Defining Attack Patterns for Industrial Control Systems

Raymond Chan, Kam-Pui Chow, Chun-Fai Chan

Chapter 15

DEFINING ATTACK PATTERNS FOR INDUSTRIAL CONTROL SYSTEMS

Raymond Chan, Kam-Pui Chow and Chun-Fai Chan

Abstract Attack patterns have been used to specify security test cases for traditional information technology systems in order to mitigate cyber attacks. However, the attack patterns for traditional information technology systems are not directly applicable to industrial control systems. This chapter considers the differences between traditional information technology systems and industrial control systems, discusses why attack patterns for traditional information technology systems are inadequate for industrial control systems, and specifies attack patterns for industrial control systems. The attack patterns are useful for creating security test cases for assessing the security levels of industrial control systems. An elevator system case study is used to demonstrate the utility of industrial control system attack patterns in specifying security test cases.

Keywords: Industrial control systems, attack patterns, security testing

1. Introduction

A large-scale industrial control system (ICS) can comprise hundreds or even thousands of programmable logic controllers (PLCs) and sensors interconnected in a network. Information technology networks at large corporations do not have control devices and sensors, but they may have similar workstations and servers as industrial control systems. Additionally, the network architectures of industrial control systems and information technology networks are similar. The interconnections of industrial control systems and information technology networks expose the control systems and the infrastructure assets they operate to cyber attacks.

The Stuxnet worm, which attacked Iran's uranium hexafluoride centrifuges, demonstrated how a cyber weapon could enter a conventional information technology asset and eventually move into a highly-secure industrial control system [15]. In 2015, BlackEnergy, an HTTP-based toolkit, enabled hackers to

launch distributed denial-of-service (DDoS) attacks on industrial control systems and supervisory control and data acquisition (SCADA) systems [2]. In 2017, the WannaCry malware infected workstations at the Chernobyl nuclear power plant, which had to switch to manual radiation monitoring as a result of the attack [5]. The Shodan search engine enables users to discover and gain information about thousands of Internet-facing industrial control systems around the world; the information collected can be used by hackers to enter the industrial control systems and disrupt, perhaps even damage, the physical assets they operate.

Attack patterns have been used to specify security test cases for traditional information technology systems in order to mitigate cyber attacks. However, the attack patterns for traditional information technology systems are not directly applicable to industrial control systems. This chapter considers the differences between traditional information technology systems and industrial control systems, discusses why attack patterns for traditional information technology systems are inadequate for industrial control systems, and specifies attack patterns for industrial control systems. The attack patterns are useful for creating security test cases for assessing the security levels of industrial control systems. An elevator system case study is used to demonstrate the utility of industrial control system attack patterns in specifying security test cases.

2. Related Work

Attack pattern research has largely focused on specifying and discovering attack patterns for information technology systems. Zhu [16] has proposed an algorithm that determines network attack patterns by mining network traffic logs. The resulting patterns are used to identify and detect network attacks.

Rahaman et al. [11] have developed an attack pattern framework for identifying and mitigating attacks on enterprise information systems. Li et al. [7] have proposed an attack pattern mining algorithm that extracts attack patterns from security logs.

Other researchers [8] have analyzed attacks using attack patterns in a comprehensive attack knowledge repository. Bozic and Wotawa [1] have proposed a formalization of attack patterns from which test cases can be generated and executed automatically to conduct security testing.

Limited attack pattern research has concentrated on industrial control systems. Pricop and Mihalache [10] have proposed a fuzzy-logic-based approach for modeling cyber attack patterns on data transfers in industrial control systems. They classified adversaries into profiles ranging from script kiddies to cyber warriors. They also introduced an adversary profile score that can be used to rate adversary skills. However, they do not discuss the types of industrial control system attacks that an adversary could perform. Indeed, from the security point of view, identifying an adversary profile may not be adequate to develop an industrial control system protection plan.

In summary, research on attack patterns has focused primarily on information technology systems and related adversary knowledge. Since attacking

industrial control systems is quite different from attacking traditional information technology systems, it is necessary to define attack patterns that are specific to industrial control systems. Attack patterns for industrial control systems can help understand the underlying security issues and assist in creating security test cases for industrial control systems.

3. Attack Patterns

An attack pattern is an abstraction mechanism for describing how a specific type of attack can be executed. An attack pattern describes the context where the attack type is applicable along with its working principle. It also defines the nature of the attack and provides general recommendations for mitigating the attack. In short, an attack pattern is a blueprint of an attack.

According to Sethi and Barnum [12], attack patterns define a series of repeatable steps that can be applied to simulate an attack against the security of a system. The Common Attack Pattern Enumeration and Classification (CAPEC) [9] specifies cyber attack patterns for information technology systems. Although some of these attack patterns can be applied to industrial control systems, it is important to define attack patterns that are specific to industrial control systems. In fact, absent attack patterns that are customized to industrial control systems, it is not possible to cover all the attack types that target industrial control systems. This means that a complete set of security test cases cannot be defined. Security testing that does not cover all possible attacks prevents proper assessments of the risk levels of industrial control systems.

3.1 Design Patterns

Gamma et al. [3] have specified design patterns for software and operating systems. These design patterns can be applied to specify attack patterns for industrial control system that are related to software, operating system and network architectures. Design patterns define common models or problems whereas attack patterns define cyber attacks that occur frequently.

Unfortunately, attack patterns for information technology systems do not cover the fact that an adversary can change the physical environment of an industrial plant. For example, sensors that monitor industrial plant equipment and environments are not covered by attack patterns for information technology systems. Because industrial control devices always trust sensor data, which is easily tampered with, the attacks cannot be mitigated by software or program logic. As a result, it is necessary to specify attack patterns for industrial control systems using the design patterns of Gamma et al. [3].

3.2 Attack Pattern Usage

Attack patterns are useful for defining and developing application security and security-related actions for information technology systems. The attack

patterns help understand the possible threats and their impacts [4]. Additionally, attack patterns are useful for testing applications and systems to identify and mitigate potential vulnerabilities.

For example, a security engineer can study attack patterns corresponding to man-in-the-middle and replay attacks before an application is designed. The security engineer would know in advance the possible attacks that the application may face. Furthermore, he/she would know the security testing that should be conducted based on the attack patterns. Last, but not least, the application can be planned and developed to achieve security by mitigating the attacks specified by the attack patterns.

Since industrial control systems do not have security testing standards, it is essential to define attack patterns for these systems. Many industrial control systems do not receive security patches or have application and operating system update policies in place for fixing vulnerabilities [14]. Attack patterns are needed to propose a security testing standard that forces industrial control system operators to define security patches and policies. Indeed, attack patterns are vital to preparing and defining test cases for assessing the security levels of industrial control systems.

3.3 System Comparison

This section discusses the common characteristics and the differences between information technology and industrial control systems.

An industrial control network hierarchy has three layers [13]. The top layer is the enterprise layer, which is similar to that of an information technology system. This layer usually comprises servers and workstations that are necessary to support operations. Examples are the mail server and the database server that stores information. The workstations are typically connected to industrial control devices, which means they can access the control devices and impact the physical equipment. Below the enterprise layer is the control layer that contains industrial control devices that monitor and manage physical equipment located in the lowest physical plant layer. The physical plant layer is maintained and managed by technicians and engineers who usually do not have a role in securing industrial control devices.

The differences between information technology and industrial control systems can be understood in terms of their architectures, constituent devices, attack goals and attack methods. As mentioned above, the enterprise layers of information technology and industrial control systems are similar. However, the bottom two layers of the network hierarchy – the control layer and the physical plant layer – are unique to industrial control systems.

In the case of industrial control systems, the control layer comprises industrial control devices while the physical plant layer comprises physical equipment and sensors. Information technology systems do not have such devices. The devices in the bottom two layers of industrial control systems are attractive cyber attack targets because they are more vulnerable than devices in the en-

terprise layer. Moreover, successful attacks can disrupt plant operations, and possibly damage or destroy plant equipment.

Attackers of information technology systems and industrial control systems generally have different goals, although some goals may be similar. In the case of information technology systems, an attacker may wish to steal sensitive or proprietary data, disrupt business operations or collect ransom [6]. Attackers of industrial control systems typically have political or terrorist motivations, but they may also be interested in accessing proprietary information, disrupting plant operations or collecting ransom [15].

Information technology systems are generally attacked via malware or by exploiting software or operating system vulnerabilities to gain system access. Industrial control system attackers typically leverage unauthenticated and unencrypted communications protocols to target workstations, human-machine interfaces, industrial control devices and sensors.

4. Attack Pattern Classification

This section defines common attack patterns for industrial control systems using the attack pattern classification profiles suggested by Sethi and Barnum [12]. The adversary profiles defined by Pricop and Mihalache [10] are used to specify the skill levels of adversaries.

The following subsections describe five industrial control system attack patterns. The Information Collection and Analysis attack pattern describes how an adversary can gather information about an industrial control device before launching an attack. The Injection attack pattern describes how the behavior of an industrial control device can be controlled or modified. The Denial-of-Service attack pattern describes how an industrial control device can be the source or target of a denial-of-service attack and how denial of service increases the vulnerability of the industrial control system. The System Resource Manipulation attack pattern describes how a software application or workstation in an industrial control system can be attacked. Finally, the Sensor Manipulation attack pattern describes how an adversary can use a sensor to alter the behavior of an industrial control device.

4.1 Information Collection and Analysis

- **Description:** A programmable logic controller periodically sends commands to and receives data from devices in its industrial control network. An adversary can collect and analyze this information to gain knowledge about the industrial control network and its devices.

- **Attack Prerequisites:** An adversary can access the internal industrial control network and capture communications traffic between the programmable logic controller, human-machine interfaces (HMIs) and workstations.

- **Targeted Vulnerabilities or Weaknesses:** The attack leverages the weakness where devices in an industrial control network do not encrypt their communications. The communications information includes MAC addresses, IP addresses, device model numbers and firmware versions. Industrial control devices also respond to the Link Layer Discovery Protocol (LLDP) and Internet Control Message Protocol (ICMP), which enables an adversary to locate the devices quickly.

  An industrial control network does not incorporate security devices such as firewalls and intrusion detection systems to isolate the control and physical plant layers, and to alert operators to intrusions. An industrial control network also may not have proper access control policies in place, enabling an adversary to utilize the available protocols to query devices. An adversary who controls a workstation can locate and connect to any and all industrial control devices in the network.

- **Attack Method:** An adversary gains access to a workstation in an industrial control network. The adversary then captures network communications and issues queries to obtain information about devices in the industrial control network.

- **Attacker Goal:** An adversary desires to collect information about devices in an industrial control network to understand the operation of the industrial control system.

- **Required Attacker Skill Level:** An adversary only requires basic hacking skills in order to gain access to the industrial control system and capture network traffic to obtain industrial control device information. The attack can be performed by all the adversary profiles defined by Pricop and Mihalache [10].

- **Example:** An adversary sniffs Link Layer Discovery Protocol messages in an industrial control network and analyzes them to obtain information about industrial control devices in the network. The adversary can use the device information to launch more sophisticated attacks on the industrial control system.

4.2 Injection

- **Description:** Industrial control device communications are insecure. The network communications are seldom protected by authentication and encryption. An adversary who knows how industrial control devices communicate with each other can inject communications messages that alter the behavior of the devices or crash the devices.

- **Attack Prerequisites:** An adversary needs to understand the working principles of industrial control devices, and how they are managed and manipulated using communications protocols (e.g., Siemens STEP 7 and

Modbus). In some cases, the adversary may issue a command to download a program from an industrial control device and understand the program logic in order to fully control the device.

- **Targeted Vulnerabilities or Weaknesses:** In order to ensure compatibility, industrial control devices use standard communications protocols. Devices often communicate using an older version of a protocol to ensure compatibility with other devices in the network. Also, protection mechanisms for information technology systems are not customized to industrial control systems; for example, they may not understand industrial control protocols. The firmware and software of industrial control devices may rarely or never be updated or patched because vendors may not support the devices or the devices have to operate continuously and cannot accommodate the downtime required to install updates. An adversary could employ an older version of a protocol to query and attack industrial control devices. Additionally, the adversary could upload altered firmware or control programs to the devices to conduct attacks.

- **Attack Method:** An adversary accesses a workstation in an industrial control network. A malicious program is installed on the workstation to inject commands and upload malicious programs or firmware to industrial control devices.

- **Attacker Goal:** An adversary desires to change the behavior of industrial control devices to crash the entire industrial control system, or to control industrial control devices in order to make the industrial control system operate in an abnormal or unsafe manner.

- **Required Attacker Skill Level:** An adversary needs to understand the industrial control network architecture, industrial control device operation and the communications protocol in order to control and change the behavior of the devices. Examples include making an elevator motor move the elevator car much faster than normal or switching off the elevator light.

- **Example:** A false command injection attack can change the behavior of an industrial control device. Based on the commands that an industrial control device sends or receives, a security testing professional can specify feasible attacks on the device.

4.3 Denial-of-Service

- **Description:** An industrial control network interface does not require a fast Ethernet connection. Unlike a traditional information technology network, the amount of network traffic is relatively low in an industrial control network. An adversary does not need to generate a massive volume of traffic to launch an effective denial-of-service attack on an industrial control network. Indeed, launching a denial-of-service attack from

just one workstation is enough to affect the performance of industrial control devices.

Attack traffic can be sent from the control center, human-machine interfaces or network devices. Attack traffic can also be generated by industrial control devices.

- **Attack Prerequisites:** An adversary installs and executes malware on an industrial control device that generates malicious network traffic.

- **Targeted Vulnerabilities or Weaknesses:** The bandwidth of an industrial control network is generally much lower than that of an information technology network; the typical throughput of an Ethernet connection interface of an industrial control device is low (e.g., 10 to 100 Mbps). Moreover, network security devices such as firewalls and intrusion prevention systems are often not installed to protect industrial control devices.

- **Attack Method:** A denial-of-service attack on an industrial control network can be launched from three types of devices:

  - *Workstation:* An adversary installs malware on a workstation to disrupt the communications channels between a human-machine interface and industrial control devices to render the industrial control system out of control.

  - *Industrial Control Device:* An adversary installs malware on an industrial control device, which generates attack traffic that crashes workstations and/or human-machine interfaces.

  - *Human-Machine Interface:* An adversary installs malware on a human-machine interface, which sends attack traffic to workstations and industrial control devices that causes them to malfunction.

- **Attacker Goal:** An adversary desires to render industrial control devices uncontrollable. The malfunctioning industrial control system disrupts the industrial process and potentially damages plant equipment.

- **Required Attacker Skill Level:** An adversary needs knowledge about the industrial control network architecture and needs to know how to generate network traffic. All types of adversaries can execute denial-of-service attacks.

- **Example:** An adversary prevents a human-machine interface from communicating with an elevator programmable logic controller, causing the elevator to go out of control. Figure 1 shows a human-machine interface screen after the execution of a denial-of-service attack on an elevator programmable logic controller.

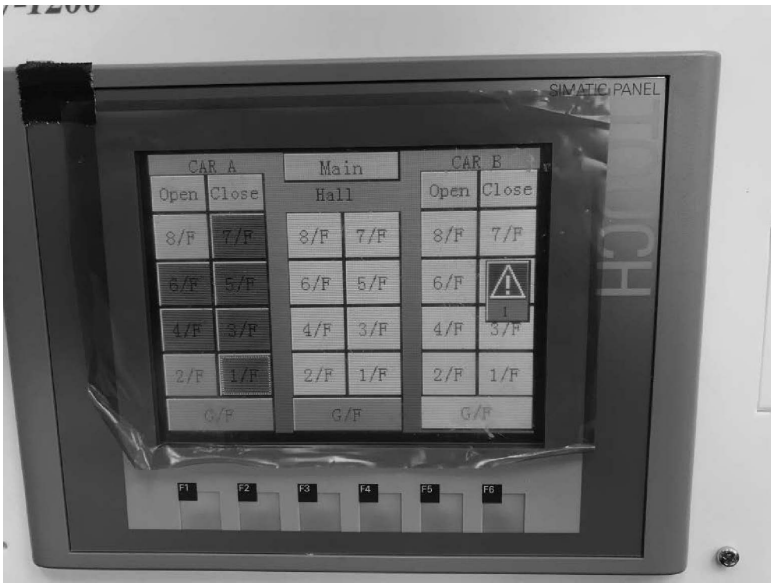

Figure 1. Human-machine interface screen after a denial-of-service attack.

4.4 System Resource Manipulation

- **Description:** Security patch management is typically not in place for workstation operating systems and applications. In many cases, a workstation may use an older operating system (e.g., Windows XP) that has never been updated because of the 24/7 operational requirement. Additionally, updated antivirus software may not be installed on the workstation. Again, because of the 24/7 operational requirement, industrial control system applications may not have been updated for years, which means they may have critical vulnerabilities that enable an adversary to access and modify industrial control devices.

- **Attack Prerequisites:** An adversary gains access to a workstation in an industrial control network and determines the vulnerable software systems and applications installed on the workstation.

- **Targeted Vulnerabilities or Weaknesses:** An adversary targets operating system and industrial control application vulnerabilities, and leverages the absence of antivirus software on a workstation. Access to the workstation enables the adversary to control and modify industrial control devices.

- **Attack Method:** An adversary exploits operating system and industrial control application vulnerabilities to gain control of a workstation.

Alternatively, the adversary may use a spear phishing (email) attack or insert a USB device with malware into the workstation.

- **Attacker Goal:** An adversary desires to disrupt a workstation and the automated operation of control devices, and ultimately disrupt plant operations or damage plant equipment. Operators would have to monitor and control the plant manually; in the worst case, the plant would have to be shut down.
- **Required Attacker Skill Level:** Attacking a workstation requires basic hacking skills. The attack can be performed by a hacker, terrorist, industrial spy or cyber warrior.
- **Example:** An attacker installs malware on a workstation. The malware discovers and issues commands that impact the behavior of industrial control devices in the network.

4.5 Sensor Manipulation

- **Description:** A sensor attack targets the sensors in an industrial control system. There are different types of sensors, including temperature sensors, light sensors and touch sensors. In general, there are two types of sensor attacks:
  - *Physical Attack:* This attack tampers with sensors or causes them to send incorrect responses. For example, an adversary can manually cover a light sensor, causing it to send an incorrect signal. Incorrect sensor values would cause an industrial control device such as a programmable logic controller to send incorrect commands to the physical plant.
  - *Wireless Attack:* This attack involves the wireless injection of incorrect sensor responses. Communications between sensors and industrial control devices rarely employ authentication and encryption. An adversary can pretend to be a sensor and send false values to industrial control devices. The industrial control devices would be unable to verify the correctness of the inputs they receive.
- **Attack Prerequisites:** An adversary must know where the sensors are located and how they are connected to industrial control devices. The adversary also has to know how to modify sensor signals that are sent to industrial control devices.
- **Targeted Vulnerabilities or Weaknesses:** Sensors are used to monitor a physical plant. Because sensor communications with industrial control devices are neither authenticated nor encrypted, an adversary can capture and modify the signals sent to industrial control devices.
- **Attack Method:** In the case of wired sensors, physical access is required on the part of an adversary to launch an attack that affects sensor signals.

In the case of wireless sensors, an adversary can capture sensor signals to industrial control devices and perform wireless signal injection and replay attacks.

- **Attacker Goal:** An adversary desires to change sensor signals to induce industrial control devices to behave incorrectly. Consider, for example, an elevator that has a light sensor to detect if an object is blocking the door of the elevator car. The adversary could modify the light sensor signal from on to off, causing the door to keep opening. Also, touch sensors in the elevator detect if the car has moved to the upper or lower limit. The elevator will not move if the adversary alters these sensor signals.

- **Required Attacker Skill Level:** An adversary needs a good understanding of how industrial devices operate a physical plant. The adversary also must know how sensors and industrial control devices are connected and how the devices behave after receiving sensor signals. The attack can be performed by a terrorist, industrial spy or cyber warrior.

- **Example:** An attacker modifies sensor signals and causes an industrial control system to behave in an incorrect manner.

5. Elevator System Case Study

This section defines the security test cases for an elevator system based on the industrial control system attack patterns described in the previous section.

An elevator system operator asked the authors of this paper to design and conduct a security test of a newly-deployed elevator system. The operator wanted an assessment of the security level of the elevator system and to determine if an adversary could exploit vulnerabilities in the workstation, industrial control devices and sensors to launch attacks that would interrupt elevator service or seize control of the elevator system.

5.1 Security Test Cases

The following security test cases are based on the industrial control system attack patterns defined in the previous section:

- **Information Collection and Analysis:** The security test cases in this category evaluate whether or not device information can be obtained by an adversary. This information could be used by the adversary to develop sophisticated attacks that interrupt elevator service or seize control of the elevator system.

  Table 1 shows five security test cases for the Information Collection and Analysis attack pattern based on the elevator system architecture.

- **Injection:** The security test cases in this category evaluate whether or not elevator system communications are protected by authentication and encryption. Additionally, the security test cases evaluate whether or not

Table 1. Security test cases for Information Collection and Analysis.

Objective	Description/Actions	Expected Result
Obtain elevator controller information – passive	1. Plug attack device into the elevator system 2. Use `tcpdump` or Wireshark to capture traffic 3. Analyze traffic to obtain elevator controller information	Elevator controller information cannot be obtained
Obtain elevator controller information – active	1. Plug attack device into the elevator system 2. Use Nmap to scan the elevator controller 3. Analyze traffic to obtain elevator controller information	Elevator controller information cannot be obtained
Obtain control device information – passive	1. Plug attack device into the elevator system 2. Use `tcpdump` or Wireshark to capture traffic 3. Analyze traffic to obtain control device information	Control device information cannot be obtained
Obtain control device information – active	1. Plug attack device into the elevator system 2. Use Nmap to scan the control device 3. Analyze traffic to obtain control device information	Control device information cannot be obtained
Obtain sensor information	1. Plug attack device into the elevator system 2. Use `tcpdump` or Wireshark to capture traffic 3. Analyze traffic to obtain sensor information	Sensor information cannot be obtained

the control protocol is vulnerable and whether or not modified control system commands and responses can be injected into elevator system communications.

Tables 2 and 3 show five security test cases for the Injection attack pattern.

- **Denial-of-Service:** The security test cases in this category cover possible TCP and UDP denial-of-service attacks on the elevator controller, control devices and sensors.

Table 2. Security test cases for Injection.

Objective	**Description/Actions**	**Expected Result**
Test authentication between the elevator controller and control devices	1. Plug attack device into the elevator system 2. Stop the communications between the elevator controller and control devices 3. Use `tcpdump` or Wireshark to capture traffic 4. Start the communications between the elevator controller and control devices 5. Analyze traffic to check if the authentication between the elevator controller and control devices is vulnerable	Communications between the elevator controller and control devices are authenticated Authentication is secure
Test for encrypted communications between the elevator controller and control devices	1. Plug attack device into the elevator system 2. Stop the communications between the elevator controller and control devices 3. Use `tcpdump` or Wireshark to capture traffic 4. Start the communications between the elevator controller and control devices 5. Analyze traffic to check if encrypted communications exist between the elevator controller and control devices and if they are vulnerable	Communications between the elevator controller and control devices are encrypted Encryption is secure
Test if the control protocol is vulnerable	1. Plug attack device into the elevator system 2. Stop the communications between the elevator controller and control devices 3. Use `tcpdump` or Wireshark to capture traffic 4. Start the communications between the elevator controller and control devices 5. Analyze traffic to check if the control protocol version used is vulnerable	Control protocol is not vulnerable

Table 3. Security test cases for Injection (continued).

Objective	Description/Actions	Expected Result
Test command injection into the elevator controller	1. Plug attack device into the elevator system 2. Stop the communications between the elevator controller and control devices 3. Use `tcpdump` or Wireshark to capture traffic 4. Start the communications between the elevator controller and control devices 5. Capture commands sent to the elevator controller 6. Modify and send commands from the attack device 7. Test if the commands are executed by the elevator controller	Commands cannot be injected into the elevator controller
Test response injection into the control devices	1. Plug attack device into the elevator system 2. Stop the communications between the elevator controller and control devices 3. Use `tcpdump` or Wireshark to capture traffic 4. Start the communications between the elevator controller and control devices 5. Capture responses sent to the control devices 6. Modify and send responses from the attack device 7. Test if the responses are accepted by the control devices	Responses cannot be injected into the control devices

Table 4 shows six security test cases for the Denial-of-Service attack pattern.

- **System Resource Manipulation:** The security test cases in this category relate to performing penetration testing on the control devices and workstation in the elevator system. Since the workstation connects to the elevator system, some security test cases assess the security levels of the workstation and network configuration.

Table 4. Security test cases for Denial-of-Service.

Objective	**Description/Actions**	**Expected Result**
Test if TCP DoS attacks can be launched on the elevator controller	1. Plug attack device into the elevator system 2. Use `hping` or LOIC to send TCP packets to the elevator controller 3. Check if the elevator controller operates properly	TCP DoS attacks cannot affect the elevator controller
Test if UDP DoS attacks can be launched on the elevator controller	1. Plug attack device into the elevator system 2. Use `hping` or LOIC to send UDP packets to the elevator controller 3. Check if the elevator controller operates properly	UDP DoS attacks cannot affect the elevator controller
Test if TCP DoS attacks can be launched on the control devices	1. Plug attack device into the elevator system 2. Use `hping` or LOIC to send TCP packets to the control devices 3. Check if the control devices operate properly	TCP DoS attacks cannot affect the control devices
Test if UDP DoS attacks can be launched on the control devices	1. Plug attack device into the elevator system 2. Use `hping` or LOIC to send UDP packets to the control devices 3. Check if the control devices operate properly	UDP DoS attacks cannot affect the control devices
Test if TCP DoS attacks can be launched on the sensors	1. Plug attack device into the elevator system 2. Use `hping` or LOIC to send TCP packets to the sensors 3. Check if the sensors operate properly	TCP DoS attacks cannot affect the sensors
Test if UDP DoS attacks can be launched on the sensors	1. Plug attack device into the elevator system 2. Use `hping` or LOIC to send UDP packets to the sensors 3. Check if the sensors operate properly	UDP DoS attacks cannot affect the sensors

Table 5. Security test cases for System Resource Manipulation.

Objective	**Description/Actions**	**Expected Result**
Scan control devices using a vulnerability scanner	1. Plug vulnerability scanner into the elevator system 2. Use the vulnerability scanner scanner on the control devices 3. Check the results provided by the vulnerability scanner	No critical vulnerabiliies are found
Scan the workstation using a vulnerability scanner	1. Plug vulnerability scanner into the elevator system 2. Use the vulnerability scanner scanner on the workstation 3. Check the results provided by the vulnerability scanner	No critical vulnerabilities are found
Check the network configuration in the elevator system	1. Use the administration console to check the network configuration	Network is configured properly
Extract the elevator program from the elevator controller	1. Plug attack device into the elevator system 2. Use the IDE (e.g., Siemens TIA Portal) to connect to the elevator controller 3. Send the download command to the elevator controller 4. Check if the elevator program can be downloaded	Elevator program cannot be extracted from the elevator controller
Modify the elevator program in the elevator controller	1. Plug attack device into the elevator system 2. Use the IDE (e.g., Siemens TIA Portal) to connect to the elevator controller 3. Send the upload command to the elevator controller 4. Check if the modified elevator program can be uploaded and execute properly	Modified elevator program cannot be uploaded to the elevator controller and execute properly
Check the elevator controller firmware version	1. Plug attack device into the elevator system 2. Use the IDE (e.g., Siemens TIA Portal) to connect to the elevator controller 3. Check the firmware version	Elevator controller firmware is the latest version

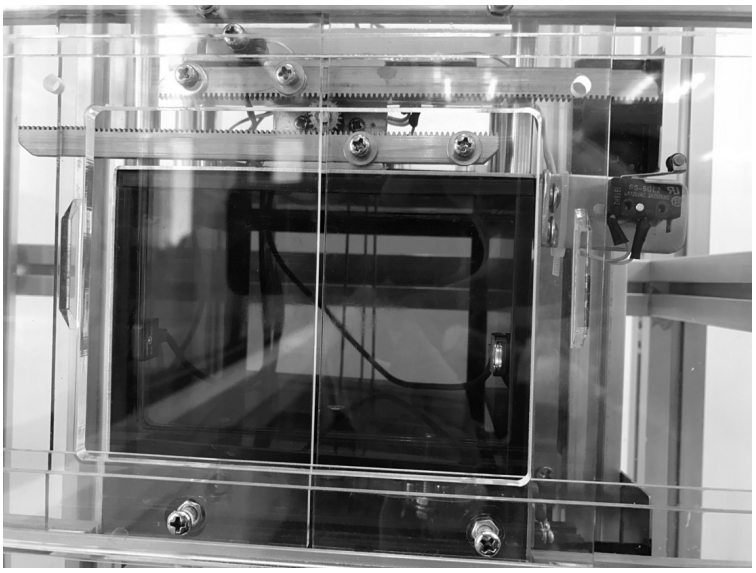

Figure 2. Elevator light sensor.

Table 5 shows six security test cases for the System Resource Manipulation attack pattern.

- **Sensor Manipulation:** The security test cases in this category relate to potential compromises of sensors. In the case of wired sensors, the sensors have to be located and attacked by physical means. In the case of wireless sensors, a Wi-Fi sniffer and/or Bluetooth sniffer are required. The security test cases for the Sensor Manipulation and Injection attack patterns are similar. However, the two attack pattern categories are treated separately for effective security testing.

  The elevator system has light sensors and touch sensors that connect to the elevator controller (Figures 2 and 3, respectively). The security test cases check whether or not it is possible to change the sensor values and the behavior of the elevator.

  Table 6 shows five security test cases for the Sensor Manipulation attack pattern.

5.2 Results

The attack patterns enabled the security testing team to define elevator system security test cases. Also, the attack patterns helped identify the types of attacks, vulnerabilities exploited by the attacks, and methods for detecting and mitigating the attacks.

Figure 3. Elevator touch sensor.

6. Conclusions

The interconnections of industrial control systems and information technology networks expose the control systems and the infrastructure assets they operate to cyber attacks. Attack patterns have been used to specify security test cases for traditional information technology systems in order to mitigate cyber attacks. However, because of differences in the architectures, constituent devices, attack goals and attack methods, the attack patterns for traditional information technology systems are not directly applicable to industrial control systems.

Five attack patterns have been specified for industrial control systems – Information Collection and Analysis, Injection, Denial-of-Service, System Resource Manipulation and Sensor Manipulation. Each industrial control system attack pattern has six components – description, attack prerequisites, targeted vulnerabilities or weaknesses, attack method, attacker goal and required attacker skill level.

As demonstrated in the elevator system case study, the attack patterns help understand the possible threats and their impacts to an industrial control system and the physical plant it operates. The attack patterns are also useful for creating security test cases for assessing the security levels of the industrial control system, and for developing and implementing attack mitigation mechanisms.

Table 6. Security test cases for Sensor Manipulation.

Objective	**Description/Actions**	**Expected Result**
Test authentication between the elevator controller and sensors	1. Plug attack device into the elevator system 2. Use `tcpdump` or Wireshark to capture traffic 3. Analyze traffic to check if the authentication between the elevator controller and sensors is vulnerable	Authentication is secure
Test encryption between the elevator controller and sensors	1. Plug attack device into the elevator system 2. Use `tcpdump` or Wireshark to capture traffic 3. Analyze traffic to check if the encryption between the elevator controller and sensors is vulnerable	Encryption is secure
Test if the sensor signals can be modified	1. Plug attack device into the elevator system 2. Use `tcpdump` or Wireshark to capture signals sent by the sensors 3. Modify and send signals from the attack device 4. Check if the signals are accepted by the elevator controller	Sensor signals cannot be modified
Test if the sensors can be accessed physically and replaced	1. Gain physical access to the elevator system 2. Locate the sensors 3. Attempt to remove and replace the sensors 4. Check if the elevator system is still operational	Sensors cannot be accessed physically and replaced
Test if the wireless sensor signals can be tampered with	1. Use `tcpdump` or Wireshark to capture wireless signals sent by the sensors 2. Modify and send wireless signals from the attack device 3. Check if the signals are accepted by the elevator controller	Wireless sensor signals cannot be tampered with

References

[1] J. Bozic and F. Wotawa, Security testing based on attack patterns, *Proceedings of the Seventh IEEE International Conference on Software Testing, Verification and Validation Workshops*, pp. 4–11, 2014.

[2] Z. Flom, Shedding light on BlackEnergy with open source intelligence, *Recorded Future Blog* (`www.recordedfuture.com/blackenergy-malware-analysis`), March 3, 2016.

[3] E. Gamma, R. Helm, R. Johnson and J. Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley, Boston, Massachusetts, 1994.

[4] M. Gegick and L. Williams, Matching attack patterns to security vulnerabilities in software-intensive system designs, *Proceedings of the Workshop on Software Engineering for Secure Systems – Building Trustworthy Applications*, 2005.

[5] M. Havis, Chernobyl under attack: Computers "shut down" at nuclear disaster plant, *Daily Star*, June 27, 2017.

[6] 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.

[7] K. Li, Y. Li, J. Liu, R. Zhang and X. Duan, Attack pattern mining algorithm based on security logs, *Proceedings of the IEEE International Conference on Intelligence and Security Informatics*, p. 205, 2017.

[8] T. Li, E. Paja, J. Mylopoulos, J. Horkoff and K. Beckers, Security attack analysis using attack patterns, *Proceedings of the Tenth IEEE International Conference on Research Challenges in Information Science*, 2016.

[9] MITRE, Common Attack Pattern Enumeration and Classification (CAPEC), McLean, Virginia (`www.capec.mitre.org/about/index.html`), 2019.

[10] E. Pricop and S. Mihalache, Fuzzy approach for modeling cyber attack patterns on data transfer in industrial control systems, *Proceedings of the Seventh International Conference on Electronics, Computers and Artificial Intelligence*, pp. SSS-23–SSS-28, 2015.

[11] M. Rahaman, C. Hebert and J. Frank, An attack pattern framework for monitoring enterprise information systems, *Proceedings of the Twenty-Fifth IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 173–178, 2016.

[12] A. Sethi and S. Barnum, Introduction to Attack Patterns, Cigital, Dulles, Virginia (`www.us-cert.gov/bsi/articles/knowledge/attack-patterns/introduction-to-attack-patterns`), 2006.

[13] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, 2015.

[14] C. Valli, Issues common to Australian critical infrastructure providers' SCADA networks discovered through computer and network vulnerability analysis, *Proceedings of the Sixth Australian Digital Forensics Conference*, 2008.

[15] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Broadway Books, New York, 2014.

[16] Y. Zhu, Attack pattern discovery in forensic investigations of network attacks, *IEEE Journal on Selected Areas in Communications*, vol. 29(7), pp. 1349–1357, 2011.