Long-Distance Remote Diagnostics for Cyber-Physical System Security

A Preliminary Investigation into Remote Security Assessments for Maintenance Testing

Kazutaka Matsuzaki
Faculty of Global Informatics
Chuo University
Tokyo, Japan
email: matsuzaki@tamacc.chuo-u.ac.jp

Masatoshi Enomoto
Faculty of Commerce
Yokohama College of Commerce
Kanagawa, Japan
email: masatoshi-e@shodai.ac.jp

Kenji Sawada
iPERC
The University of Electro-Communications
Tokyo, Japan
email: knj.sawada@uec.ac.jp

***Abstract*— This extended abstract introduces an initial application of long-distance remote security diagnostics for Cyber-Physical Systems (CPS), focusing on Industrial Control Systems (ICS) during maintenance testing. Through the Internet, a distance of 350 kilometers was bridged to conduct a preliminary security assessment of a building automation system. Emphasizing the importance of monitoring essential functions of ICS, such as digital outputs and serial communication, we utilized a pair of devices designed to encapsulate digital outputs using TCP/IP, enabling remote monitoring at the test device over a temporally configured site-to-site Virtual Private Network (VPN). Despite an average network latency of 33 milliseconds and an approximate delay of around 3 seconds for digital outputs, the system was able to effectively communicate changes in the essential services of the control systems to the test device. Preliminary results underline the feasibility of this long-distance approach, setting the stage for future work on comprehensive real-world demonstrations using diverse simulated control systems, namely factory automation and gas plant control systems. The goal is to advance the field of remote security diagnostics during maintenance testing, providing reliable and effective security evaluation of CPS.**

Keywordss-Industrial Control Systems (ICS); Remote Security Diagnostics; Maintenance Testing.

I. INTRODUCTION

As society increasingly relies on Cyber-Physical Systems (CPS) in sectors such as distributed solar power plants, cloud-based building management, and smart factories, the inherent cyber risks and potential disruptions multiply. A successful cyberattack on CPS can cause significant damage in both digital and physical realms, rendering critical infrastructures like pipelines, water treatment facilities, and power grids vulnerable to shutdowns and disruptions.

In an environment where new vulnerabilities are continuously discovered and cyber attackers' tactics constantly evolve, it is crucial to persistently assess cybersecurity measures. Existing security evaluation frameworks include certification tests for control systems and embedded devices, focusing on known vulnerabilities and communication robustness. However, executing such tests on systems under operation is fraught with challenges due to time, workforce, and cost constraints [1].

This extended abstract discusses the potential of remote, network-based testing as an alternative strategy for enhancing cybersecurity in CPS. We delve into a cloud-based diagnostic approach designed to minimize on-site testing while providing a practical assessment of the security posture of these systems [2].

The primary focus of this extended abstract is to establish whether the distance between testing and target sites impacts the efficacy of remote security diagnostics during the maintenance testing of Industrial Control Systems (ICS), according to IEC 62443 standards. A key challenge we seek to address is determining how remote testing conditions can simulate Local Area Network (LAN) testing conditions, despite significant physical distances between systems.

The rest of the extended abstract is organized as follows: Section 2 provides an overview of the proposed methodology for remote security diagnostics, while Section 3 presents an analysis of our initial findings. Section 4 discusses potential implications, and Section 5 concludes.

II. METHODOLOGY

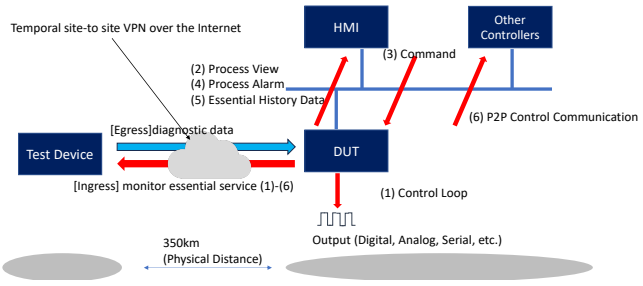

Figure 1. Whole Picture of Remote Security Diagnosis for ICS.

In our study, we designed and executed a series of tests utilizing a practical testbed with the following characteristics (Figure 1):

Physical distance from the Test Device: The target systems were located 350 kilometers away from the Test Device. This considerable physical distance provides a realistic scenario for assessing the capability of remote diagnostics during the maintenance of ICS.

Temporal site-to-site VPN over the Internet: The test environment temporally utilized an Internet-based Virtual

 ISBN: 978-1-68558-092-6

Private Network (VPN) for communication between the Test Device and the target systems.

Diverse Simulated Control Systems: The subjects of our security diagnostics were different types of simulated control systems, each using varied control protocols and implemented using different control devices. These systems were:

- Building Automation System: This system controls elements such as air conditioning, lighting, and electricity reception in a building.
- Factory Automation System: This system simulates a section of a robotic arm in an automobile assembly factory, specifically one that sorts parts.
- Gas Plant Control System: This system controls the pressure in gas tanks to maintain consistency.

The diversity of these systems provides a comprehensive testing ground to evaluate our remote diagnostic approach across various operational conditions and requirements. The results from these tests provide insights into the efficacy of remote security diagnostics during maintenance testing and can inform future development in this field.

III. Implementation and Preliminary Results

In the implementation phase of our study, we first set up the necessary equipment for our testing environment. This included a pair of devices designed to encapsulate digital outputs using TCP/IP and enable Ethernet-based remote monitoring of distant equipment, bridging the physical gap of 350 kilometers (Figure 2) [3]. These devices were placed at both the test device and the Device Under Test (DUT), a Programmable Logic Controller (PLC) of the building automation system, in our preliminary testing.

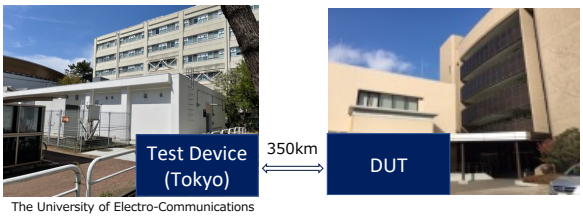

Figure 2. Two buildings to run long-distance remote diagnostics trials.

Once the setup was complete, we conducted preliminary testing by sending diagnostic data from the test device to the DUT and remotely monitoring the state of the building automation system's essential services from the test device as closely as possible. Notably, this was achieved despite the inherent latency in our network setup, characterized by an average network latency of 33 milliseconds (ICMP: Internet Control Message Protocol) and a delay of around 3 seconds for digital outputs (DO over TCP/IP).

Our preliminary results showed that the proposed system effectively conveyed changes in the essential services of the control systems to the test device, even in the presence of notable network latency and digital output delay. The tests demonstrated that the method could consistently deliver changes to the test device from the remote building automation system, fulfilling its goal of reliable remote security diagnostics.

IV. Future Work

We will extend the remote diagnostic methodology developed and tested preliminarily on a building automation system to other control systems, specifically factory automation and gas plant control systems. This diversity will provide a more comprehensive view of the applicability and efficacy of our methodology across different industrial scenarios.

Firstly, we will refine our approach to remote monitoring of essential services. Essential services, which include communication between DUT, Human-Machine Interfaces (HMI), and other controllers, are integral to the functioning of control systems. It is, therefore, crucial to ensure the reliability and accuracy of their remote monitoring, despite the inherent challenges posed by the physical distance and consequent latency. To achieve this, we will continue optimizing the systems for encapsulating digital outputs and transferring data over temporal site-to-site VPN.

Furthermore, we will investigate the impact of the 350 kilometers distance, particularly the associated network latency and digital output delay, on the quality of the remote diagnostics. Our preliminary results have shown that the proposed methodology can reliably deliver changes in the essential services to the test device from a remote building automation system. However, a more in-depth understanding of how the inherent latency affects the quality of diagnostics is crucial. This analysis will aid in refining the methodology for optimal performance even over long distances.

V. Conclusion

In this extended abstract, we have presented an initial application of remote diagnostics over a long-distance network for the security evaluation of CPS. Our preliminary results, based on a building automation system situated 350 kilometers away, demonstrate the feasibility of this approach. We have highlighted the importance of reliable data transfer and effective monitoring of essential services, even in the presence of inherent network latency. The future research will continue to refine this methodology, exploring the impacts of long distance on diagnostic quality across different control systems.

References

[1] K. Matsuzaki and S. Honiden, "Enhancing ICS Security Diagnostics with Pseudo-Greybox Fuzzing During Maintenance Testing," in Proceedings of the 18th International Conference on Software Technologies (ICSOFT 2023) pp. 660-667.

[2] M. Enomoto, K. Sawada, S. Hosokawa, and K. Matsuzaki, "Prototype Experimental Environment Using Actual Equipment for Remote Control Security Verification," IEEE 12th Global Conference on Consumer Electronics (GCCE 2023).

[3] K. Matsuzaki, K. Sawada, and S. Honiden, "Remote Security Assessment for Cyber-Physical Systems: Adapting Design Patterns for Enhanced Diagnosis," in Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023) pp. 805-812

 ISBN: 978-1-68558-092-6