

Building a Secure Home Network

By Shay Friel
Computer Networks & Cybersecurity

1. Introduction

Cybersecurity is protecting all computers, networks, data and programs across the world from unauthorised access and cyberattacks. New attacks and threats are made every day by malicious hackers, they can vary from small but harmful attacks such as someone trying to steal your Facebook password, to national level cyberwarfare between governments. This project focuses on deploying cyberattacks against a home network, displaying the vulnerabilities when not maintaining network security and providing solutions to prevent threats/risks and attacks. Two different cyberattacks will be used to penetrate the network, a Phishing attack and a Man-in-the-Middle ARP spoofing attack. Both attacks will be conducted in Kali Linux operating system and used against all devices on the network.

5. Man-in-the-Middle ARP Spoofing

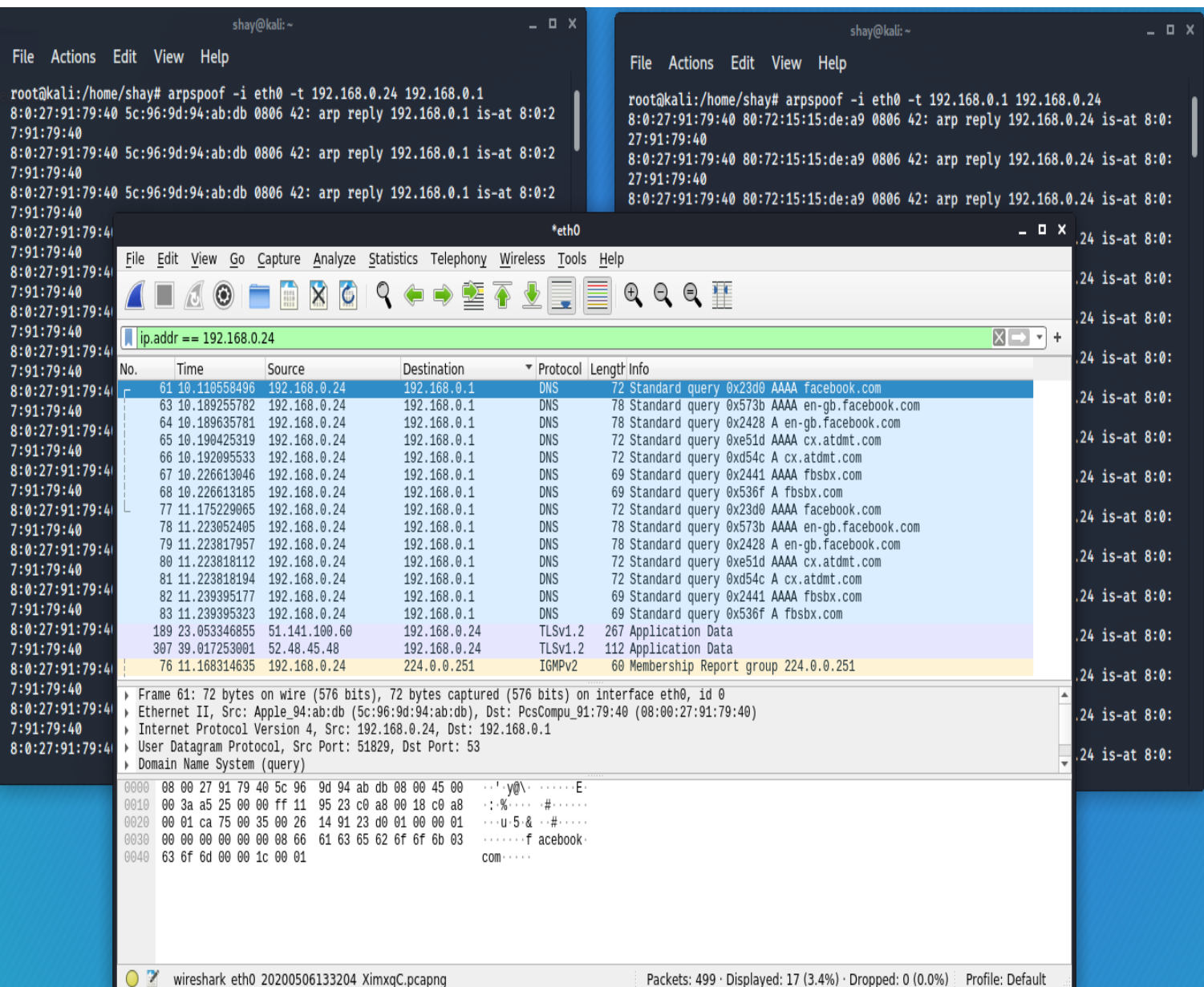


Figure 2: Shows results of sniffing and capturing packets from the target device using Wireshark

2. Aims & Objectives

Aim:

The aim of this project is to build a home network and attempt to penetrate the network through a series of experiments with different cyberattacks in order to identify the vulnerabilities and provide the solutions to maintain a secure network.

Objectives:

- Literature review of books, articles and journals on network vulnerabilities and security
- Investigate threats/vulnerabilities and cyberattacks
- Design and implement a home network
- Carry out experiments on the network using penetration testing software and hardware
- Analyse the results and findings and provide solutions to prevent the attacks

6. Email Phishing

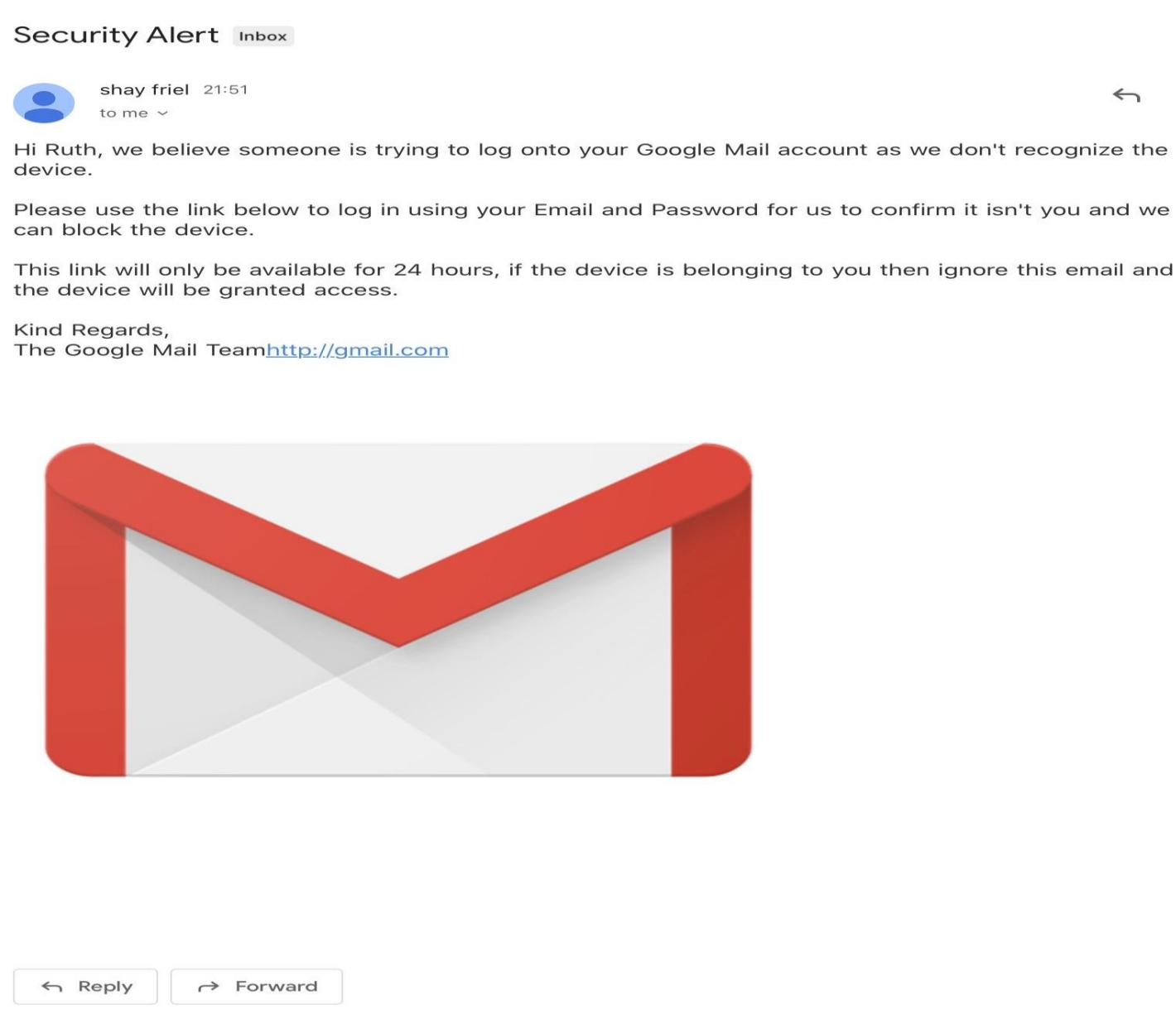


Figure 3: Shows the victim receiving an email disguised as a weapon from the attacker

3. Design & Implementation

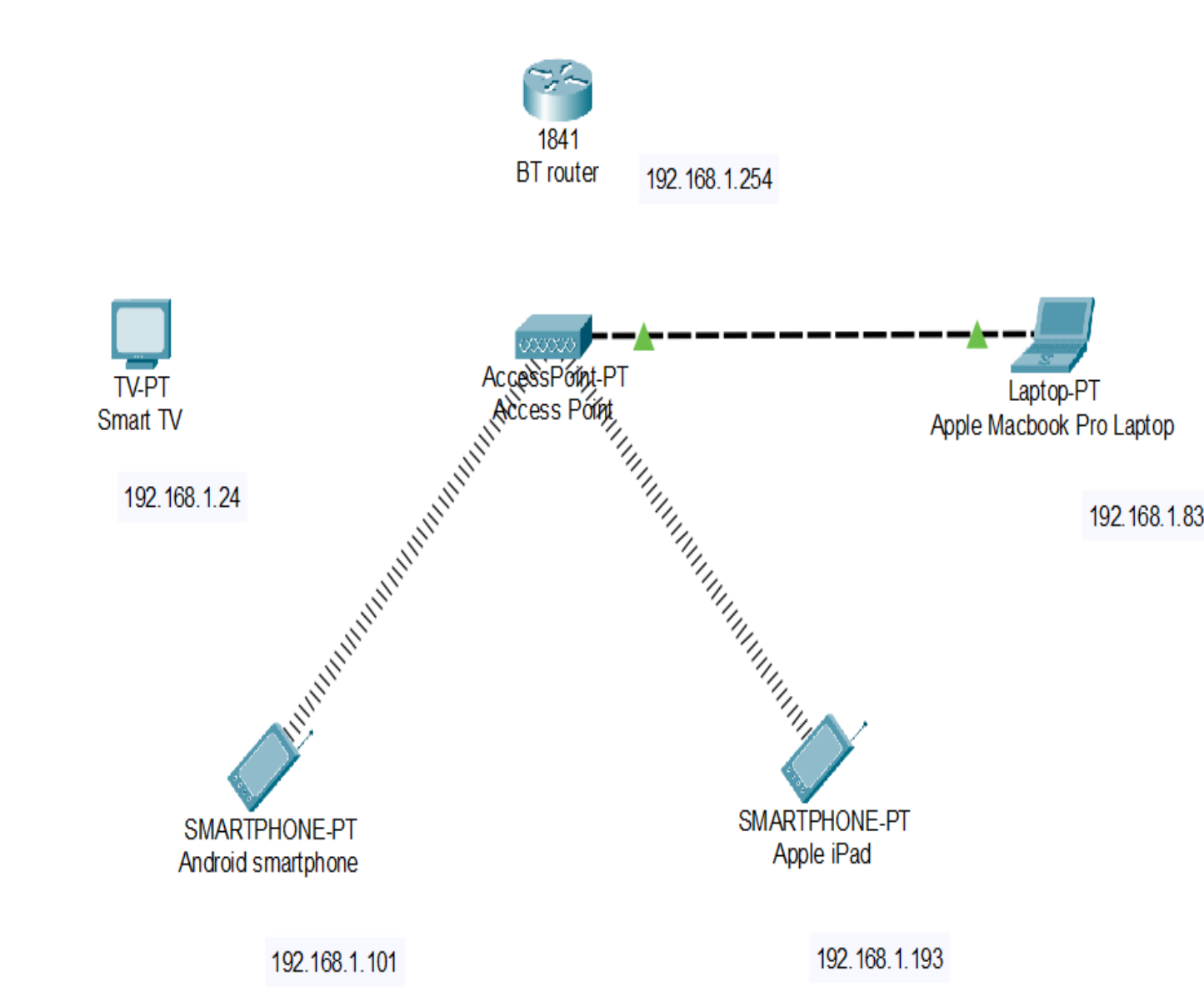


Figure 1: Design and implementation of the home network

7. Email Phishing Results

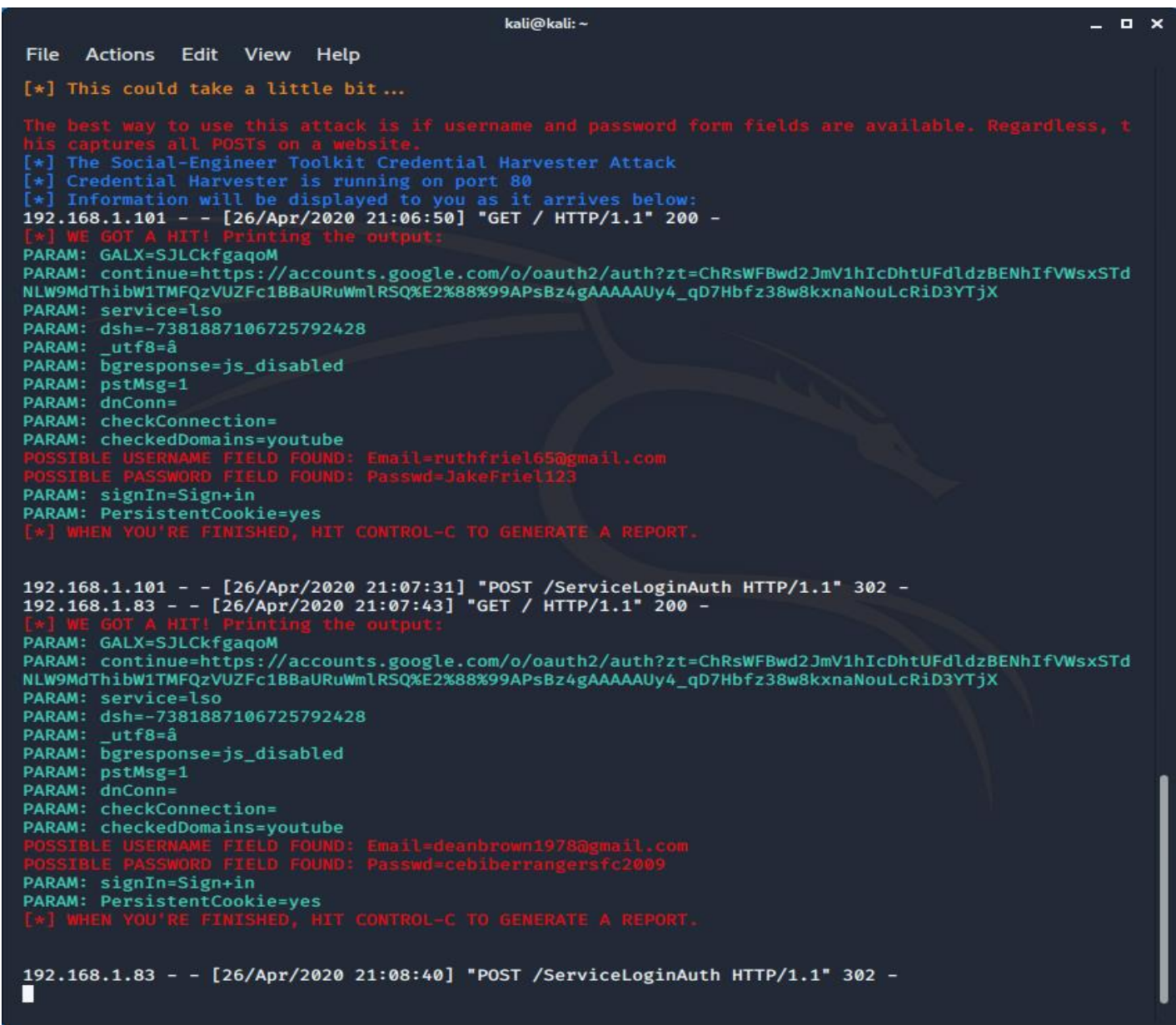


Figure 4: Shows credentials of the victims displayed on the attacker's laptop

4. Experiment & Results

The first experiment to penetrate the network was a Man-in-the-Middle ARP spoofing attack. The results in Figure 2 shows the attacker using Wireshark to sniff and capture the victim's packets. Here the attacker can see that the victim was frequently logging in and out of Facebook, allowing the attacker to spy and steal Facebook credentials. Results of the experiment and literature review show that there is not yet a working defense mechanism to prevent ARP spoofing. The second experiment to take place was an email phishing attack, where a fake Gmail login page is created and sent to victims. See Figure 3 & 4. Results from this experiment show how to prevent phishing attacks being successful by thinking before you click and use secure browsers such as Chrome and Firefox.

8. Conclusion

The project was started to test the results of other researchers work to see if their results were valid and reliable. Whilst researching other researchers work a lot of information was discovered in link to the vulnerabilities of home networks, the variety of cyberattacks criminals use every day and solutions to prevent such attacks. The main findings of solutions to prevent the threat of cyberattacks are always keeping devices updated, a newer version of software could reduce the chances of an attack. Think before you click is a major factor when it comes to email phishing scams, more than 90% of email phishing attacks are successful due to human error. To conclude, the project has been a success, presenting the deliverables and providing results which supports the research.

References

- [1] Rajkumar Buyya(Editor), Amir Vahid Dastjerdi(Series Editor), Internet of Things: Principles and Paradigms, 1st edition, 11 May 2016
- [2] Nilanjan Dey 1984, Internet of everything: advantages, challenges and applications, publisher: De Gruyter, 2019
- [3] The Role of Human Error in Successful Cyber Security Breaches, Micke Ahola, October 18th, 2019