A survey of offensive security research on PLCs

Rongkuan Ma*, Qiang Wei and Qingxian Wang
State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan 450001 - China

*Corresponding author. Email: big_ma@qq.com

Abstract. Industrial Control Systems (ICSs) are widely deployed in critical infrastructures, such as electric power, water filtration and distribution. Programmable Logic Controllers (PLCs) work as the core components of an ICS. The offensive security technology of PLCs has attracted the popular interests of both attackers and researchers. In this paper, we firstly abstract a 4-layers model of PLC’s implementation, and then summarize and classify attacks against PLCs into 5 types. Further, we point out the features and trends of the related attack studies, which is helpful to promote the research in the ICS security community and provide vital suggestions for defenders.

1. Introduction
Industrial Control Systems (ICSs) are widely deployed in automated industry and critical infrastructures, such as manufacturing, electric power, water filtration and distribution. With the development of Industrial 4.0, Internet Technology (IT) has been deeply embedded in the ICS domains, such as Ethernet communication, operating system, and embedded system. Merging of IT and Operation Technology (OT) has been promoting the development of the industry, at the same time, brought tremendous Internet network attack threats (Stuxnet [1], etc.). Unlike the general goals of traditional cyber-attacks, cyber-attacks against ICS are usually dedicated to destroying physical plants by attacking the controllers in ICS. Programmable Logic Controllers (PLCs) are the control center of an ICS, which can communicate with operators and engineers with Ethernet communication protocols, and monitor and control field devices in the plant, such as waves and sensors. Thus, compromising program logic controllers become the priority goal for ICS attackers.

The offensive security technology of PLCs has attracted the popular interests of both attackers and researchers. Since Stuxnet was revealed, multiple attack events and corresponding malicious code have been found by security researchers. The security research group also participates actively in exploring new attack methodologies and vulnerabilities for finding and solving the security implications before the attackers. Although the researchers have made some progress in vulnerabilities hunting, mitigation, and defense measures, the offensive security technology research of PLC are just in an embryonic stage. In this paper, we survey the literature of offensive security technology of PLCs for promoting the research in the ICS security community and providing vital suggestions for defenders.

2. PLC Implementation Architecture
The implementation of a PLC can be divided into 4 layers abstractly, as shown in Fig.1.
Logic Layer is the top abstract layer of PLC implementation, which define the specific behaviors of devices. In this layer, the logic program is executed by the runtime system periodically. Logic programs are always developed by programmers on an Engineering Workstation (EWS) and downloaded to the PLC. A variety of languages compliance with the IEC61131-3 standard can be used for programmings such as Ladder Logic, Structured Text Language or Function Block Diagram.

Task Layer is the upper abstract of the firmware. We consider the tasks or processes that are in charge of communication, executing logic programs and debugging as the task layer. Among this layer, the runtime system is the main task, which communicates with management systems, executes logic programs, and handles physical inputs and outputs through kernel layers. Other tasks such as web, FTP, telnet or other services also exist in some PLC devices. This layer is the main interface to interact with the outside, thus, it is also the main objective of cyber-attacks.

Kernel Layer is also part of the firmware, which is a clear abstract layer in general-purpose OS-based devices, and not very clear in other devices. It handles the operations of peripherals, scheduling and supporting task layer, or lower-level functionality such as bootloader that initializes and loads the operating system. Adversaries could escalate privilege, deploy rootkit malicious by utilizing flaws in this layer.

Hardware Layer comprises microchips and other electronic components. The key components include microprocessors, volatile memory and non-volatile storage.

3. Overview of PLC Attack Techniques

We divide attack vectors into the following 5 types against abstract implementation layers of PLCs. These attack vectors involve specific features of ICS tightly, such as control logic code, industrial Ethernet protocol, and customized operating system. Attacks against some general IT systems are out of scope due to missing the attack scenario conditions generally in the ICS. For example, Cross-site Scripting (XSS) attack has a huge impact on the Web application systems with a large number of user interactions but has little impact on the intranet system of the ICS.

Attack Type-1: Control Logic Modification. It happens in the logic layer. The functionalities of malicious control logic include safety violations, logic bomb and PLC worms. The malicious logic code can alert a physical control process, for example, closing a wave to cause pressure to rise. A logic bomb could cause the PLC to enter an infinite loop. As a result, the right logic code cannot be executed in scan cycles. PLC worms could contact a Command and Control (C&C) server which can then take control of the PLC remotely, and spread malicious code from one PLC to another PLC.

Attack Type-2: False Data Injection. It happens in the Task layer. A PLC has rich memory management and remote access functions for other entities in an ICS. For example, an operator can close/open a wave by modifying an Output variable to be 0/1. However, the adversary can also utilize
these features to manipulate and damage the physical plants. Such attacks usually utilize inherent flaws of ICS protocol, lack of authentication and encryption.

**Attack Type-III: Software Vulnerability Exploitation.** It also widely exists in the Task layer. PLCs are also embedded devices. Memory corruption is a common class of security vulnerabilities. An adversary usually exploits it to crash a running process and even hijack its execution flow to execute arbitrary code.

**Attack Type-IV: Firmware Modification.** It is another important attack in PLCs. Adversaries can gain system-level access to PLC and take full control of it by firmware modification attack. Firmware modification attacks can be carried out either as standalone attacks or as secondary attacks. Standalone firmware modification attacks utilize firmware update design flaw to inject malicious firmware, and secondary attacks usually follow initial exploitation using traditional attack vectors like memory modification or filesystem attacks to write the faked firmware in the memory of PLC, which can also evade mandatory firmware signature verification.

**Attack Type-V: Rootkit Attack.** It exists at a lower-level in firmware. Malicious rootkit within firmware involves directly manipulating physical pins to alert the control logic by low-level code, which can destroy the physical facilities and hidden from operators. And it is also really hard to detect by some host-based defense mechanism.

4. Academic and Industrial Efforts

*Control logic modification attack* and *false data injection attack (FDI)* have attracted the popular interests of malicious attackers and security researchers, as shown in Table 1. In the real-world attacks, Stuxnet [1] injected malicious logic code to destroy the Iranian nuclear centrifuges and the TRISIS [18] malware implemented a backdoor to allows the adversary to inject the post payloads. In the researches, Langner [3] designed a logic bomb. Naman Govil [17] explored multi kinds of logic bombs against the ControlLogix 5571 PLC. McLaughlin [5, 6] provided a specification-based payload generation method for attacking the physical plant automatically. In blackhat 2015 and 2016, researchers [10, 12] demonstrated the feasibility of constructing a worm malware in a logic program. In 2019, Keliris [19] launched a completely automated process-aware attack. Yoo H and Kalle S, etc., [20, 21] implemented stealthy logic program attack payloads in a PLC. Control logic modification attacks on PLCs tend to be more functionality-rich and stealthy.

Dillon [2] described multi FDI attack vectors on Siemens PLCs in 2011. McLaughlin [9] verified the threat to physical plants. Lei [16] found the strengthened protocols of the Siemens 1200 and 1500 PLC are also vulnerable. Insecure ICS protocols are still the main cause of PLC being vulnerable to FDI attacks in practice [13, 15].

**Software vulnerability exploitation and Firmware modification attack** have also been studied in the early years. Magnus Almgren [4] has tried to implement a fuzzing tool based on ICS protocol and found some new problems. J. Butts [7, 8] provided a methodology to modify the firmware of a PLC. A. Garcia [14] constructed a physic-aware malicious firmware to attack the power grid. Cheng P [22] combined several software vulnerability exploitations and firmware modification vulnerabilities to launch a stealthy attack against redundant controller architecture systems.

**Rootkit attack** in the PLC is harmful and difficult to detect. Ali [11] provided a pin control attack utilizing the flaw of the GPIO subsystem in the Linux kernel. Luis [14] injected the rootkit to hijack the input/output of PLC by modifying the low-level binary code of firmware.

| Study          | Year | Sector       | Attack Types Involved | I | II | III | IV | V |
|---------------|------|--------------|-----------------------|---|----|-----|----|---|
| Langner [1]   | 2011 | Siemens PLCs | √                     |   |    |     |    |   |
| Dillon [2]    | 2011 | Siemens PLCs | √ √                  |   |    |     |    |   |
5. Summary
In this paper, we surveyed offensive security technology of PLCs from 2011. Based on the 4-layers abstract model, we firstly summarize and classify attacks against PLCs into 5 types. Further, we point out the features and trends of the related attack studies, which will be helpful to security research in this area.

Acknowledgement
This research was supported by a grant from the National Key R&D Program of China (No. 2020YFB2010902).

References
[1] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” IEEE Security & Privacy, vol. 9, no. 3, pp. 49–51, 2011.
[2] D. Beresford, “Exploiting siemens simatic s7 PLCs,” Black Hat USA, vol. 16, no. 2, pp. 723–733, 2011.
[3] R. Langner, “A time bomb with fourteen bytes,” https://www.langner.com/2011/07/atime-bomb-with-fourteen-bytes/, 2011.
[4] M. Almgren, “Report on automated vulnerability discovery techniques,” http://www.crisalis-project.eu/sites/crisalisproject.eu/files/crisalis deliverable-D5.3.pdf/, 2011.
[5] S. E. McLaughlin, “On dynamic malware payloads aimed at programmable logic controllers.” in HotSec, 2011.
[6] S. McLaughlin and P. McDaniel, “Specification-based payload generation for programmable logic controllers,” in Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 439–449.
[7] Z. Basnight, J. Butts, J. Lopez Jr, and T. Dube, “Firmware modification attacks on programmable logic controllers,” International Journal of Critical Infrastructure Protection, vol. 6, no. 2, pp. 76–84, 2013.
[8] C. Schuett, J. Butts, and S. Dunlap, “An evaluation of modification attacks on programmable logic controllers,” International Journal of Critical Infrastructure Protection, vol. 7, no. 1, pp. 61–68, 2014.

[9] McLaughlin S, Zonouz S. Controller-aware false data injection against programmable logic controllers[C]//2014 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, 2014.

[10] J. Klick, S. Lau, D. Marzin, J.-O. Malchow, and V. Roth, “Internet-facing plcs-a new back orifice,” Blackhat USA, 2015.

[11] A. Abbasi, M. Hashemi, E. Zambon, and S. Etalle, “Stealth low-level manipulation of programmable logic controllers i/o by pin control exploitation,” in International Conference on Critical Information Infrastructures Security. Springer, 2016, pp. 1–12.

[12] R. Spenneberg, M. Brüggemann, and H. Schwartke, “Pcc-blaster: A worm living solely in the PLC,” Black Hat Asia (p. N/A), 2016.

[13] S. Senthivel, I. Ahmed, and V. Roussev, “Scada network forensics of the pccc protocol,” Digital Investigation, vol. 22, pp. S57–S65, 2017.

[14] L. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. A. Mohammed, and S. A. Zonouz, “Hey, my malware knows physics! attacking plcs with physical model aware rootkit,” in NDSS, 2017.

[15] A. Ghaleb, S. Zhioua, and A. Almulhem, “On PLC network security,” International Journal of Critical Infrastructure Protection, vol. 22, pp. 62 – 69, 2018.

[16] C. Lei, L. Donghong, and M. Liang, “The spear to break the security wall of s7commplus,” Blackhat USA, 2017.

[17] Govil N, Agrawal A, Tippenhauer N O. On ladder logic bombs in industrial control systems[M]//Computer Security. Springer, Cham, 2017: 110-126.

[18] A. C. Alessandro Di Pinto, Younes Dragoni, “Triton: The first ICS cyber attack on safety instrument systems,” Black Hat USA, 2018.

[19] Anastasis Keliris, and Michail Maniatakos, "ICSREF: A Framework for Automated Reverse Engineering of Industrial Control Systems Binaries", in NDSS, 2019.

[20] Yoo H, Ahmed I. Control logic injection attacks on industrial control systems[C]//IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, Cham, 2019: 33-48.

[21] Kalle S, Ameen N, Yoo H, et al. Clik on plcs! attacking control logic with decompilation and virtual plc[C]//Binary Analysis Research (BAR) Workshop, Network and Distributed System Security Symposium (NDSS). 2019.

[22] Ma R, Cheng P, Zhang Z, et al. Stealthy attack against redundant controller architecture of industrial cyber-physical system[J]. IEEE Internet of Things Journal, 2019, 6(6): 9783-9793.