Hes·so VALAIS WALLIS

School of Engineering

Hes·so
Haute Ecole Spécialisée de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences and Arts Western Switzerland

Degree Programme

Systems Engineering

Major Infotronics

Midterm Report

DIPLOMA 2024

Rémi Heredero

OT Security

PEN-testing and security about embedded devices

Professor
Prof. Medard Rieder, medard.reider@hevs.ch

Expert
Rico Steiner, rico.steiner@hooc.ch

Submission date of the report
01 July 2024

HES-SO Valais

SYND	ETE	TEVI
X	X	X

Données du travail de bachelor
Aufgabenstellung der Bachelorarbeit

FO 1.2.02.07.FB
che/13.03.2024

Filière / Studiengang **SYND**	Année académique / *Studienjahr* **2023-24**	No TB / *Nr. BA* **IT/2024/78**
Mandant / *Auftraggeber* ☒ HES—SO Valais-Wallis ☐ Industrie ☐ Etablissement partenaire *Partnerinstitution*	Etudiant·e / *Student/in* **Heredero Rémi** Professeur·e / *Dozent/in* **Rieder Medard**	Lieu d'exécution / *Ausführungsort* ☒ HES—SO Valais-Wallis ☐ Industrie ☐ Etablissement partenaire *Partnerinstitution*
Travail confidentiel / *vertrauliche Arbeit* ☐ oui / ja ☒ non / nein	Expert·e / *Experte/Expertin* *(nom, prénom, E-mail/Name, Vorname, E-Mail)* **Steiner Rico** - rico.steiner@hooc.ch HOOC AG, Visp	

Titre / *Titel* **OT Security labs development**

Description

The goal of this Bachelor thesis is to prepare several security related experiments in an Operational Technology (OT) environment. The environment is simulated, either using a platform named "Winter Resort Simulator Pro" or using Minecraft. In the latter case, the simulated environment still must be defined and developed. The scenarios that will be developed include wired communication by MODBUS, wireless communication using a 862 MHz radio, process control using sensors and PLC's.

Tasks

- Create an environment and select tools permitting to intercept, modify and reinject MODBUS packets, assuming the intruder has access to the communication infrastructure. Propose solutions to monitor the communication infrastructure and therefor detect and prevent such activity.
- Create an environment and select tools permitting to scan a wireless network. Intercept packets and reinject them into the network. Propose solution to harden wireless protocols against such actions.
- Create an environment and select tools to intercept sensor data to compromise the function of the controller due to invalid data. Propose approaches permitting hardening the controller software against such action.
- Prepare a setup and tools permitting to break into a PLC. Propose solutions hardening PLCs against such action.

Deliverables

- A report
- A working demonstrator
- All source code and tools
- A presentation

Signature ou visa / *Unterschrift oder Visum*	Délais / *Termine*
Responsable de l'orientation / *Leiter/in der Vertiefungsrichtung:* ..... [1] Etudiant·e / Student/in:	Attribution du thème / *Ausgabe des Auftrags:* **27.05.2024** Présentation intermédiaire / *Zwischenpräsentation*: **Semaine/Woche 27** (01-05.07.2024) Remise du rapport final / *Abgabe des Schlussberichts:* **30.08.2024, 12:00** Expositions / *Ausstellungen der Bachelorarbeiten:* **23.08.2024** – HEI **26.08.2024** – Monthey **29.08.2024** – Visp Défense orale / *Mündliche Verfechtung:* **Semaine/Woche 38** (16-20.09.2024)

[1] *Par sa signature, l'étudiant·e s'engage à respecter strictement la directive DI.1.2.02.07 « Travail de bachelor ».*
Durch seine Unterschrift verpflichtet sich der/die Student/in, sich an die Richtlinie DI.1.2.02.07 „Bachelorarbeit" zu halten.

Information about this report

Contact Information

Author:	Rémi Heredero
	Bachelor Student
	HEI-Vs
Email:	remi.heredero@students.hevs.ch

Declaration of honor

I, undersigned, Rémi Heredero, hereby declare that the work submitted is the result of a personal work. I certify that I have not resorted to plagiarism or other forms of fraud. All sources of information used and the author quotes were clearly mentioned.

Place, date: Sion, 29.06.2024

Signature: 

Contents

1 Introduction

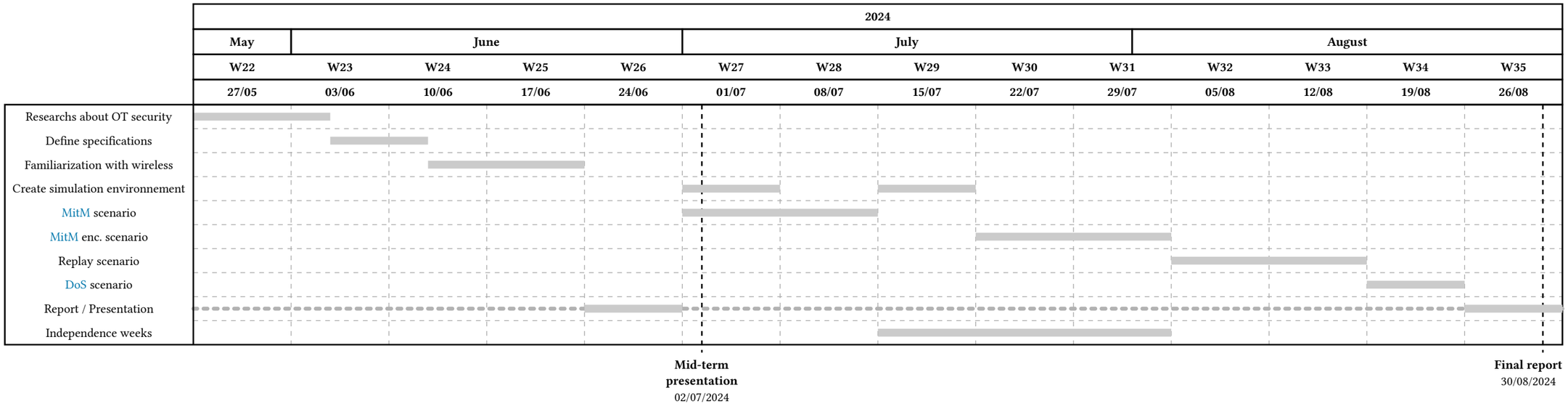
At HEI-VS, students specializing in Infotronics take a course on Operational Technology (OT) Security. This course is somewhat outdated and will be redone for next year. The aim of my Bachelor's thesis is to create several attack scenarios that can be used in this course to create a laboratory module for students. These scenarios could also be utilized in industrial training partnerships with HEI-VS. I will implement between three and four attack scenarios, including at least one wireless attack and one Modbus attack.

I chose this thesis due to my keen interest in Security and PEN-testing. Additionally, I already did some basic ethical hacking for fun and would like to specialize in security of embedded systems during the remainder of my studies. This thesis presents a valuable opportunity to delve into this field, and I have already enrolled for a master's degree to continue on this path.

This midterm report presents the planning of the thesis, an analysis of various attacks, communication medium and simulation environments and a conclusion outlining the next steps.

2 | Initial Planning

Before beginning the implementation of some attacks, it's crucial to be well-informed about all aspects of this project. Hence, the first step involves thorough research on OT security. The simulation environment is essential so that this Bachelor's thesis can be reused in the laboratory. Consequently, I spent a week on it (Hide on "Define Specifications"). Wireless communication is another non-trivial point that needs to be handled properly.
After conducting the research, I have to properly explain everything in the first part of this report in Section 4. There is a time dedicated to the report, but a bit of it is also done all along the project.



On Mid-term presentation, it's time to get to the heart of the matter.
Create simulation environment involves establishing the link between the controller and the simulation environment that has been chosen (Section 4.3 and Section 4.4). It's also included the creation of the wireless link with the protocol that will be used for the replay attack (Section 4.2 and Section 4.4).
All **attack scenarios** are described in Section 4.1 and Section 4.4.
Independence week will happen in week 29, 30 and 31. This thesis will end the Friday, 30th of August 2024 at 12pm with the render of the final report.

3 Impact on Sustainability

This section explores the impact of this thesis on sustainability, with a specific focus on the United Nations Sustainable Development Goals (SDGs) . By examining the intersection of OT security and sustainability, this section demonstrates how securing industrial and home automation systems contributes to achieving global sustainability targets.

The SDGs provide a blueprint for achieving a better and more sustainable future. This thesis aligns particularly with the following goals:

Goal 9: Industry, Innovation, and Infrastructure
Industry 4.0 relies heavily on interconnected OT systems. By addressing vulnerabilities and enhancing the security of these systems, this thesis promotes the development of robust and resilient infrastructure. Secure industrial processes foster innovation and sustainable industrialization. This thesis contributes to building infrastructure that supports economic development and human well-being, with a focus on sustainable industrialization and fostering innovation.

Goal 11: Sustainable Cities and Communities
Home automation systems are integral to the development of smart cities. This thesis examines security measures for these systems, ensuring they are protected against cyber threats. Secure home automation contributes to the safety, efficiency, and sustainability of urban environments. By protecting the systems that manage energy use, water distribution, and waste management, this research supports the development of cities and human settlements that are inclusive, safe, resilient, and sustainable.

Goal 12: Responsible Consumption and Production
Efficient resource management is a key aspect of responsible consumption and production. This thesis enhances the security of systems that monitor and control resource usage, such as smart meters and automated manufacturing processes. By preventing tampering and ensuring accurate data collection, this research helps optimize resource consumption and reduce waste. This aligns with the goal of ensuring sustainable consumption and production patterns.

Conclusion
This bachelor thesis on OT security helps to advance on sustainability goals. By enhancing the security and reliability of industrial and home automation systems, this research supports the UN's Sustainable Development Goals, promoting a more sustainable and secure future. Integrating security into these systems is crucial for sustainable development, highlighting the need for interdisciplinary approaches in addressing global challenges.

4 Analysis

This section discusses various attacks, communication mediums and simulation environments that could be used in the laboratory. It aids in selecting the appropriate attack on the right medium and simulation environment, essential for the future laboratory. The requirements of this thesis include the use of Modbus and an attack with the Flipper Zero device.

Contents

4.1 Attacks

Numerous attacks can occur in the context of OT security and can be classified into different categories. This thesis covers some attack as following, though many others exist.

4.1.1 Sniffing Attack

This attack consists in listening to the communication between two devices [1]. It can be performed on every communication medium with varying levels of difficulty. Wireless communication is particularly vulnerable because anyone can intercept the signals. For example, in Figure 1, Alice sends a message to Bob over the air without encryption, allowing Eve to listen to and read the message.

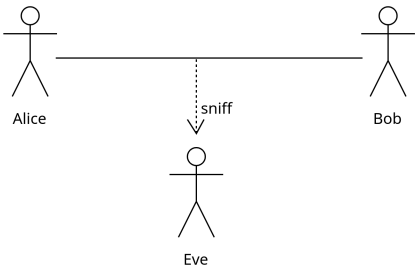


Figure 1: Sniffing attack

A sniffing attack can be performed to get secret information or understand a chemical recipe, for example. This attack can also be used for other attacks.

Security Measures

To protect against sniffing attack, the communication must be encrypted. The encryption must be strong enough to not be broken by the attacker. A simple encryption by symmetrical key, worth it. A specific attention to the key exchange must be done. At least an exchange with Diffie-Hellman protocol is recommanded to be protected against sniffing attack.

4.1.2 Spoofing

In network security, spoofing involves impersonating another device. This attack is often used in combination to other attacks, such as creating a fake Wi-Fi hotspot. In the context of OT security, spoofing is less relevant and will not be discussed further in this thesis.

4.1.3 Denial of Service

An attack by DoS aims to render a service unavailable by overloading a device or network with message [2]. In OT environments, a capable computer can execute a DoS attack effectively. To reach this goal, a device sends a large amount of message to surcharge a device or a network. In Figure 2 we can see that Mallory wants to surcharge Bob with messages. Bob can't answer to all the messages and becomes unavailable. In Information Technology (IT) world, it is more often a Distributed Denial of Service (DDoS) because usually servers are more powerful than a computer. The attacker distributes the attack on multiple device to make the attack more difficult to block. In OT world, it's useless to perform a DDoS to make a device unavailable, a DoS with a capable computer is enough. Another perspective is that OT world is typically in closed loop network and not accessible from outside.

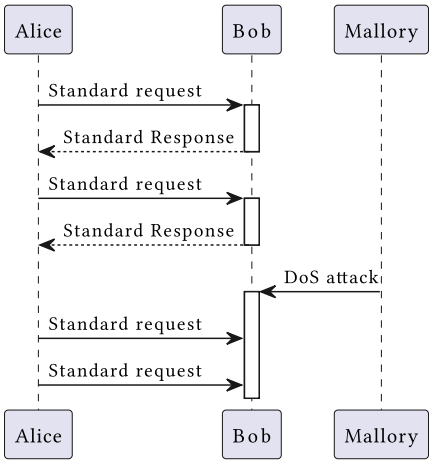


Figure 2: DoS attack

There are two primary types of DoS attacks in OT systems:

- **DoS on the communication medium**: This type of attack focuses on disrupting the data flow between devices by flooding the network with excessive traffic. This leads to network congestion and delays or blocks legitimate communication.
- **DoS on the controller**: This attack targets the processing capabilities of the controllers, such as Programmable Logic Controllers (PLCs), by sending numerous commands. This overcharge of the PLC, causing crash and make it unresponsive.

> Did you know that when the Apollo 11 mission landed on the moon, the navigation system was so overloaded due to a defect sensor that the navigation system crashed [3], forcing Neil Armstrong to take manual control of the landing?
> This is an example of an unintentional DoS.

Security Measures

Several ways exist to protect against DoS. At this stage, the best is to avoid doing an action at the reception of a message. To prevent intentional and unintentional DoS. Unfortunately, is not always possible. Another way is to limit the number of messages that can be received in a certain time. To achieve that, it's probably necessary to use another device to filter the message. This device can be a firewall, for example. But in the case of a DDoS, it's almost impossible to block the attack. The only way is to have a very powerful device that can filter the message. But even with a very powerful device, the attack can be successful.

4.1.4 Replay

A replay attack involves resending a previously intercepted message as if it were from the original sender [4]. As we can see in Figure 3 Mallory sniff the message between Alice and Bob. Mallory can send the message to Bob as if Alice had sent it. This is particularly relevant in OT environment with wireless communication, such as the typical example: replaying a command to open a garage door. The attacker sniffs the command and replays it to open the door.

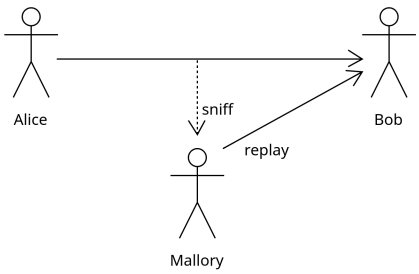


Figure 3: Replay attack

Security Measures

Two main ways exist to protect against replay attack. It depends on if it broadcast or bidirectional communication.

When both device communicates together in a bidirectional communication, it's possible to add a timestamp to the message and sign the hash.

When communication is broadcast, the sender device is often without any connection to other devices. In this case, it's not possible to have a timestamp. Using rolling code is a good way to secure against replay attack. The rolling code is a code that changes at each message. Both devices use a pseudo-random number generator to generate the code. The receiver device can check if the code is in the next code sequence.

4.1.5 Man in the Middle - Connected

A MitM attack occurs when a third party can intercept actively, modified or send packets on a network [5]. Commonly, this involves connecting a new device to a star or bus network topology. Once connected to the network, Mallory (Figure 4) can perform a sniffing attack or send a message. The aim is often to understand an Alice message, modified it and send it to Bob.

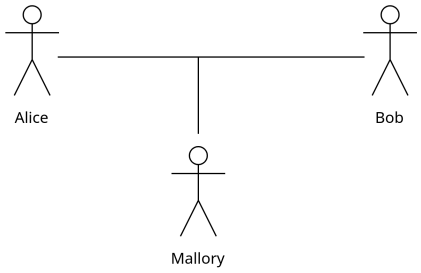


Figure 4: MitM on a connected network

Security Measures

Encryption with a symmetrical key can be used to protect the message from being intercepted, modified or impersonated. The key can be exchanged with a standard Diffie-Hellman exchange.

4.1.6 Man in the Middle - Full interception

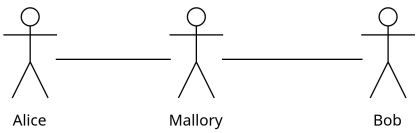


Figure 5: MitM intercept everything

When Mallory is on the gateway or between Alice and Bob like in Figure 5 Mallory can intercept all messages and neither Alice nor Bob can be sure that they send and receive messages to the right person. This is the most dangerous attack because Mallory can impersonate Alice and Bob and send a message to the other person. Even with the security measures see on Section 4.1.5, Mallory was able to impersonate Alice and Bob with create its own key with each other. This is why a MitM attack is so dangerous.

Security Measures

When a Mallory attacker can intercept all messages exchanged since the beginning of the communication, it isn't possible to be sure that the message is from the right person. We need to trust someone before. Certificates are made for that. There are signed by a trusted third party and can be used to verify the identity of the person or device. The most common certificate is X.509 certificate.

4.2 Communications medium

Different communication mediums are vulnerable to these attacks, highlighting the critical distinction between IT and OT security. In OT security, communication is a highly sensitive aspect, and historically, security measures were minimal or non-existent [6].

4.2.1 Modbus

Modbus is a communication protocol developed by Modicon in 1979 [7]. It involves a Modbus Master requesting data from a Modbus Slave. The client (master) sends a request to read or write data to a server (slave). Modbus was originally designed for serial communication (call Modbus RTU). It has since been adapted for use over TCP/IP (call Modbus TCP).

Modbus RTU

Modbus with RTU is a serial communication, compacted, binary representation of the data. It transported on physical layer RS232 or RS485. Modbus RTU includes a Cyclic Redundancy Check (CRC)–16 bits checksum for error detection.

A frame is composed of:

- Address: 1 byte
- Function code: 1 byte
- Data: 0-252 bytes
- CRC: 2 bytes

Each byte of the frame is sent as 11 bits:

- 1 start bit
- 8 data bits
- 1 parity bit
- 1 stop bit

Modbus TCP

Modbus over TCP is a modern adaptation of Modbus. It's still a binary protocol, but it's transported over TCP. This adaptation eliminates the need for CRC due to inherent error detection in TCP. Otherwise, the frame is composed like Modbus RTU and the default port for Modbus TCP is 502.

4.2.2 wM-Bus

wM-Bus [8, part. 4] is a wireless version of the Meter-Bus (M-Bus) [8] protocol, used primarily in Europe for metering applications. It adheres to the ISO layer model [9] but implements only specific layers :

- Layer 1: Physical layer ([8, part. 2] for wired and [8, part. 4] for wireless)
- Layer 2: Data link layer ([8, part. 2] for wired and [8, part. 4] for wireless)
- Layer 7: Application layer ([8, part. 3])

The wireless specification has several modes of operation, to work on several frequency bands. The most common are:

Mode S

This mode [8, part. 4, p. 16] work on 868 MHz with 2-Level Frequency-Shift Keying (2FSK) modulation on a single channel. Meters send data many times a day to a stationary collector. The collector can be used in a power-saving function and is waking up by the long heading of the frame. This mode has a one-directional (S1) or bidirectional (S2) sub-mode.

Mode T

This mode [8, part. 4, p. 19] work on 868 MHz with 2FSK modulation. The one-directional sub-mode T1 has a single-channel, but the bidirectional sub-mode T2 can use 2 channels. Meter is frequently sending data to a collector. This collector can be mobile.

Mode R2

This mode [8, part. 4, p. 24] work on 868 MHz with 2FSK modulation. This mode is bidirectional and has 10 channels. This mode can use frequency hopping for a higher duty cycle than other modes.

Mode C

This mode [8, part. 4, p. 27] work on 868 MHz with 2FSK modulation. The one-directional sub-mode C1 has a single channel and the bidirectional sub-mode C2 has 2 channels with 2 different bandwidths. It can be used for stationary or mobile collector.

Mode N

This mode [8, part. 4, p. 30] work on 169 MHz with 4-Level Gaussian Frequency-Shift Keying (4GFSK) modulation. This mode can be one or bidirectional and has 13 channels. This mode is used for long-range communication to a stationary collector.

Mode F

This mode [8, part. 4, p. 35] work on 433 MHz with 2FSK modulation. This mode has only a bidirectional sub-mode. It's used for long-range communication to a stationary or mobile collector.

4.3 Simulation environments

As this thesis is part of the preparation of a new laboratory, the simulation environment must extend beyond abstract communication. The objective is to have a real physical controller interfaced with a simulated process. This simulated process remains necessary because a fully physical setup is prohibitively expensive and far less flexible than a simulated one.

4.3.1 Factory I/O

Factory I/O, developed by Real Games, is a realistic simulation software designed to emulate a factory environment. It allows for the creation of custom scenes, providing flexibility for various industrial scenarios. However, the software comes with an expensive licence, which must be considered when selecting the simulation environment. Factory I/O could also be beneficial for Power & Control specialization. This software can interface with modbus over TCP, but an additional third-party software is required to implement a security layer. While Factory I/O is only available on Windows, it operates effectively on Linux using Wine.

Figure 6: Factory I/O palletizer scene

Scenario idea

In this scenario, a PLC could control the palletizer scene (Figure 6). A Wireless sensor could indicate the presence of a truck to be loaded. The Wireless replay attack could target this sensor. The DoS attack could be executed on the same sensor. The MitM attacks could be conducted on the Modbus/TCP communication between the PLC and the palletizer, with the objective of gaining control over the clamp.

4.3.2 Home I/O

Home I/O is also developed by Real Games, simulates a House (Figure 7) equipped with extensive home automation features. This software is available at a lower organizational licence cost and could be of interest to ETE students. Home I/O offers a REST API for interfacing with all sensors and actuators. Similar to Factory I/O, it runs well on Linux using Wine.

Figure 7: Home I/O scene

Scenario idea

In this scenario, a PLC manages the alarm and access systems, including the main door and garage. The garage door can be opened using a wireless remote, which could be the target of a wireless replay attack. An external presence detector on the main door could be used for the DoS attack. MitM attacks could be executed on the Modbus/TCP communication between the PLC and the alarm system, aiming to deactivate the alarm system.

4.3.3 Minecraft

Another suitable approach would be to use the Electrical Age world of Minecraft (Figure 8) which was previously utilized in a Telecommunication course. The goal of this lab was to control a Factory and an energy system to maximize production. Continuing this lab could provide valuable opportunities for students to explore and secure communication systems. In Minecraft, security can be implemented using Open Computers or by creating an extension mod for Modbus over Transport Layer Security (TLS), which might be simpler than using Lua with Open Computers.

Figure 8: Minecraft Electrical Age scene

Scenario idea

The scenario involves reusing the PLC from the previous lab, which controls various operations. A physical Human-Machine Interface (HMI) could be constructed to manage the factory and coal production, similar to the HTLM interface used in the previous lab. A wind wireless sensor could be added to the setup. Wireless replay and DoS attack could be targeting this sensor. The MitM attacks could be executed on the Modbus/TCP communication between the PLC and the Factory, with the goal of gaining control over the Factory operations.

4.4 Conclusion

This section presented various attacks that can be performed on OT systems. The communication mediums discussed during the preparatory phase of this work were also outlined. Additionally, potential simulation environments for laboratory use were evaluated.

Based on this information, M.Rieder and M. Clausen have decided on the simulation environment. The chosen platform is Home I/O, as it can be utilized by ETE students.

The planned attacks include a replay attack on a wireless control or sensor, a DoS attack on an external sensor with valid data (overloading the controller rather than the communication medium) and a MitM attack on the Modbus/TCP communication. The MitM attack will be conducted in two phases. The first phase will involve an unencrypted Modbus/TCP communication while the second phase will involve encrypted Modbus/TCP communication with symmetrical key exchanged by Diffie-Hellman.

Wired communication will be carried out using Modbus, a widely used protocol in OT systems, which aligns with the brief for this thesis.

For the Replay attack on a wireless control or sensor, the idea is to use the Flipper Zero to record and replay a message. This attack will be performed only on the physical layer. The Flipper Zero can only execute such an attack on basic wireless protocols, as it cannot perform a replay attack on frequency hopping protocols. The wireless protocol must employ On-Off Keying (OOK), Amplitude-Shift Keying (ASK) (with 270 or 650 kHz Bandwidth) or 2FSK modulation. Consequently, protocols like Zigbee or DigiMesh are not suitable for this attack and were not explored in depth.

wM-Bus is a single canal 2-Level Gaussian Frequency-Shift Keying (2-GFSK) protocol, is well-suited for replay attacks using the Flipper Zero. Given that typical wM-Bus T-mode application include electricity or water meters, incorporating such meters into the simulation would be relevant with a replay attack targeting these devices.
If the wM-Bus implementation proves it challenging, a contingency plan involves using a simple OOK modulation at 433 MHz.

5 Conclusion

In conclusion, this midterm report provides a comprehensive overview of the initial phase of this bachelor's thesis. After reviewing the schedule and discussing sustainability, the core of this report contains the analysis part of the thesis. We have determined that the simulation environment will be Home I/O and identified three key attacks that will be carried out.

1. **Replay attack on a wireless device.** This attack will be probably carried out on a Wireless M-Bus (wM-Bus) electricity meter. If this proves too challenging within the available time, an alternative would be to target the garage door remote control using simple OOK modulation on 433 MHz. One potential countermeasure to protect against this attack, have to be confirmed later, would be implementing a rolling code.
2. **Denial of Service (DoS) attack on an external sensor.** This attack will involve flooding the PLC with valid messages at a frequency too high for the PLC to handle, effectively overloading it. To mitigate this, a better programming design will have to be developed.
3. **Man in the Middle (MitM) attacks.** Two phases of MitM attack will be conducted on Modbus communication. The first will target an unencrypted Modbus TCP communication. Protection against this will involve implementing a symmetrical key exchanged using Diffie-Hellman. The second phase will exploit the key exchange process, demonstrating that if an attacker is present from the start, it is impossible to guarantee the authenticity of the communication partner. Utilizing certificates is the only way to ensure secure communication. So Modbus over TLS will be used instead of TCP to protect against this attack.

This foundational analysis sets the stage for the subsequent phases of the project. The next steps will include mastering Modbus communication with Home I/O and executing the MitM attack on this protocol, followed by the other planned attacks. The development of the wM-Bus interface remains a critical task for future task on this thesis.

6 Glossary

Flipper Zero: Flipper Zero is a portable multi-tool for pentesters and geeks in a toy-like body. 4, 12

***HMI* – Human-Machine Interface**: A human-machine interface (HMI) is a user interface or dashboard that connects a person to a machine, system, or device. 12

***IT* – Information Technology**: Information Technology (IT) is the use of computers to store, retrieve, transmit, and manipulate data or information. 6, 8

***OT* – Operational Technology**: Operational Technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. 1, 2, 5, 6, 7, 8, 12

***PLC* – Programmable Logic Controller**: A programmable logic controller (PLC) is an industrial digital computer that has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, robotic devices, or any activity that requires high-reliability control and ease of programming. 6, 10, 11, 12, 13

***SDG* – Sustainable Development Goal** 3

6.1 Attacks

***DDoS* – Distributed Denial of Service**: A distributed DoS is basically the same as a DoS attack, but the attack comes from multiple sources. 6

***DoS* – Denial of Service**: A denial-of-service (DoS) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. 2, 6, 10, 11, 12, 13, 14

***MitM* – Man in the Middle**: A Man in the Middle (MitM) attack is a form of eavesdropping in which communication between two users is monitored and modified by an unauthorized party. 2, 7, 8, 10, 11, 12, 13

6.2 Communications

***2FSK* – 2-Level Frequency-Shift Keying**: 2-Level Frequency-Shift Keying (2-FSK) is a form of Frequency-Shift Keying (FSK) modulation that uses two levels of frequency to encode digital data. 9, 12

***2-GFSK* – 2-Level Gaussian Frequency-Shift Keying**: 2-Level Gaussian Frequency-Shift Keying (2-GFSK) is a form of FSK modulation that uses two levels of Gaussian filtering to encode digital data. 12

***4GFSK* – 4-Level Gaussian Frequency-Shift Keying**: 4-Level Gaussian Frequency-Shift Keying (4-GFSK) is a form of FSK modulation that uses four levels of Gaussian filtering to encode digital data. 9

***ASK* – Amplitude-Shift Keying**: Amplitude-shift keying (ASK) is a form of modulation in which the amplitude of a carrier wave is varied proportionally to that of a modulating signal. 12, 15

***CRC* – Cyclic Redundancy Check** 8

***FSK* – Frequency-Shift Keying**: Frequency-shift keying (FSK) is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier wave. 14

***IP* – Internet Protocol** 8

***M-Bus* – Meter-Bus** 9

***OOK* – On-Off Keying**: On-Off Keying (OOK) denotes the simplest form of ASK modulation that represents digital data as the presence or absence of a carrier wave. 12, 13

***RTU* – Remote Terminal Unit** 8

***TCP* – Transmission Control Protocol** 8, 10, 11, 12, 13

***wM-Bus* – Wireless M-Bus** 4, 4, 9, 12, 13

6.3 Cryptography

Diffie-Hellman: Diffie-Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel. 7, 12, 13

***TLS* – Transport Layer Security**: Transport Layer Security (TLS) is a cryptographic protocol that provides communications security over a computer network. 11, 13

X.509: X.509 is a standard that defines the format of public key certificates. 8

Bibliography

[1] "Sniffing Attack." Jun. 04, 2023. Accessed: Jun. 24, 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Sniffing_attack&oldid=1158437808

[2] "Denial-of-Service Attack." May 27, 2024. Accessed: May 28, 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Denial-of-service_attack&oldid=1225934024#DDoS_extortion

[3] "Lunar - Missions - Apollo 11 Mission." Accessed: Jun. 24, 2024. [Online]. Available: https://www.lpi.usra.edu/lunar/missions/apollo/apollo_11/

[4] "Replay Attack." Jan. 04, 2024. Accessed: May 28, 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Replay_attack&oldid=1193515559

[5] "Man-in-the-Middle Attack." Jun. 20, 2024. Accessed: Jun. 25, 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Man-in-the-middle_attack&oldid=1230046662

[6] Fahmida Y. Rashid, "The Old Ways Aren't Working: Let's Rethink OT Security," Nov. 2021, [Online]. Available: https://www.darkreading.com/cyber-risk/the-old-ways-aren-t-working-let-s-rethink-ot-security

[7] "Modbus." May 23, 2024. Accessed: May 27, 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Modbus&oldid=1225269451

[8] "EN 13757 - Communication Systems for Meters." Swiss Association for Standardization (SNV).

[9] "ISO/IEC 7498-1:1994 - Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model." Swiss Association for Standardization (SNV).