Chapter 10

THREAT ANALYSIS OF AN ELEVATOR CONTROL SYSTEM

Raymond Chan and Kam-Pui Chow

Abstract Programmable logic controllers are key components of industrial control systems that are used across the critical infrastructure. The infamous Stuxnet malware attacked programmable logic controllers that managed uranium hexafluoride centrifuges in Iran's Natanz facility, causing the centrifuges to operate outside their designed limits while leading plant operators to believe all was well. This attack and others have rendered the task of securing programmable logic controllers an important problem. Most research in the area has focused on network-level intrusion detection and protection mechanisms. Few research efforts have specifically considered threats to the internal networks of industrial control systems, which include connections from the computer platforms that manage programmable logic controllers. This chapter analyzes the threats to the internal environment of an elevator control system that engages a Siemens programmable logic controller. Several approaches for mitigating the threats are presented.

Keywords: Programmable logic controllers, elevator control, threats, mitigation

1. Introduction

Industrial control systems are used across the critical infrastructure to manage physical processes. Industrial control systems include supervisory control and data acquisition (SCADA) systems and distributed control systems (DCSs), both of which incorporate component devices such as programmable logic controllers (PLCs). Programmable logic controllers are connected to human-machine interfaces (HMIs) to enable command and control by human operators and to engineering/development workstations for configuration, programming and diagnostics. Programmable logic controllers commonly execute ladder logic programs to perform their monitoring and control activities.

Traditionally, industrial control systems operated using proprietary protocols in closed (air-gapped) networks. However, many industrial control net-

M. Rice and S. Shenoi (Eds.): Critical Infrastructure Protection XI, IFIP AICT 512, pp. 175–192, 2017.
https://doi.org/10.1007/978-3-319-70395-4_10

works are now connected to external networks – even the Internet – to support remote operations, configuration and diagnostics. This exposes industrial control systems and the critical assets they manage to external attacks in addition to attacks by malicious insiders.

Several issues impact the security of industrial control systems. One is that engineers and operators are more concerned about availability than security. Another is the lack of a security mindset. Yet another is the fact that the scale, complexity and diversity of industrial control systems render the implementation of security mechanisms extremely cost-prohibitive. Moreover, adding extra layers of protection can significantly affect the performance and reliability of industrial control systems – asset owners and operators are reluctant to implement security mechanisms that can affect command and control.

Stuxnet has demonstrated that a sophisticated adversary can gain access to an extremely well-protected industrial control network. Once inside the network, the adversary can leverage the fact that programmable logic controllers, because they have limited memory and processing power, are unable to implement security controls such as encryption and intrusion detection. This makes it possible to extract and reprogram the ladder logic to change the behavior of the control system.

This research focuses on programmable logic controllers, arguably the most vulnerable components of industrial control systems. It analyzes the threats to the internal environment of an elevator control system that engages a Siemens programmable logic controller and presents a proof-of-concept program that demonstrates the feasibility of attacks. Also, it describes several approaches for mitigating the threats to the elevator control system.

2. Related Work

Considerable research has focused on industrial control system security (see, e.g., [9]) and managing the risks (see, e.g., [15]). Hadziosmanovic et al. [6] discuss the challenges involved in protecting industrial control system hosts and networks. Several high-level solutions have been developed for protecting industrial control systems (see, e.g., [12, 14]). Wei and Ji [17] have proposed a three-layer architecture for enhancing the security and reliability of industrial control systems. Cohen [4] has specified a reference architecture and guidelines for securing industrial control networks. Jie and Li [7] have analyzed industrial control system security risks and have proposed strategies for protecting control devices. Ghena et al. [5] have leveraged wireless access to maliciously control traffic lights. These research efforts discuss security problems and solutions for industrial control systems, but ignore threats to the internal networks of industrial control systems.

Several researchers have focused on discovering vulnerabilities in industrial control networks. Beresford [2] has analyzed the Siemens S7 protocol and has developed exploits that target Siemens programmable logic controllers. In particular, Beresford demonstrated that it is possible to bypass the authentication protocol and perform memory-read, write-logic and other attacks. Timorin [16]

has demonstrated how to capture S7 challenge-response messages and perform replay attacks. Also, Timorin has analyzed the Siemens Total Integrated Automation (TIA) Portal project file, and has shown how to extract the SHA-protected password and change user permissions in the file. Korkmaz et al. [8] have discovered a time delay attack on a control system that could result in the failure of an entire power generation facility. Abe et al. [1] have identified several cyber attacks on Internet-connected control systems; these attacks leverage malware that sends STOP and RESET commands to programmable logic controllers, negatively impacting the industrial control system and the underlying process.

Cardenas et al. [3] have specified a threat model that covers outsider attacks, key-compromise attacks and insider attacks on SCADA systems. Hadziosmanovic et al. [6] have classified industrial control system threats into system-related threats and process-related threats. McLaughlin and Zonouz [11] have introduced a threat model that covers the use of any industrial control system component to upload malicious code to a programmable logic controller. Malchow et al. [10] have proposed a threat model that covers a scenario where an adversary can control an engineering workstation using malware and inject malicious code into a programmable logic controller.

In general, most industrial control system security approaches focus on redesigning the entire architecture or incorporating security mechanisms throughout the architecture. In the case of operational industrial control systems, there are certain latent security problems, especially pertaining to the internal environment, which often has fewer security mechanisms than external networks – examples are the development zone and human-machine control zone. As a result, this research seeks to identify potential vulnerabilities that enable practical and reproducible attacks on the internal networks of industrial control systems. An elevator control system is used as a case study because it is small and ubiquitous, but still a representative, real-world industrial control system. Additionally, the elevator system has several sensors and safety protection mechanisms that can be targeted to cause harm.

3. Threat Model

This research assumes that an adversary can gain access to the internal network of an industrial control system by various means and is able to launch attacks. The attacks are assumed to target: (i) confidentiality; (ii) integrity; or (iii) availability. The proposed threat model focuses on Siemens programmable logic controllers. The model considers the attack capabilities of an adversary upon gaining access to an industrial control network; these capabilities are in addition to implanting malware on a programmable logic controller. In general, it is difficult for an adversary to enter an industrial control network via a phishing email, external USB thumb drive or even as an insider.

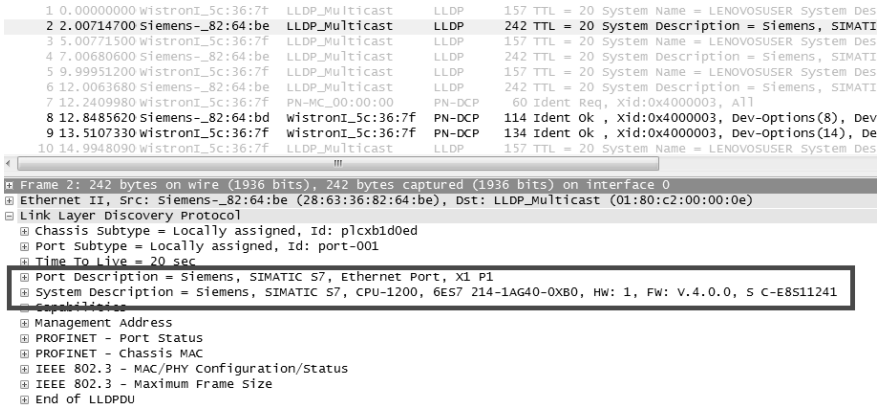

Figure 1. Leveraging LLDP broadcast messages to discover device information.

3.1 Confidentiality Threats

Most industrial control systems do not use encryption and authentication. As a result, an adversary who has access to a network and captures communications data can perform the following attacks:

- **Programmable Logic Controller Discovery Attack:** An adversary can discover all the programmable logic controllers in an internal industrial control network by connecting to the network and capturing network packets using a tool such as Wireshark. Figure 1 illustrates the network packet capture process in the case of a Siemens programmable logic controller that uses the Link Layer Discovery Protocol (LLDP) to broadcast its presence. Important information such as the MAC address, model number, CPU information, hardware information and firmware information are transferred in plaintext. An adversary who captures the internal network traffic can easily obtain detailed information about the programmable logic controllers that could be used to plan specific attacks.

- **False Command or Signal Injection Attack:** Most industrial control system designs assume that all the devices operate in a trusted and closed network. No encryption and authentication mechanisms are implemented between human-machine interfaces and programmable logic controllers. Moreover, many human-machine interfaces and programmable logic controllers are connected to external networks, including the Internet. An adversary who accesses the network interface could inject various control commands. For example, injecting a STOP or RESET command would move a programmable logic controller to the STOP mode and the controller would not operate until it receives a START command.

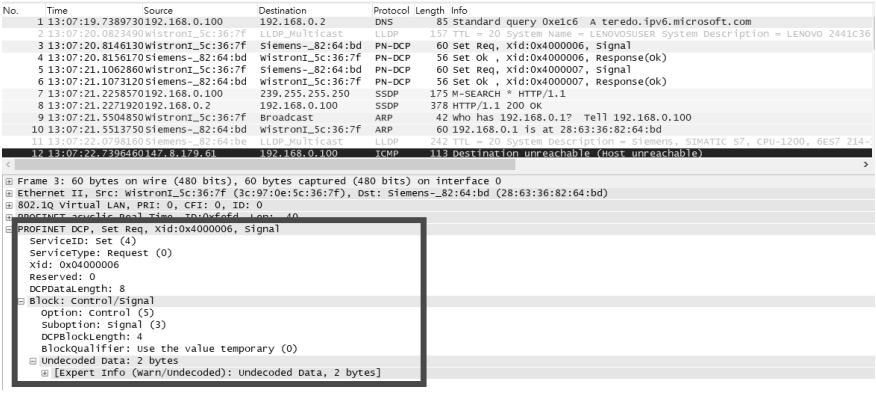

Figure 2. Manipulating the LED of a programmable logic controller.

Many programmable logic controllers in production systems have been operational for several years and often have outdated firmware. McLaughlin and Zonouz [11] have developed the CaFDI tool that sends false data to programmable logic controllers. Abe et al. [1] have demonstrated that sending a STOP or RESET command is adequate to disrupt most programmable logic controllers. An adversary could also send a fake sensor input signal in order to alter an output, potentially causing the entire industrial control system to crash [13].

A personal computer installed with the Siemens Step 7 software can send a discovery command to flash the LED light of a Siemens PLC, leading the operator to believe that the programmable logic controller is malfunctioning. Figure 2 shows the command sent from a personal computer to manipulate the LED of a Siemens programmable logic controller.

- **Ladder Logic Program Leakage Attack:** A ladder logic program specifies how a programmable logic controller should process input signals and generate responses in the form of output signals. A Siemens programmable logic controller implements a control command that enables an engineer to download the ladder logic program from the controller. An adversary who has the requisite access can request the programmable logic controller to send its ladder logic program, enabling the adversary to access and reverse engineer the program.

3.2 Integrity Threats

As mentioned above, programmable logic controllers usually do not implement any authentication checks. An adversary who knows the IP address of a programmable logic controller could seize control of the device and transmit

messages. The operator at the human-machine interface would be unable to determine that the messages do not come from an authorized entity.

The following attacks target the integrity of an industrial control system:

- **Response Injection Attack:** Since it is not possible to determine whether or not a message is sent by an authorized programmable logic controller, an adversary can execute a man-in-the-middle attack and inject or alter a response message variable or sensor value sent by a programmable logic controller to display false information on a human-machine interface. Any number of replay attacks are also possible.

- **Ladder Logic Modification Attack:** No authentication checks are performed when uploading a ladder logic program from a development workstation to a programmable logic controller. Thus, an adversary to can create a malicious ladder logic program and upload it to the programmable logic controller so that it replaces the original program. This is possible because no software attestation or protection mechanisms are implemented to verify that the new ladder logic program is authentic. If the new ladder logic program sends valid outputs to the human-machine interface, a behavior-based protection mechanism would be unable to detect the attack at the network level.

3.3 Availability Threats

Programmable logic controllers are devices with low processing power that are designed to operate in real time. It is possible to send malformed packets that delay or disrupt the responses of a programmable logic controller. An example attack on availability is:

- **Denial-of-Service Attack:** One type of denial-of-service attack involves the transmission of malicious commands or packets that delay the response or even crash a programmable logic controller. Another type of attack targets the human-machine interface by installing malware on programmable logic controllers. In this case, an adversary uploads malicious ladder logic programs to all the programmable logic controllers in the industrial control network. When certain attack criteria are satisfied (e.g., time or process conditions), the programmable logic controllers could be made to disrupt the human-machine interface by simultaneously sending it malicious packets.

4. Elevator System Case Study

An elevator system testbed was used to validate the proposed threat model and demonstrate the feasibility of attacks.

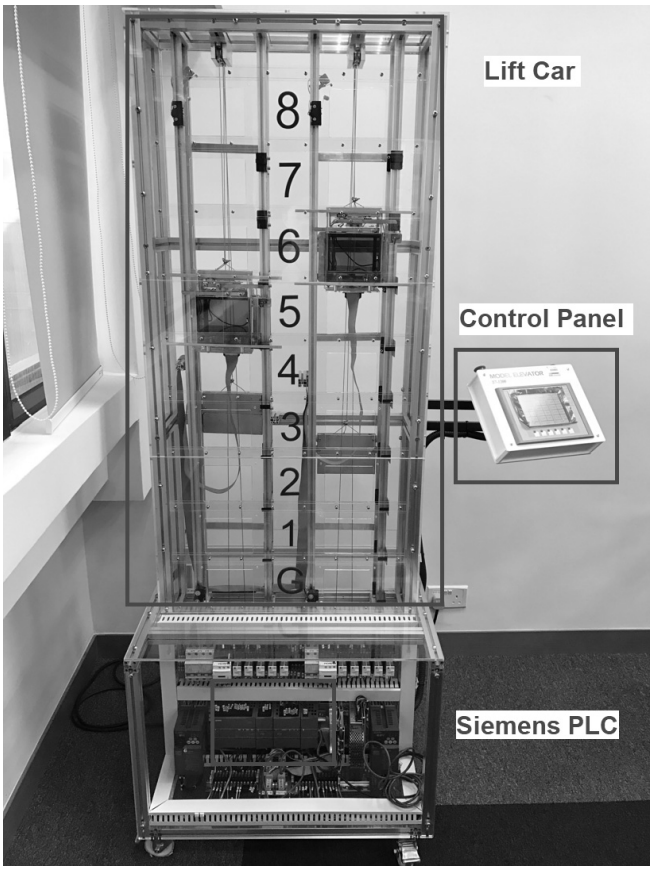

Figure 3. Elevator system testbed.

4.1 Experimental Setup

Figure 3 presents the elevator system testbed used in the experiments. The control circuit of the model elevator system comprised a DC power supply, programmable logic controller, magnetic circuit breaker contactors, relays and variable frequency drives. The control circuit provided an interface for controlling high power devices (e.g., three-phase AC motor) via small control signals transmitted by the programmable logic controller. The KTP600 Control Panel served as the human-machine interface for an operator to obtain status data and control elevator operation. A personal computer installed with the Siemens TIA Portal and connected to the switch of the elevator system (i.e., internal network) was assumed to be exploited by the adversary to launch attacks.

The programmable logic controller was configured to control the model elevator. The model elevator system had two cars that operated over nine floors. Sensors were located on every floor for elevator car positioning. As in a typical modern passenger elevator, the model had two call buttons (car call and hall call) to choose a floor. Door controls were incorporated to close or reopen the doors. An object in the path of the moving doors was detected by sensors or were handled by manually activating a switch that reopened the doors. Otherwise, the elevator doors closed after a preset time.

A driving mechanism moved the elevator car up and down. The elevator control system coordinated the movements of the two elevator cars to provide optimal service by reducing passenger wait times.

In the experiments, the ladder logic program for elevator control was uploaded to the Siemens S7-1200 programmable logic controller (Firmware v4.0) using the Siemens TIA Portal v13. The Siemens S7-1200 programmable logic controller is one of the popular models available in the market and has been deployed in numerous infrastructure assets.

The experiments assumed that the adversary had installed malware in the personal computer connected to the elevator switch, which enabled him to discover, monitor and control the programmable logic controller in the elevator system. Specifically, the adversary could perform three actions: (i) discover the presence of the programmable logic controller in the network; (ii) query information about the programmable logic controller; and (iii) launch attacks to control and crash the programmable logic controller.

4.2 S7 Base Protocol and Configuration

The S7 base protocol is used by Siemens programmable logic controllers for communications. The protocol has been exploited by Beresford [2] and several third-party software tools are available to control Siemens programmable logic controllers. Starting with Firmware V4.0, Siemens updated the S7 protocol (S7 Plus) for the Siemens S7-1200/1500 programmable logic controller model to provide additional security features. However, this research discovered that the S7 base protocol can still be used to query and command a new programmable logic controller due to the design decision to maintain compatibility with older versions. In particular, the experiments used the S7 base protocol to retrieve information from the programmable logic controller and then change its behavior.

The S7 base protocol incorporates commands for querying and changing the digital inputs (PA) and digital outputs (PE) of the programmable logic controller. No configuration settings were available for protecting access to the PA and PE entries. In fact, this research discovered that the S7 base protocol could be used to communicate with the programmable logic controller without the authentication checks required by the new S7 protocol implemented in the controller. Indeed, the experiments confirmed that the new S7 protocol does not provide any protection to the digital inputs or outputs when the base protocol is used.

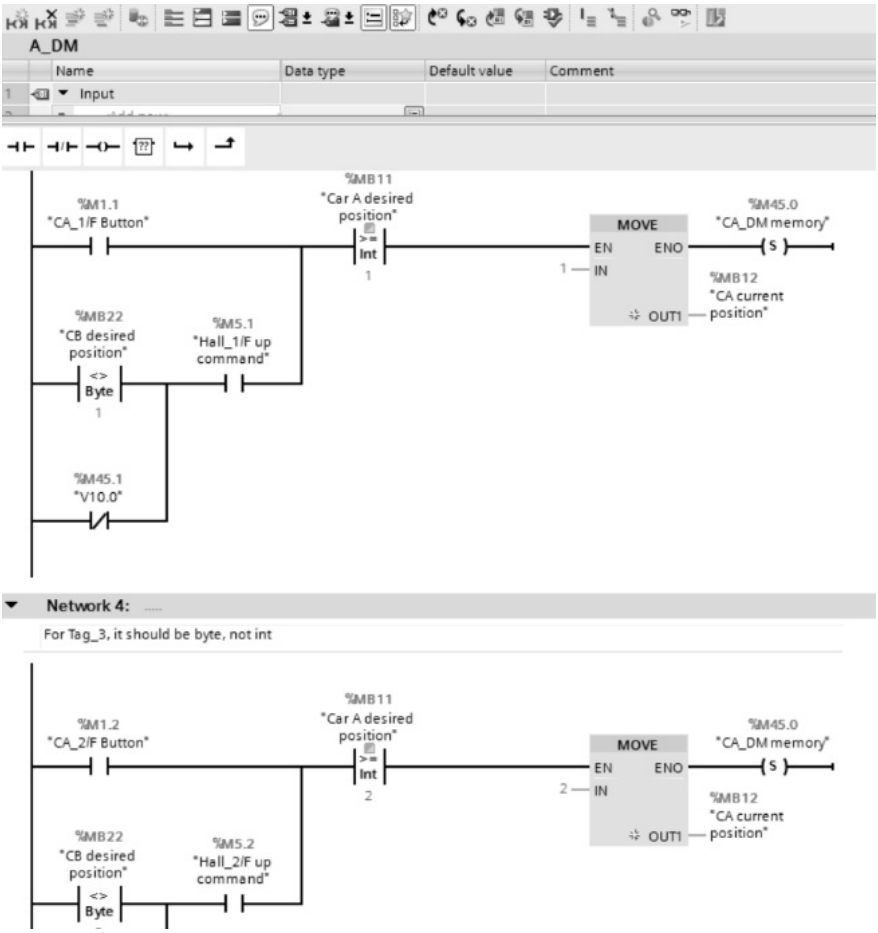

Figure 4. Ladder logic program used by the elevator system.

Based on these findings, a proof-of-concept ladder logic program was developed to send S7 base protocol commands to change the behavior of the elevator system. Figure 4 shows the ladder logic program that manages the elevator system. Figure 5 shows the attack entry point to the elevator system.

4.3 PLC Discovery Attack

As discussed in the section on confidentiality threats, an adversary has to first locate the personal computer with Siemens Step 7 installed and the Siemens programmable logic controller in the internal industrial control network. Information about these devices may be collected in a passive or ac-

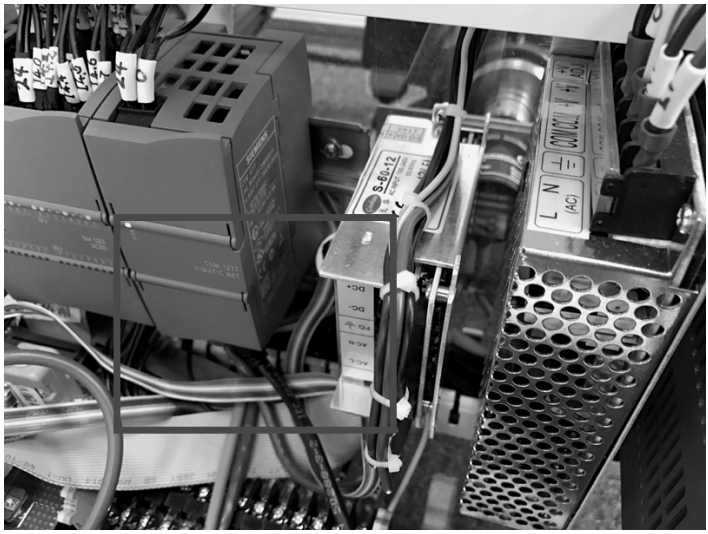

Figure 5. Attack entry point to the elevator system.

tive manner. In the passive collection mode, the personal computer and programmable logic controller broadcast their information to the network periodically using LLDP, which enables the adversary to capture and analyze LLDP packets to identify the devices. In the active collection mode, the adversary uses the PROFINET Discovery and Basic Configuration Protocol (PN-DCP) to query and determine the existence of the personal computer and programmable logic controller [16],

The proof-of-concept program developed in this research sends PN-DCP messages to the network devices and captures and analyzes the response packets to identify the devices of interest. The model information and IP addresses of the devices were obtained by sending simple PN-DCP broadcast packets. Figure 6 shows the response packets from the programmable logic controller that were captured by Wireshark.

4.4 False Command Injection Attack

After the programmable logic controller was discovered, the proof-of-concept program attempted to modify the behavior of the elevator system by sending a write command to the PA entry of the programmable logic controller. After the input value was changed, the programmable logic controller responded to the input according to its ladder logic program. The injected input signal requested the elevator to go to a different floor; this injected signal was the same as the signal that would be sent upon pressing the car call button on the control panel. Figure 7 shows how the proof-of-concept program used the S7 base protocol

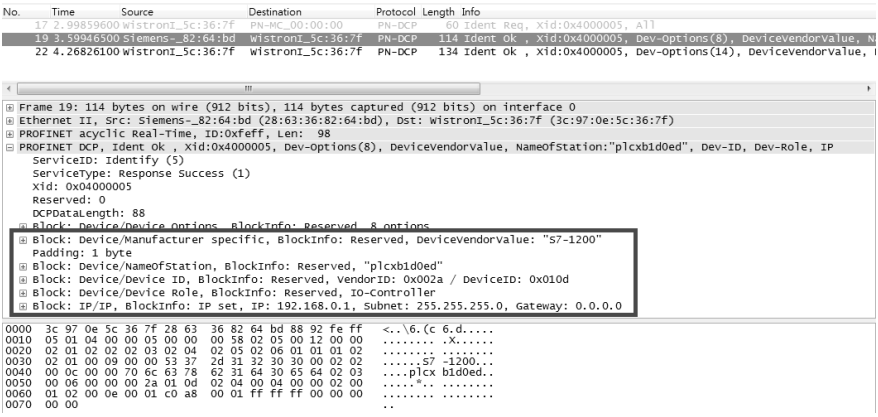

Figure 6. Discovering programmable logic controller information via PN-DCP.

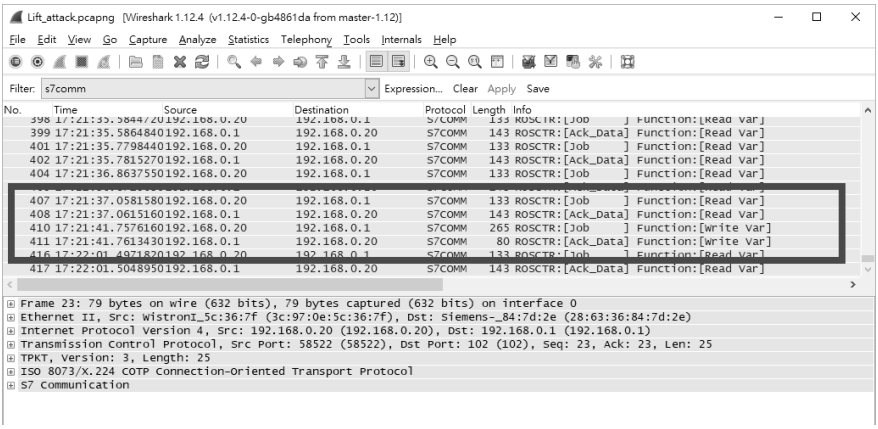

Figure 7. Using the S7 base protocol to read and write data.

read-variable and write-variable commands to query and manipulate the status of the programmable logic controller.

4.5 Control Signal Injection Attack

The false input command injection attack changed the behavior of the elevator system by sending a write command to the PE entry of the programmable logic controller. An output (control) signal injection attack is more harmful. This attack can change the power output directly, which means that the programmable logic controller would behave differently from the manner specified by its ladder logic program. In the case of the elevator, the false command in-

Figure 8. Stopping the elevator car between two floors.

jection attack merely moved the elevator in the same way as when the control panel is used. However, the output control signal injection attack can force the elevator to stop between two floors. Figure 8 shows the result – the elevator car stopped between the fifth and sixth floors after the false control signal was sent to the programmable logic controller.

4.6 Control Variable Injection Attack

A ladder logic program contains a number of variables called programmable logic controller tags that control or perform various operations. An adversary who is able to control the personal computer with the TIA Portal installed would be able to obtain the running ladder logic (including the variables and their addresses) using the Download from PLC function.

In the case of the model elevator system, after the downloaded ladder logic program was modified and uploaded to the programmable logic controller, it was possible to fully control the elevator, including making it function improperly. In the experiments, the buzzer variable was changed from false to true,

	Name	Data type	Address	Retain	Visibl...	Acces...	Monitor value
86	Hall_ 8/F down command	Bool	%M8.0		☑	☑	FALSE
87	Hall_ 7/F down command	Bool	%M7.7		☑	☑	FALSE
88	Hall_ 6/F down command	Bool	%M7.6		☑	☑	FALSE
89	Hall_ 5/F down command	Bool	%M7.5		☑	☑	FALSE
90	Hall_ 4/F down command	Bool	%M7.4		☑	☑	FALSE
91	Hall_ 3/F down command	Bool	%M7.3		☑	☑	FALSE
92	Hall_ 2/F down command	Bool	%M7.2		☑	☑	FALSE
93	Hall_ 1/F down command	Bool	%M7.1		☑	☑	FALSE
94	Hall_G/F down command	Bool	%M7.0		☑	☑	FALSE
95	Hall_8/F up command	Bool	%M6.0		☑	☑	FALSE
96	Hall_7/F up command	Bool	%M5.7		☑	☑	FALSE
97	Hall_6/F up command	Bool	%M5.6		☑	☑	FALSE
98	Hall_5/F up command	Bool	%M5.5		☑	☑	FALSE
99	Hall_4/F up command	Bool	%M5.4		☑	☑	FALSE
100	Hall_3/F up command	Bool	%M5.3		☑	☑	FALSE
101	Hall_2/F up command	Bool	%M5.2		☑	☑	FALSE
102	Hall_1/F up command	Bool	%M5.1		☑	☑	FALSE
103	Hall_G/F up command	Bool	%M5.0		☑	☑	FALSE
104	CB_door closing request	Bool	%M4.3		☑	☑	FALSE
105	CB_door_open request	Bool	%M4.2		☑	☑	FALSE
106	CB overload alert	Bool	%M4.1		☑	☑	FALSE
107	CB_8/F Button	Bool	%M4.0		☑	☑	FALSE
108	CB_7/F Button	Bool	%M3.7		☑	☑	FALSE
109	CB_6/F Button	Bool	%M3.6		☑	☑	FALSE
110	CB_5/F Button	Bool	%M3.5		☑	☑	FALSE
111	CB_4/F Button	Bool	%M3.4		☑	☑	FALSE

Figure 9. Variables used to store commands.

which caused the buzzer to sound forever. The current position of the elevator was also changed while it was moving, which caused the elevator to move to the wrong floor. Note that these variables cannot be configured as read-only as a security measure because the human-machine interface must be able to change the values of variables during normal operations. Figure 9 shows some of the programmable logic controller variables in the TIA Portal that are used to command the elevator. Figure 10 shows the current and desired positions of the elevator while it was moving.

4.7 Sensor Value Response Modification Attack

Sensor values are stored as programmable logic controller tags. These values can be changed to negatively impact the elevator logic. Since the communications between the sensor and programmable logic controller are neither encrypted nor authenticated, the ladder logic program of the programmable logic controller would then execute based on the changed sensor values. In the experiments, the door light sensor value was changed, which prevented the elevator control system from detecting that something was jammed between the doors and the elevator kept trying to close the doors. Figure 11 shows the sensor variables in the TIA Portal that may be modified in sensor value response modification attacks.

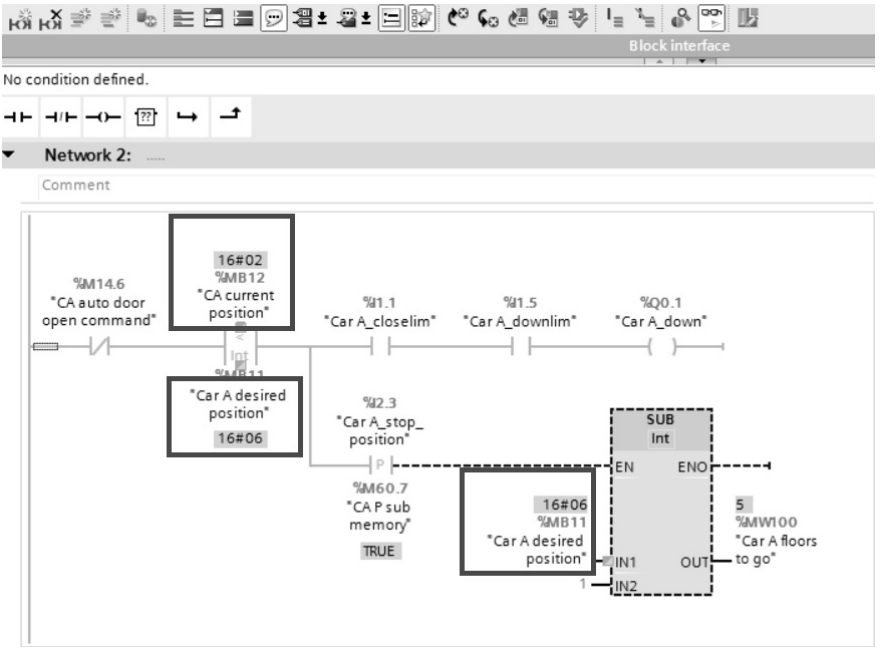

Figure 10. Variables used to store the current and desired elevator positions.

	Name	Data type	Address	Retain	Visibl...	Acces...	Monitor value
162	CA_UM memory	Bool	%M45.5		☑	☑	FALSE
163	CB_DM memory	Bool	%M45.6		☑	☑	FALSE
164	CB_TM memory	Bool	%M45.7		☑	☑	FALSE
165	CB_UM memory	Bool	%M46.0		☑	☑	FALSE
166	Car B floors to go	Word	%MW102		☑	☑	16#0006
167	Car A floors to go	Int	%MW100		☑	☑	6
168	Car A sensor 1 memery	Bool	%M74.0		☑	☑	TRUE
169	Car A sensor 2 memory	Bool	%M74.1		☑	☑	TRUE
170	Car A sensor 3 memory	Bool	%M74.2		☑	☑	TRUE
171	Car A sensor 4 memory	Bool	%M74.3		☑	☑	FALSE
172	Car B sensor 1 memory	Bool	%M72.0		☑	☑	FALSE
173	Car B sensor 2 memory	Bool	%M72.1		☑	☑	FALSE
174	Car B sensor 3 memory	Bool	%M72.2		☑	☑	FALSE
175	Car Bsensor 4 memory	Bool	%M72.3		☑	☑	FALSE
176	Car B STOP_S	Bool	%M72.4		☑	☑	FALSE
177	Car A STOP_S	Bool	%M74.4		☑	☑	TRUE
178	CA_floor alarm memory	Bool	%M43.0		☑	☑	FALSE
179	CB_floor alarm memory	Bool	%M43.1		☑	☑	FALSE
180	disabled alarm button	Bool	%M43.2		☑	☑	FALSE
181	CA_buzzer limit	Bool	%M43.3		☑	☑	FALSE
182	CB_buzzer limit	Bool	%M43.4		☑	☑	FALSE

Figure 11. Sensor variables in the TIA Portal.

4.8 Discussion and Recommendations

Current programmable logic controller security mechanisms are inadequate for combating malicious attacks. All workstations and personal computers installed with the Siemens TIA Portal and located in an internal control network are attractive targets for attacks. As shown in Figure 1, an adversary can discover these computing platforms by capturing and analyzing LLDP packets.

Installing sensors throughout an industrial control network provides situational awareness about attacks and anomalies, but sophisticated adversaries can tamper with the sensor values and send false commands and signals to programmable logic controllers. Because of the complexity of industrial control systems and their underlying physical processes, network intrusion detection and prevention systems have obvious limitations. A promising solution is to encrypt and authenticate all communications involving human-machine interfaces, programmable logic controllers and engineering/development workstations. This is especially important because future industrial control system attacks will go beyond utilizing an engineering workstation to download malicious ladder logic programs and seek to control and attack the programmable logic controllers directly.

Programmable logic controller protection mechanisms also must be enhanced because adversaries can exploit the S7 base protocol and bypass the security configurations to execute attacks. The S7 base protocol should be locked down in modern versions of Siemens programmable logic controllers. In the case of the Siemens TIA Portal, the PE and PA entries in programmable logic controllers should be configured to provide adequate security.

Figure 12 shows that malware can easily discover the development personal computer by capturing and analyzing LLDP packets. Having discovered the personal computer, the adversary could attempt to gain access to it. Firewalls or other network filtering mechanisms must be deployed to block these protocol packets so that it is more difficult to discover devices in an industrial control network.

The following recommendations are made to secure the internal network of an industrial control system:

- The development personal computer should be well protected. External device and Internet connections should be disabled to prevent malware attacks.
- Firewalls should be deployed to ensure that discovery and control commands only come from authorized devices.
- Multiple programmable logic controllers from different vendors should be employed in order to survive attacks that target a specific programmable logic controller model or brand.
- Logging and heartbeat mechanisms should be incorporated in ladder logic programs to detect unauthorized modifications.

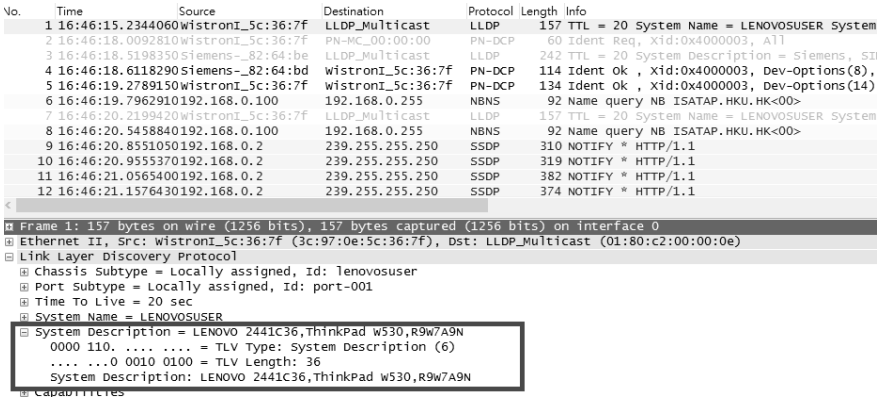

Figure 12. Using the Siemens TIA Portal to obtain information via LLDP.

- Industrial control engineers must be cognizant of programmable logic controller vulnerabilities and potential attacks.

5. Conclusions

The vast majority of research in industrial control system security has focused on network-level intrusion detection and protection mechanisms. In contrast, this research has specifically considered the threats to the internal networks of industrial control systems, which include the connections from the computer platforms that manage programmable logic controllers. The threat model assumes that an adversary can gain access to the internal network of an industrial control system by various means and specifies several attacks on the confidentiality, integrity and availability of programmable logic controllers. Experiments involving a model elevator system with a Siemens programmable logic controller demonstrate the potential attacks and their impacts, and provide guidance for implementing security solutions that can mitigate the attacks.

Future research will concentrate on a larger testbed with programmable logic controllers from different vendors. Additionally, efforts will be directed at developing lightweight security solutions for programmable logic controllers that satisfy the real-time constraints of production industrial control systems.

References

[1] S. Abe, M. Fujimoto, S. Horata, Y. Uchida and T. Mitsunaga, Security threats of Internet-reachable ICSs, *Proceedings of the Fifty-Fifth Annual Conference of the Society of Instrument and Control Engineers of Japan*, pp. 750–755, 2016.

[2] D. Beresford, Exploiting Siemens Simatic S7 PLCs, presented at *Black Hat USA*, 2011.

[3] A. Cardenas, T. Roosta and S. Sastry, Rethinking security properties, threat models and the design space in sensor networks: A case study in SCADA systems, *Ad Hoc Networks*, vol. 7(8), pp. 1434–1447, 2009.

[4] F. Cohen, A reference architecture approach to ICS security, *Proceedings of the Fourth International Symposium on Resilient Control Systems*, pp. 21–25, 2011.

[5] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek and J. Haldeman, Green lights forever: Analyzing the security of traffic infrastructure, *Proceedings of the Eighth USENIX Workshop on Offensive Technologies*, 2014.

[6] D. Hadziosmanovic, D. Bolzoni, S. Etalle and P. Hartel, Challenges and opportunities in securing industrial control systems, *Proceedings of the Workshop on Complexity in Engineering*, 2012.

[7] P. Jie and L. Li, Industrial control system security, *Proceedings of the International Conference on Intelligent Human-Machine Systems and Cybernetics*, vol. 2, pp. 156–158, 2011.

[8] E. Korkmaz, A. Dolgikh, M. Davis and V. Skormin, ICS security testbed with delay attack case study, *Proceedings of the IEEE Military Communications Conference*, pp. 283–288, 2016.

[9] M. Krotofil and D. Gollmann, Industrial control systems security: What is happening? *Proceedings of the Eleventh IEEE International Conference on Industrial Informatics*, pp. 670–675, 2013.

[10] J. Malchow, D. Marzin, J. Klick, R. Kovacs and V. Roth, PLC Guard: A practical defense against attacks on cyber-physical systems, *Proceedings of the IEEE Conference on Communications and Network Security*, pp. 326–334, 2015.

[11] S. McLaughlin and S. Zonouz, Controller-aware false data injection against programmable logic controllers, *Proceedings of the IEEE International Conference on Smart Grid Communications*, pp. 848–853, 2014.

[12] T. Miyachi and T. Yamada, Current issues and challenges on cyber security for industrial automation and control systems, *Proceedings of the SICE Annual Conference*, pp. 821–826, 2014.

[13] Y. Mo and B. Sinopoli, False data injection attacks in control systems, presented at the *First Workshop on Secure Control Systems*, 2010.

[14] R. Piggin, Emerging good practice for cyber security of industrial control systems and SCADA, *Proceedings of the Seventh IET International Conference on System Safety*, 2012.

[15] T. Spyridopoulos, T. Tryfonas and J. May, Incident analysis and digital forensics in SCADA and industrial control systems, *Proceedings of the Eighth IET International System Safety Conference*, 2013.

[16] A. Timorin, SCADA deep inside: Protocols and security mechanisms, presented at the *Balkan Computer Congress*, 2014.

[17] D. Wei and K. Ji, Resilient industrial control system (RICS): Concepts, formulation, metrics and insights, *Proceedings of the Third International Symposium on Resilient Control Systems*, pp. 15–22, 2010.