Survey: PLC vulnerabilities and Industrial Intrusion Detection Systems IIDS

Saber Mhiri

***Abstract*—Industrial Control Systems (ICS) are frequently used in manufacturing and critical infrastructures like water treatment, chemical plants, and transportation schemes. Citizens tend to take modern-day conveniences such as trains, planes or tap water for granted without considering the critical systems involved for their operations.**

Programmable Logic Controllers (PLCs) are the essential components in many Industrial Control Systems that control physical processes. However, in recent years the security flaws of these devices have come under scrutiny, particularly since the widely discussed Stuxnet attack.

Interrupting these industries could lead to disastrous consequences, leading to financial losses or even costing human lives. For that reason, researchers have been actively investigating the threats targeting ICS.

To help the industry state-of-the-art to move forward and to provide information required to improve the security for these controllers, this work investigates the existing vulnerabilities that affect these vulnerable controllers as well as the last mechanisms of attack detection and mitigation for attacks. In this work we focused on recent works related to PLC vulnerabilities and IDS (Intrusion Detection Systems).

***Index Terms*—OT network, PLC vulnerabilities, s7CommPlus, threat detection, Intrusion Detection Systems IDS.**

I. Introduction

Industrial Control Systems (ICS) control important physical processes in critical infrastructures and various industrial environments. Programmable Logic Controllers (PLC) are one of the most crucial components in many such systems, as PLCs are the point of interaction between the cyber and physical world. Well known previous attacks that targeted PLCs, like Stuxnet, have demonstrated the security challenges faced by these devices.

The industry has since attempted to improve the security of PLCs but the impact of these measures is often not widely understood, despite various attacks that took place post-Stuxnet. Moreover, there is a relatively small amount of information available in the research community on the security of state-of-the-art PLCs, firmware and programming environments. Therefore, to help improve the security of PLCs, and thereby ICS more generally, in this work we presented the most recent research related to PLC security and vulnerabilities in chapter 1 as well as the last proposed IDS (Intrusion Detection System) in chapter 2.

II. PLC Vulnerabilities

Klick, Johannes, et al. (2015) [1] used an approach similar to Stuxnet through inserting code in the beginning of a scan cycle of the PLCs while applying a SNMP scanner and a SOCKS proxy on a Siemens S7-300 PLC. Through this vulnerability, a backdoor can be opened that can be used to send packets through the network via an outward facing PLC. Although the PLC vendors' proprietary software usually provide password protections, the work of Wardak, et al. (2016) [2] showed the possibility of password stealing, password reset and memory control attacks on the Siemens S7-400 PLCs using replay attacks. Sandaruwan, et al. (2013) [3] have previously proven the feasibility of replay attack, man- in-the-middle (MITM) attack and authentication bypass attack.

Spenneberg, et al. (2016) [4] introduced a PLC worm capable of affecting newer PLCs. This worm has been developed and demonstrated that it can be introduced as a malicious code into the PLC without human interaction. The vulnerabilities of Siemens' proprietary protocol, S7CommPlus have been exploited in this attack. The S7CommPlus is used for the communication between the TIA Portal and the S7-1200 PLCs with firmware version 3. Their work also documented the protocol architecture and processes for setting up PLC connections.

Lv, Xuefeng, et al. (2017) [5] recently suggested a way to decompile and map byte codes into PLC program instructions allowing the understanding the details and the processes that are running in the PLC to the attackers. Yet, the PLC used for the experience was an S7-200, a product already listed as a phase-out product in 2013 (Industry Support Siemens, 2013).

Lim, Bernard, et al. (2017) [6] used some reverse engineering techniques on the Shneider Tricon PLC in order to identify the general structure of the Tricon communication protocol. Then an attack was carried through recalculating packet length, CRC and checksum. This attack affected the device functioning causing a failure that requires a reset of the Tricon PLC. Their experiment showed the effect of such an attack in a real ICS environment.

Cheng et al. (2017) [7] used reverse engineering techniques to identify the three encryption processes happening during the authentication process of the S7 protocol. Through this work, a description of the anti-replay mechanism that is used in the newest version of the S7CommPlus protocol such as the version 4 of the S7-1200 PLC and the most advanced PLC, S7-1500. Yet, there is a lack of details concerning these three encryptions.

Hui, Henry, and al. (2020) [8] presented several ways of exploiting the Siemens S7-1211C PLC, the proprietary protocol, and software, by using simple tools like Windbg and Scapy. Session stealing, phantom PLC, cross connecting PLCs and DoS of S7 communication has been demonstrated. Experiments have been carried out using the most current suite of PLC devices and software available, thus going beyond many published works that investigate now outdated technologies, e.g. the worm that can spread among PLCs (Spenneberg, 2016) and byte code de-compilation (Lv et al., 2017).

In particular, this work uncovered on the potential exploit of the S7-ACK packet.

III. Industrial Intrusion detection systems IIDS

S. Adepu, J. Prakash, and al. (2017) [9] exposed the vulnerabilities associated with the Cyber Physical System (CPS) design using a Software Defined Radio (SDR) for jamming attacks on the SWaT system. The scenario of their experiment consists of an attacker aiming to block the Level 0 and Level 1 of the network communication channels. The Level 0 also referred to as the field-bus network (K. Stouffer, V. Pillitteri, and al. (2015) [10]) consists of the links between the PLC and it's sensors and actuators. While the Level 1 communication consists of the link between the PLC and the SWaT system.

Their work showed that on one hand, jamming the Level 0 communications led the compromised sensors to stop sending data to the PLC. This level of attack was not detected by the operator since no alerts were launched through the SCADA/HMI screen.

On the other hand, jamming the Level 1 communications caused the unit's wireless link to disconnect from the SCADA, HMI and the SWaT Server, which catched the attention of the operator of the communication problem due to the significant impact of the event.

Ahmed, Chuadhry Mujeeb, and al (2017) [11] used the SWaT testbed to detect attacks on physical components of a CPS, their work focused on using ultrasonic level sensors proposing the use of sensor noise fingerprinting to detect such attacks. They started by calculating the noise fingerprint of the sensor. They extracted the data of the sensor from a normal run (where no attack was performed). Then they extracted the noise from these collected data and averaged them to obtain the sensor's fingerprint. This step was repeated for all the sensors. Finally, fresh data will be collected from the SWAT plant and correlated with the sensors noise fingerprints to detect anomalies.

Ahmed, Chuadhry Mujeeb, and al (2017) [11] used two attack types on the sensors: the swap attack, where the attacker changes the sensors levels, and sensor replace attack, where the attacker brings his own sensors and replaces them with the existing ones. Using the fingerprint of the sensors have proven to be efficient in detecting the attacks.

Clotet, Xavier, José Moyano, and al. (2018) [12] proposed an anomaly-based Intrusion Detection System that operates at the industrial control process. Their proposed solution performs a real time intrusion detection that works in two phases. The first phase consists of the IDS learning the normal behavior of the control process, then in the second phase, they raise an alarm whenever an abnormal behavior appears in the system. The IDS system uses two algorithms: the latest version of Negative Selection Algorithm and the Artificial Immune System. The IDS system has been validated using multiple network traffic samples including the dataset provided by the SWaT testbed. The solution proven accuracy of 85% using nominal attack and attacks with no labels.

Ghaleb, Asem, and al. (2018) [13] focused on analyzing the communication between an engineering station and a PLC, where the engineering station is in charge of setting up and configuring the PLC. They used 3 types of attacks: Reply, MITM, and Command Modification. The used PLC was a Siemens S7-400 Simatic PCS7 8.1 software. The results of their experience showed that the programming and configuration traffic between the Engineering Station and the PLC can be replayed, sniffed, and/or modified after successfully executing Reply, MITM, and Command Modification attacks.

Robles-Durazno, Andres, et al. (2019) [14] analyse the impact of network attacks on the area of memory addressed to the PLC inputs. The attacks performed in this research shows that it is possible to disrupt the control system operation bringing the system to an unstable state. The attacks are performed to the input memory of the PLC; however, it should be noted that it is also possible to execute the same attacks to the PLC output. For instance, the attacker could drive the pump at different speeds by overwriting the space of memory addressed to it.

IV. Conclusion

In this paper, we presented several recent works focused on PLC vulnerabilities, these work incorporated the use of multiple models of PLCs, multiple versions of firmwares as well as multiple protocols. We also presented the different Industrial Intrusion detection systems IDS techniques and work recently proposed to help protect the Industrial Control Systems (ICS).

References

[1] Klick, Johannes, et al. ”Internet-facing PLCs as a network backdoor.” 2015 IEEE Conference on Communications and Network Security (CNS). IEEE, 2015.

[2] Wardak, Haroon, Sami Zhioua, and Ahmad Almulhem. ”PLC access control: a security analysis.” 2016 World Congress on Industrial Control Systems Security (WCICSS). IEEE, 2016.

[3] Sandaruwan, G. P. H., P. S. Ranaweera, and Vladimir A. Oleshchuk. ”PLC security and critical infrastructure protection.” 2013 IEEE 8th International Conference on Industrial and Information Systems. IEEE, 2013.

[4] Spenneberg, Ralf, Maik Brüggemann, and Hendrik Schwartke. ”Plc-blaster: A worm living solely in the plc.” Black Hat Asia, Marina Bay Sands, Singapore (2016).

[5] Lv, Xuefeng, et al. ”A technique for bytecode decompilation of PLC program.” 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). IEEE, 2017.

[6] Lim, Bernard, et al. ”Attack induced common-mode failures on plc-based safety system in a nuclear power plant: Practical experience report.” 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC). IEEE, 2017.

[7] Lei, Cheng, Li Donghong, and Ma Liang. ”The spear to break the security wall of S7CommPlus.” Blackhat USA (2017).

[8] Hui, Henry, and Kieran McLaughlin. ”Investigating current plc security issues regarding siemens s7 communications and TIA portal.” 5th International Symposium for ICS SCADA Cyber Security Research 2018 5. 2018.

[9] Adepu, Sridhar, and Aditya Mathur. ”From design to invariants: Detecting attacks on cyber physical systems.” 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2017.

[10] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-82r2.pdf. [Accessed: 27-Apr-2018].

[11] Ahmed, Chuadhry Mujeeb, and Aditya P. Mathur. ”Hardware identification via sensor fingerprinting in a cyber physical system.” 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2017.

[12] Clotet, Xavier, José Moyano, and Gladys León. ”A real-time anomaly-based ids for cyber-attack detection at the industrial process level of critical infrastructures.” International Journal of Critical Infrastructure Protection 23 (2018): 11-20.

[13] Ghaleb, Asem, Sami Zhioua, and Ahmad Almulhem. ”On PLC network security.” International Journal of Critical Infrastructure Protection 22 (2018): 62-69.

[14] Robles-Durazno, Andres, et al. ”PLC memory attack detection and response in a clean water supply system.” International Journal of Critical Infrastructure Protection 26 (2019): 100300.