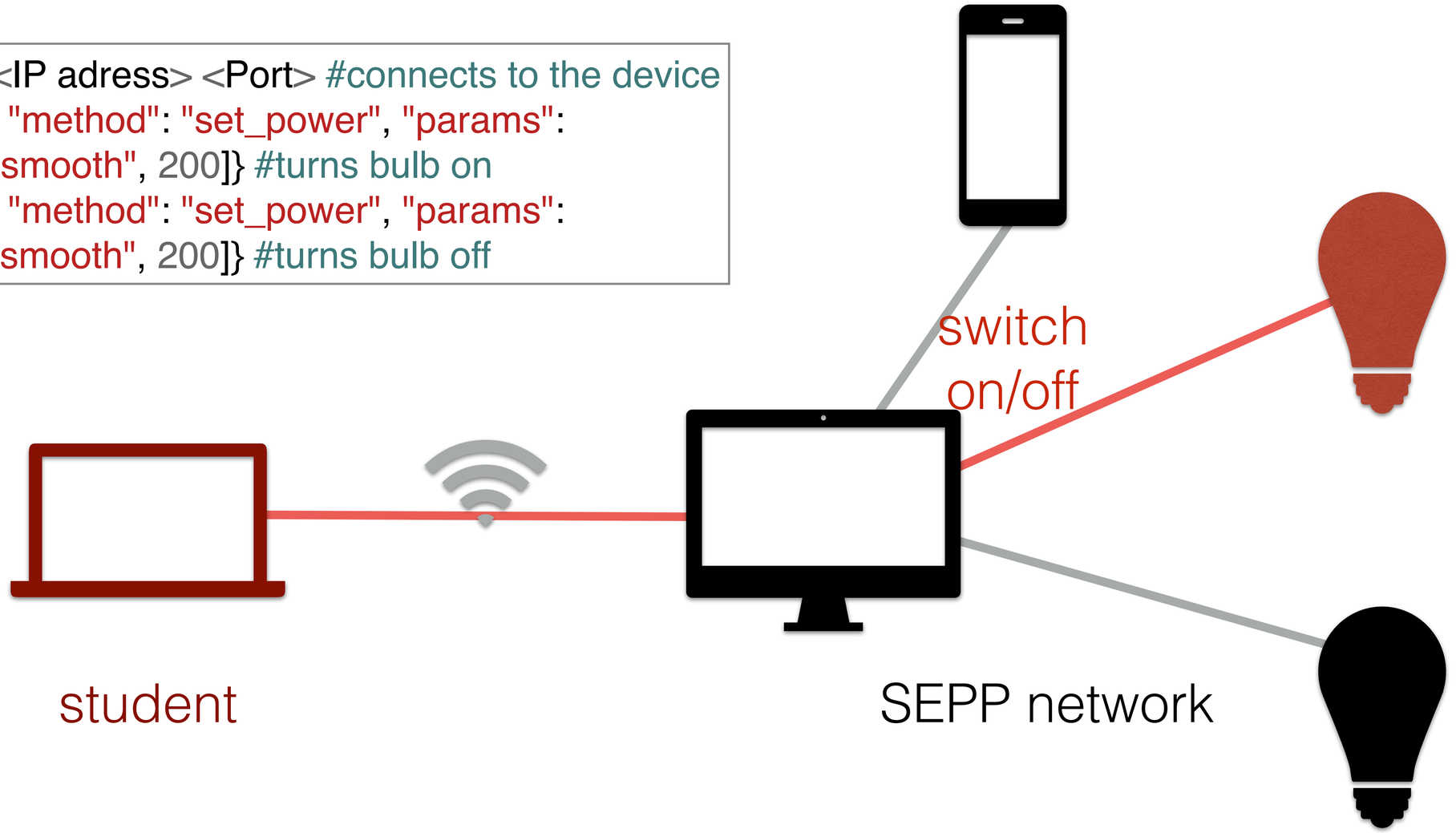
Capture communication with Wireshark



OTH REGENSBURG

Send command via telnet

```
telnet <IP adress> <Port> #connects to the device
{"id":0, "method": "set_power", "params":
["on", "smooth", 200]} #turns bulb on
{"id":0, "method": "set_power", "params":
["off", "smooth", 200]} #turns bulb off
```



Evaluation Results

Generally positive feedback

+ High student engagement
+ Clear benefits from working with real IoT devices in a Hands-On approach
+ Ability to apply the knowledge learned in the lecture
+ Surprised by the simplicity of certain attacks (e.g. DoS, Man-in-the-Middle)
+ … and tools used to collect the necessary information (e.g. Nmap, Wireshark)

Evaluation Results: Areas of Concern

1) Device Choice:

   - Not all devices provided clear feedback if an attack was successful

   - Unintentional DoS scenario on some devices due to multiple groups sending commands at the same time

2) Repetition of attacks:

   - Performing a DoS attack was part of four of the ten exercises

3) Arrangement within the semester:

   - Tools and vulnerabilities were included on exercise sheets before they were introduced in the lecture

Evaluation Results: Areas of Concern

4) Instructions and guidance:

   - Errors / Incompleteness of the instructions on some exercise sheets
   - Often no guidance or examples for tools that were not introduced in the lecture

5) Understanding:

   - The security relevancy of all steps was not always apparent

6) Preparation of the exercise sessions:

   - Provide clear instructions on how the exercise needs to be prepared

Evaluation Results: Areas of Concern

7) Wi-Fi issues:

- Raspberry Pi is not suitable as router, as it can not handle the desired number of clients

8) Timely constraints:

- Students should be provided with ready-to-go laptops and phones that have all necessary tools installed
- Files like Python scripts should be distributed efficiently (e.g. via Git)
- Students should not waste time on unnecessary steps (e.g. full Nmap UDP port scan)

Conclusion and Outlook

The SEPP platform is a promising and well-received tool

- Eliminate areas of concern
- Ongoing evaluation and improvements
- More platforms needed for more parallel groups
    - we are trying to get a founding Add another setup

Contact

- **Prof. Dr. Sebastian Fischer**
- Computer Science and System Security
- Ostbayerische Technische Hochschule Regensburg, Germany

- sebastian.fischer@oth-regensburg.de

References

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010, Retrieved: 2026.02.18, ISSN: 1389-1286. DOI: https:/ /doi.org/10.1016/j.comnet.2010.05.010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128610001568.

[2] R. H. Weber, “Internet of Things – New security and privacy challenges,” Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, 2010, Retrieved: 2026.02.18, ISSN: 2212-473X. DOI: https:/ /doi.org/10.1016/j.clsr.2009.11.008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364909001939.

[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015, Retrieved: 2026.02.18, ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2014.11.008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128614003971.

[4] D. Hauser, J. Graf, S. Fischer, and R. Hackenberg, “SEPP: Security Education and Penetration-Testing Platform for IoT,” in Proceedings of The European Conference on Education 2025, Retrieved: 2026.02.18, 2025, pp. 443–453. DOI: https://doi.org/10.22492/issn.2188-1162.2025.36.

[5] D. Hauser and S. Fischer, “SEPP 2.0 - Advanced IoT Hacking Scenarios for Hands-on Security Education,” 2025, Unpublished.

[6] I. Edelmann, “IoT Vulnerabilities: Evaluation and Improvement of the Exercises,” Unpublished bachelor’s thesis, 2025.

[7] L. Herrmansdörfer, “Evaluation and Analysis of Cyber-Security Challenges in Relation to the Internet of Things,” Unpublished bachelor’s thesis, 2025.