Hacking The Assembly Line: Evaluating Vulnerabilities and Best Practices for Cyber-Physical System Security

Marc Geggan, BSc (Hons) Ethical Hacking, School of Design and Informatics
1902548@uad.ac.uk

INTRODUCTION

Industry 4.0 represents the fourth industrial revolution, combining traditional processes with advanced technologies like machine-to-machine communication, industrial IoT, and cloud computing. This convergence of operational technology and information technology creates **"Cyber-Physical Systems"** where physical assets and digital processes merge. However, the vulnerabilities and threats arising from this integration have not been fully realised.

The lack of awareness and understanding of potential risks is a significant challenge, necessitating research and development of new techniques. **Penetration testing is one method used to identify vulnerabilities within CPS**, but it should be conducted in replicated testbeds or digital twins to avoid damage or disruption to critical systems.

The security and resilience of Industry 4.0 and cyber-physical systems heavily rely on the **advancement of academic and professional research**. Additionally, collaboration between the security industry and technology vendors is crucial in developing effective solutions and strategies to mitigate threats and vulnerabilities in these systems

AIM

Research question: "**What vulnerabilities arise from the convergence of IT/OT systems, particularly in relation to Programmable Logic Controllers, in the architecture of smart factories, and what are the best practices for organisations to mitigate them?**".

The aims of this project are as follows:

- **Analyse the architecture** of cyber-physical systems in use in smart factories to distinguish the attack surface of IT/OT converged systems.
- **Investigate the specific vulnerabilities** of PLCs in smart factories, considering their communication methods and internet connectivity.
- **Evaluate potential mitigations** for vulnerabilities in PLCs in smart factories, with **a focus on best practices** for industrial control systems.
- Design and **build a physical PLC penetration testbed** that accurately simulates a real-world industrial control system and **conduct a comprehensive analysis of potential vulnerabilities and mitigations.**

METHOD

A proof-of-concept testbed was developed to replicate an Industrial Control System environment. It included physical and virtual components, such as a **Koyo Click Plus C2-03CPU PLC** with **Modbus and MQTT protocols** enabled. Inputs and processes controlled by the PLC were simulated using **physical selector switches and LEDs** attached to the PLC. **Three virtual machines** were used: Ubuntu for SCADA software, Windows 10 for PLC provisioning, and Kali Linux for penetration testing. The testbed enabled communication between the physical PLC and virtual machines and facilitated realistic testing and assessment of ICS devices and protocols.

The vulnerability exploitation phase of the lab involved several methods to assess the security of the system. **First, Shodan.io was used to search for public-facing internet-enabled PLCs**, focusing on Koyo Click and Allen-Bradley devices, as well as identifying the widespread usage of MQTT and Modbus protocols. **Nmap was then employed to scan devices and ports** within the network, demonstrating the ports and services found in ICS environments. **Wireshark was used to capture and analyse Modbus messages**, revealing important details being communicated between devices. The **Mbtget tool was used to read and write to the coils,** testing the security of the Modbus protocol. **MQTTExplorer was then used to connect to an MQTT broker**, allowing monitoring and publishing of messages related to LED status. Lastly, a **DoS SYN Flood attack was launched on the PLC to assess its resilience with Hping3.**

The comprehensive vulnerability testing methods employed in this study provided a strong assessment of ICS device security and highlighted areas for further investigation and improvement.

RESULTS

Shodan revealed **numerous publicly accessible ICS devices**, including 29 Koyo Click and over 5,800 Allen Bradley devices. The search for MQTT showed over 431,000 results, while the Modbus protocol search yielded 364,541 results, highlighting the prevalence of ICS devices using these protocols.

Nmap scanning provided valuable network information, identifying specific devices like the Koyo Click Plus PLC with an open Modbus port, the engineer-scada-machine with open ports for Mosquitto and IgnitionSCADA software, and a Windows 10 Enterprise Edition machine with multiple open ports.

Successful Modbus protocol tests revealed **the ability to read and write to PLC coils with no authentication,** allowing an attacker to manipulate LED light status regardless of switch positions (Figure 2), demonstrating lack of security. Similar vulnerabilities were observed with the MQTT protocol, enabling an attacker to **manipulate LED light status within the MQTT broker by publishing to the topic.** A DoS SYN Flood attack using **Hping3 caused the PLC's connection to drop, rendering it inaccessible over Wi-Fi.** The device reappeared in the list of connections only after the attack was stopped.

Figure 2: Comparison of PLC status - Left: PLC in normal working order, Right: PLC with switches in the ON position, but one LED light turned off due to a malicious Modbus command.

Figure 1: Final PLC and protocol testbed for vulnerability exploitation.

DISCUSSION

This project analyses vulnerabilities and mitigations in industrial control systems using a testbed that simulates a real-world ICS environment. The study explores specific vulnerabilities in PLCs, highlighting risks such as **lack of authentication, encryption, and exposure to insecure protocols**. The testbed successfully demonstrates these vulnerabilities and proposes **mitigations such as secure configurations, implement authentication mechanisms, network segmentation, and incident response plans**. However, it's important to acknowledge the limitations of the lab, such as its inability to fully replicate the size and complexity of larger industrial control systems.

CONCLUSION

This paper **successfully addresses the research question regarding vulnerabilities in IT/OT convergence**, using a literature review and a hardware lab testbed. The testbed demonstrates **multiple specific vulnerabilities and the need for strong security measures**, although it has limitations in representing the wide range of protocols and technologies used in real-world environments. The research **contributes to ICS security knowledge and suggests future exploration of vulnerabilities and enhancements to the lab.**

ACKNOWLEDGEMENT

I am grateful for my supervisor, Jamie O'Hare, and technician, Gerry, for the constant support throughout this project. I also extend my gratitude to Mazars LLP for funding this research and providing me with great opportunities to expand my knowledge and share my research with other security professionals.