Chapter 8
Retracted Chapter: Cyber-Physical System Security Controls: A Review

Subhrajit Majumder, Akshay Mathur, and Ahmad Y. Javaid

RETRACTED CHAPTER

Abstract The term cyber-physical system (CPS) could be described as a system that integrates the computational and physical capabilities and can work as the connection between the cyber and physical worlds. The capabilities of the system to interact with the physical world through more efficient implementations of these "connections" is a crucial enabler for developing the future technologies. For these, there should be a targeted approach to ensure successful implementation of security measures to address the issues of security such as curtail any illegitimate activity or the breach of data that could lead to damage of a large group of the population, influential business entity or even a government agency. Over the years, researchers have proposed novel techniques and security measures to ensure the security and proper functioning of CPSs. Although with time, many such measures have become obsolete and pose a completely new series of security challenges as the recent attacks have become more deleterious and harder to detect. In this chapter, we identify the threats on CPSs due to the systems' vulnerabilities, discuss recent successful attacks on the systems, problems in security control of the system, investigate the defenses that it can provide and propose a set of challenges that need to be addressed for the improvement of cyber-physical systems security.

8.1 Introduction

A CPS is a system made with diverse types of components where the high-end components can monitor and control the other low-end components present in our physical world through cyber (Internet) and physical (wired) connections

The original version of this chapter was retracted. The retraction to this chapter is available at https://doi.org/10.1007/978-3-319-92564-6_9

S. Majumder · A. Mathur · A. Y. Javaid (✉)
University of Toledo, Toledo, OH, USA
e-mail: subhrajit.majumder@rockets.utoledo.edu; akshay.mathur@rockets.utoledo.edu; ahmad.javaid@utoledo.edu

© Springer International Publishing AG, part of Springer Nature 2019

S. Guo, D. Zeng (eds.), *Cyber-Physical Systems: Architecture, Security and Application*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-92564-6_8

with the help of computer-based algorithms. In a CPS, the software and physical components work together on their respective spatial scales, displaying numerous distinct behavioral modalities while interacting with each other. In recent times, we have seen an exponential development in various CPSs. In our life, the applications of CPSs are constantly enhancing such as industrial control systems, smart grid, medical devices, autonomous automobile system (smart cars), process control systems, automatic pilot avionics, and robotics. However, with more technologies come more vulnerabilities which need to be managed to keep the system secure. Mainly four contents are discussed in this chapter which are (1) the cyber, physical, and cyber-physical components, (2) the possible threats and vulnerabilities of the CPS, (3) the real-life attacks on the CPS, and (4) the existing research on security controls that are required as solutions of these attacks, and what security measures are required to make these solutions even better. We discuss these in detail about four most popular CPS which are

- Industrial Control System
- Smart Grids
- Medical Devices
- Smart Cars

These CPSs are selected primarily because, in our world, the above-mentioned applications of CPS are the most conventional ones and environments around these are very critical. Thus, attacks on these CPSs can bring severe consequences in our daily life. We have briefed about each of the applications which will give an overview of these separately and the synopsis of the communication structure between different components. The components of a CPS are categorized into three types, i.e., cyber, cyber-physical, and physical. Due to heterogeneous properties, we have focused on these distinct categories of aspect individually according to their applications. We have discussed the possible threats due to the vulnerabilities present in the CPSs and the real-life attacks on the systems which have taken place till now. This helps to decide which technologies are required to secure the systems properly as we have shown that different components of the systems were exploited in those real-life attacks, even though there were some security measures present. For references, research which has been made regarding this is demonstrated along with the challenges which will give the idea of which area needs more research.

RETRACTED CHAPTER

8.2 Background

8.2.1 Cyber-Physical Systems

In simple words, CPSs are the systems that are used to monitor and control our physical world [128]. In other words, CPS is an integration of computation process with the physical world's components [80]. The developments in the information and communication technologies (ICT) have made this integration operate properly. These explanations describe the heavyweight of the interactions between the cyber and physical worlds.

RETRACTED CHAPTER

8.2.1.1 Industrial Control Systems (ICS)

ICS is used to better control, monitor, and produce in various industries such as nuclear plants, irrigation systems, and hydro plants. ICS is an integration of Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), and many smaller control systems such as Programmable Logic Controller (PLC) or Remote Terminal Units (RTU). These systems contain many controllers with different capabilities that accomplish numerous tasks with collaboration. Among many ICS components, one of the most popular is the Programmable Logic Controller (PLC) which is an industrial digital computer designed for controlling manufacturing processes like assembly lines, robotic activity, or any other activity which requires control with high reliability. It communicates through wired or wireless or both connections which are configured with the surrounding environment. PLC can operate continuously in a hostile environment with the help of its sensors and actuators that are connected to the physical world [81].

8.2.1.2 Smart Grid Systems

Power grid is an electric grid that is built up as a network of transformers, transmission lines, and more that has been used for electricity generation, transmission, and distribution. The primary function of a smart grid is to deliver electricity from the power plant to the electric home appliances of customers as efficiently as possible so that it reduces the management cost for utility and power cost for the customer. The two major components of the smart grid are supporting infrastructure and power application [143]. The supporting infrastructure is the intelligent one that concerns mainly with monitoring and controlling the core operations of the smart grid. However, the core functions of the smart grid are done by the power application. The current smart grid of ours was built in the 1890s and has been improving with the advancements in technology through the years. Today, more than 9200 electric generating units are there with the generating capacity of more than 1 million megawatts that are connected to more than 300,000 miles of transmission lines [74].

8.2.1.3 Medical Devices

For the betterment of health care services, medical devices have integrated with information technologies that are cyber-based. This allows the physician along with the patient to control the devices more conveniently and not compromising accuracy at the same time. Since decades, we are more interested making devices that have cyber capabilities and a better physical impact on the patients. These devices are either implanted inside a patient's body, or the patient wears it. The devices that are implanted are called Implantable Medical Devices (IMD) and which are worn by the patient are called wearable devices. Since medical cyber-physical devices (MCPS) are context-aware, life-critical, and a networked system of the medical devices, the usage of these devices is increasing in the hospitals for continuous high-quality treatment of patients. These devices can be equipped with the wireless capabilities also, which allows the devices to communicate with each other or the programmer. For example, wearable devices can be controlled remotely by a physician through a smartphone. These devices need to be safe, efficient, and effective as a minor fault in it can be fatal for someone's life [131].

8.2.1.4 Smart Cars

The passenger-carrying vehicles are evolving to become smarter, for which the electronic components that make these vehicles smart are introduced to new models continuously. Smart cars are those cars which are more fuel-efficient, environment-friendly, safe, and have more convenient features. Advanced entertainment units in smart cars are also desired, like advanced music player and even a video player. Besides these, comfort factors like automated tinted glass, window controllers, displays on the screen, cruise control, reverse camera and more are equally important. As this brings new features and benefits, it also brings security concerns. Numerous computers working together make these advancements possible. These computers are called Electronic Control Units (ECUs). ECUs monitor and control various functions of a smart car like brake control, engine emission control, entertainment units, and comfort features.

8.2.2 CPS Communications

Communication is a major part of a cyber-physical system as the cyber and physical components communicate with each other the whole time that makes these systems run properly. Different CPS applications have different communication technologies. They use different protocols and technologies like open and proprietary, wired and wireless. Here we have discussed the common communication technologies used by each of the four applications.

8.2.2.1 Communications in ICS

In ICS, there are two diverse types of communication protocols which are deployed. One of them controls and automates the Distributed Network Protocol (DNP3), Modbus, while the other interconnects the control centers of ICS, for example, Inter-Control Center Protocol (ICCP). These protocols are used in addition to the general-purpose protocols like TCP/IP.

RETRACTED CHAPTER

RETRACTED CHAPTER

8.2.2.2 Communications in Smart Grid

Smart meters use two types of networks: one is using Modbus and DNP3 in field device communications and the advanced protocol IEC 61850 which is developed by the International Electrotechnical Commission (IEC). The other type of network used is control center communication. This is like ICS as it relies on ICCP. Additionally, smart meters and field devices also use wireless communications for sending measurements and receiving control from the control centers. Smart meters usually use short-range frequency signals like Zigbee to diagnose operations done by the technicians or the readings generated by digital smart readers.

8.2.2.3 Communications in Medical Devices

To avoid surgical extraction, it is necessary to configure and update the IMDs wirelessly, which makes wireless communication the most common method of communication for medical devices. Though, the wearable devices and IMD use different types of technologies and protocols for communications. For example, for the communication with programmers, low-frequency (LF) signals are used by the IMD. These LF signals are specified by the Federal Communications Commission (FCC). This communication through low signals, specified by FCC, is called Medical Implant Communication Service (MICS), whereas the wearable devices use a different type of communication called Body Area Network (BAN). This wireless communication uses numerous wireless communication protocols and technologies like Zigbee and Bluetooth [18].

8.2.2.4 Communications in Smart Cars

There are different types of communications in smart cars, which are Vehicle to Infrastructure (V2I), Vehicle to Vehicle (V2V), and in-vehicle communications. This paper focuses on the latter. As we mentioned above, there are around 70 computers connected in a smart car which are called ECUs. These ECUs communicate with each other through a bus network. These networks are also divided into bus networks which have their bus topology. The messages are exchanged among the subnetworks through a gateway. The gateway separates the messages according to the source and destination of the messages. This is not only for security concerns but also for the bandwidth. The most common protocols which are used are (1) Local Interconnect Network (LIN), (2) Controller Area Network (CAN), (3) FlexRay, and (4) Media-Oriented Systems Transport (MOST). LIN is used for comparatively low-speed applications like shutting windows on/off. CAN runs the soft real-time applications such as antilock braking system. Where the speed of transmission is critical, FlexRay is needed for hard real-time applications. MOST is usually used for in-car entertainment-oriented applications [160]. Some cars are also operated with wireless connections like cellular interfaces and Bluetooth.

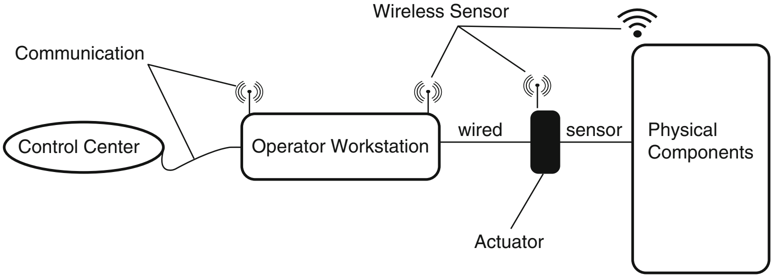

Fig. 8.1 Aspects of a CPS

RETRACTED CHAPTER

8.2.3 CPS Models and Aspects

As shown in Fig. 8.1, there are mainly three categories of components in cyber-physical systems: (1) monitoring and manipulating, (2) computation and control, and (3) communication. The CPS is connected with the high-level systems like control centers and/or lower-level components which exist in the physical world through the wired or wireless communication channel. The intelligence is embedded in the computation and control part since all the control commands are sent, and the sensed measures are received here CPS is connected to the physical system by monitoring and manipulating components through the sensors and the actuators.

A Cyber-Physical System component can communicate with other CPS components or control centers. There are different security implications for each one of these components which may be the result of heterogeneous properties and capabilities of the components. For example, the physical world is not expected to get affected by the cyber world of a CPS, and yet the physical components might be damaged by unexpected attacks which may cause physical consequences. Similarly, the cyber components can also be affected through the communication channel by the exploitation of physical components.

Therefore, different aspects need to be distinguished properly and the respective security analysis must be done separately. The cyber aspects of CPS include those components which do not interact with the physical world directly such as data computations, monitoring communications, communication protocols, etc. Whereas other channels through which cyber world interacts with the physical world and vice-versa are considered as cyber-physical aspects. Finally, the components of a CPS that can be accessed, controlled, or monitored physically come into the physical aspects category.

8.2.3.1 ICS

A scenario of the network of ICS is depicted in Fig. 8.2. The Corporate Network is the cyber part of the ICS which has no direct connection with the physical world. All the ERP servers and production management system are parts of the cyber world. The cyber components have wired/wireless communication with the cyber-physical

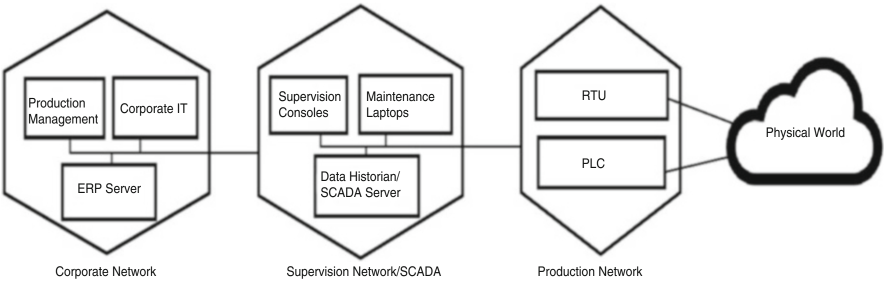

Fig. 8.2 Aspects of industrial control system

RETRACTED CHAPTER

components which, on the other hand, have connections with the physical world, too. In this part, the operations of the physical world are supervised, controlled, and the data regarding their functions, requirement are stored. This is mainly the control and supervisory section which interacts with the physical world through field devices such as PLC/RTU.

As an example, the PLC/RTU is used to control and monitor the temperature of an industrial plant. If the temperature exceeds a certain amount of temperature in any instrument, it notifies the PLC/RTU through the wireless connection and in return the PLC informs the control center about the undesired changes in temperature. As a response, the control center will instruct the PLC/RTU to initiate the cooling system to reduce the temperature.

8.2.3.2 Smart Grid

In Fig. 8.3 the cyber-physical aspects of smart grids are shown. To every house, there is a smart meter attached to provide the utility companies more accurate data of electric consumption. It also makes more convenient for the customers to have a track on their usage. The smart meter, on the one hand, connects the house appliances with the Home Energy Management System (HEMS), and on the other hand, it interacts with the data collector components. Although wireless communication is the most convenient and common way of interaction for data collectors, wired communication is available too, i.e., Power Line Communications. There is a meter equipped with diagnosing port which relies on the short wireless range, and a meter with a diagnosing port which relies on the short wireless range, to make the access more convenient for the digital meter readers and diagnostic tools [71]. The measurements of the smart meter are sent to a collector which forwards those in an aggregated form to the distributed control center which is managed by the utility company. The AMI head-end stores this data and shares it with the Meter Data Management System (MMDS). The MMDS manages the data with other systems like demand response system, billing system, and historians. These connections with high-end sectors can be disconnected by remotely sending commands to smart meters. If many smart meters are sent signals to disconnect with the high-end systems, a large-scale blackout will occur.

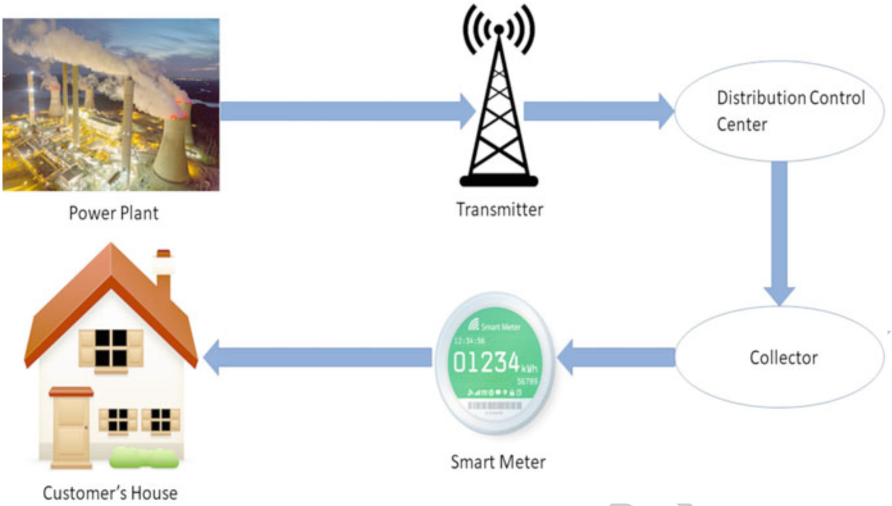

Fig. 8.3 Aspects of smart grid cyber-physical system

RETRACTED CHA

In Fig. 8.3 we have described the overview of aspects of a smart meter. The cyber aspect is present in the control center where the data of the smart meter are stored, shared, and analyzed. The control center can also be a cyber-physical aspect when a connect/disconnect command is sent to the smart meter from high-end AMI. The cyber-physical component is very apparent in a smart meter as it can send data to the utility companies which is a cyber-operation, whereas it can also connect/disconnect electricity services on command which is an example of physical activity. Other field devices also have a high presence of cyber-physical aspects as they interact with the physical components very closely, such as the devices in the generation, transmission, automation, distribution, etc. The amount of energy used by any home appliance can be controlled by the utility companies based on the time when it is needed, which is a cyber-physical activity [113].

8.2.3.3 Medical Device

Figure 8.4 portraits the networking of two of the most important Inter-operable Medical Devices (IMD)s—the Implantable Cardioverter Defibrillator (ICD) and the insulin pump. If a rapid heartbeat is detected, an electric shock is delivered to maintain a normal heartbeat rate. The role of an insulin pump is to inject insulin into the diabetic patients automatically or manually when its needed [52]. To get the measurement of blood sugar, the insulin pump uses Continuous Glucose Monitor (CGM). As both the devices have small needles which are injected into patient's body, the CGM sends the received blood sugar measurement from the patient to the insulin pump or other devices like a computer or any remote-control devices through wireless signals, and the pump decides whether it should inject the insulin or not based on the measurements. The remote-control devices are usually held by the

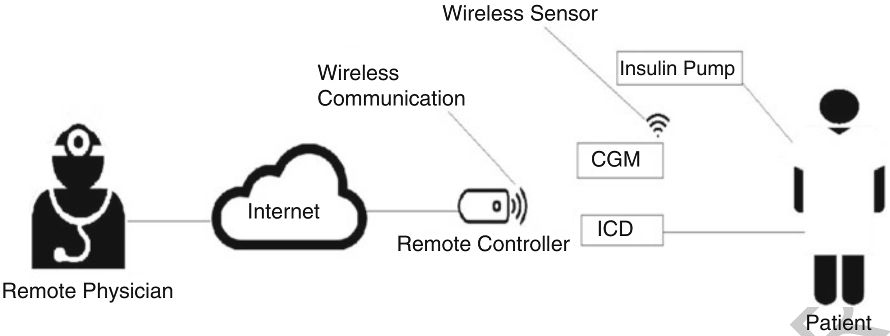

Fig. 8.4 Aspects of medical cyber-physical system

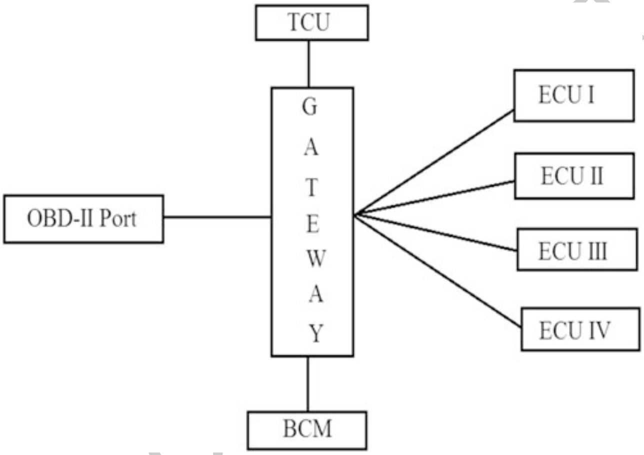

Fig. 8.5 Aspects of smart car cyber-physical system

RETRACTED CHAPTER

patient or the doctor. In the fig, four cyber aspects are embodied in the monitoring computers, whereas the cyber-physical aspects are those devices which directly interact with the patients' implant devices. In the end, the patient is considered as the physical aspect.

8.2.3.4 Smart Cars

Figure 8.5 demonstrates the architecture of the network in a smart car. Each of the Electronic Control Units (ECUs) is connected to their respective sub-network according to the tasks expected from those. Each of the ECUs can interact with each other through gateways. In this chapter, we mainly discuss the Controller Area Network (CAN) bus. Behind this, there are primarily two reasons: (1) Maximum number of security issues are generated from CAN-based networks, and (2) since 2008 every vehicle in the United States requires CAN to be installed in it, so almost every car around us possesses it.

Figure 8.5 shows various aspects of a smart car network. The cyber aspects are held by those ECUs which don't communicate with the physical components directly, such as the Telematics Control Unit (TCU) and the media player. The TCU has wireless interfaces which allow remote software update by the car manufacturer, phone pairing, hands-free facilities which can be used by a connected smartphone. The ECUs which interact with the physical components such as the Remote Keyless Entry (RKE) and parking assist are considered as the cyber-physical aspect. The RKE sends wireless signals to have a physical impact on the car such as locking and unlocking. Finally, the engine, tires, etc. are the physical aspects.

RETRACTED CHAPTER

8.2.4 Security in CPS

We have motivated the importance of security in CPS in this section. We have illustrated four different examples based on this. Usually, security systems are linked with mechanisms like cryptography, intrusion detection, access control, and many other solutions which are used in IT field. Those mechanisms play a key role in securing the information and communication in the architecture. The reported attacks on the Cyber-Physical Systems are the result of sole dependency on these mechanisms as discussed in Sect. 8.5. Hence, the solution which takes these aspects into consideration is required and can be used along with the IT security solutions.

8.2.4.1 Security in ICS

If the security of a CPS is compromised, it can bring a catastrophic consequence. For example, if a nuclear plant's security is breached, the result can be a worldwide threat. On the other hand, if a smart grid is violated, it will stop the services to the consumer and bring economic loss to the utility company since the use of CPS is very wide and its pervasiveness and the security of CPSs are very critical. In fact, even now it is advised that the ICS should not be connected to the internet because of the inherent security vulnerabilities which can bring possible catastrophic consequences [44].

8.2.4.2 Security in Smart Grids

Inadequate security in smart meters creates the threat by remote attackers which could evolve to extensive blackout. The extended results of this could be data loss, malfunctioning of medical devices, and even an increased crime rate. Another possible result can be an ability of attackers to reveal customer's information.

8.2.4.3 Security in Medical Devices

Security in IMDs and wearable devices makes them immune to the attacks which can compromise patient's privacy and safety. There are other different circumstances around the medical devices which mandate the need for definite security in them. The security goals of the medical devices, integrity, confidentiality, and availability, are initiated by Halperin et al. [53]. The security goals must allow the entities to access accurate data, configure identified data, update software, and maintain the availability of the devices. On the other hand, privacy deals with the security of the private information of the devices, such as their type, unique ID along with patient's information.

8.2.4.4 Security in Cars

Car Manufacturing companies always thrive to come up with innovative ideas such as how to enhance the comfort and functionalities of the vehicle, etc. However, the safety issues are not concerned in the design phase. The safety of cars means their ability to function accurately in different favorable and adverse situations. The advanced features of a smart car like wireless communications and components escort more security vulnerabilities with which arise the importance of security issue.

8.3 CPS Security Threats

To secure a CPS, there are various challenges which need to be considered. Before securing a system, we must understand the possible threats upon that. We have analyzed different angles of potential threats on CPS in this section. At first, we have reviewed the general threats which are vulnerable to almost any CPS application. Then, we deal with various threats that are distinct with different CPS applications.

8.3.1 General CPS Threat Model

The knowledge of from whom to secure a CPS is as important as the knowledge of its existing vulnerabilities and security mechanism. The definition of a security threat is *"a set of circumstances that has the potential to cause loss and harm"* [120]. The loss from an attack might be in confidentiality, safety measures, integrity, or availability of resources. On the contrary, the harm refers to harming people, systems, or the environment. We have identified the five factors which every threat has: source, target, motive, attack factor, and potential consequences.

RETRACTED CHAPTER

- **Source**: Source of attack is where the attack initiates from. It is categorized into three types: Adversarial threats, accidental threats, and environmental threats.
- **Target**: Targets are on which the attacks have been made. In this paper, the targets are the CPSs and their components.
- **Motive**: The reasons behind the attack made. It could be political, personal revenge, criminal, terrorist, spying, or cyberwar [138, 152].
- **Attack Vector**: A successful attack must have one or more of the four mechanisms: interception, interruption, modification, or fabrication [120].
- **Consequence**: The outcome of a successful attack on a CPS, such as lose of confidentiality, data integrity, privacy, availability, or safety.

8.3.2 CPS Security Threats

We consider the potential threats to each of the four applications of CPS using the proposed threat model. The threats specific to each application have been emphasized on the five factors of attack: source, target, motive, attack vector, and consequence.

8.3.2.1 Threats Against ICS

- **Politically influenced cyberwar (motive):** A cyberwar could be initiated by a hostile nation (source) with another nation (target) by remotely attacking on the nation's critical infrastructure like nuclear plant, by injecting malware or controlling their field devices (vector) which can result in a complete shutdown of a plant, huge economic loss, or polluting the environment (consequences) [8, 75, 132, 149].
- **Politically influenced espionage (motive):** A party or even a nation can use their intelligence agencies (source) to attack any rival's critical infrastructure (target) by spreading malware in their system (vector) to access or have their critical confidential data (consequence) [101, 110].
- **Physical Threats (motive):** A sensor of any environment (target) can be attacked by an attacker (source) to falsely increase or decrease the temperature of the environment (vector) resulting in control center receiving false measurement (consequence).
- **Financially Motivated Threats (motive):** A skillful customer (source) can tamper with the utility physical devices or inject false data (vector) to reduce the utility bill which will affect the utility company (target) and lose financially (consequence) [150].
- **Criminal Attackers (motive):** A capable attacker who is familiar with a system (source) could utilize the wireless connection (vector) to control a CPS application (target) to interrupt its operations (consequence).

RETRACTED CHAPTER

8.3.2.2 Threats Against Smart Grids

- **Financially Influenced Threats (motive):** A customer (source) who wants to fabricate his utility data in smart meters (vector) which will result in reduction of his utility data (consequence) made by the utility company (target) [4, 97, 98, 108, 127]. On the other hand, to advertise their product, the utility companies (source) look into the private information of their customers (target) by looking into their usage and house appliances (vector) which result in privacy violation [24, 97, 123, 143]. An attacker (source) can also have control over many smart meters (target) by injecting malware (vector) and extort money in exchange for not shutting them down which will result in a wide blackout (consequence) [4].
- **Criminally motivated threat (motive):** A capable robber (source) can consider a person's smart meters (target) to access the utility measurements (vector) by which he can predict that whether the person is home or not to conduct a successful robbery (consequence) [143].
- **Politically motivated threat (motive):** An organization (source) can gain remote access to a set of smart meters (vector) to cause a blackout, economic loss, or any disturbance (consequence) to its rivals (target) [97].

8.3.2.3 Threats Against Medical Devices

- **Criminal motivated threat (motive):** An Attacker (source) can inject modified data or retransmit the previously given command (vector) to the medical devices attached to the patient (target) to cause harm to the patient's health condition (consequence) [53]. Additionally, the attacker (source) can also jam the wireless communication of the medical device and the control center (vector) which are responsible for maintaining the desired health condition of the patient (target) will fail to conduct the accurate operations (consequence) [53, 54, 131].
- **Spying Motivated Threat (motive):** An attacker (source) can intercept the communications between the medical devices (vector) of a patient to access the confidential information of the patient (target) which results in privacy violation (consequence) [53]. On the other hand, medical devices send this information to the other control centers (target) also which contain a huge set of confidential information of numerous patients (motive) which can be accessed by a hacker (source) by intercepting the wireless communication (vector) which also results in privacy violation (consequence) [82].
- **Politically motivated threat (motive):** To harm a nation (target) politically, a hostile nation (source) can interpret and control the wireless communication of the medical devices (vector) of a political leader which can cause tremendous harm to him or even death (consequence) [153]. US Vice President Dick Cheney had the wireless communications of his pacemaker disabled as he was aware of his possible assassination [131].

RETRACTED CHAPTER

8.3.2.4 Threats Against Smart Cars

- **Criminal motivated Threats (motive):** A criminal hacker (source) can attack a car's ECUs (target) by utilizing the weakness in the wireless communications of the ECUs (vector) to cause a malfunction in the ECUs or an accident (consequence) [15].
- **Privacy invasion Motivated (motive):** A hacker (source) can hack into the TCU (vector) of a car (target) to listen to the private conversations going inside the car [15].
- **Tracking motivated threats (motive):** A law enforcement agent or a hacker (source) can hack into the GPS system (vector) to track the car (target) which is an example of privacy invasion (consequence) [7, 15].
- **Profiling motivated threat (motive):** Car manufacturing companies (source) can look into the detailed car logs stored in the ECUs of that particular car (vector) to gather detailed information about its usage and if it has violated any traffic rules or not (target), without the consent of the car owner which is a violation of privacy (consequence) [7, 60].
- **Politically motivated Threats (motive):** An unfriendly nation (source) can attack another nation's transportation system (target) by hacking into fully remote-control cars (vector) to cause large-scale accidents (consequence) [15].

RETRACTED CHAPTER

8.4 CPS Security Vulnerabilities

We first identify the existing vulnerabilities in a cyber-physical system. Then, on each of the applications, the vulnerabilities are highlighted as different applications may have different kinds of vulnerabilities. Hence, for the suitable solutions, the generic and application-specific vulnerabilities need to be distinguished.

8.4.1 Causes of Vulnerabilities

- **Isolation Assumption:** Usually the designing dependable and safe modules are focused, and the security factor is not emphasized much [93]. The logic behind this is if the system is isolated from the outside world, then automatically it is secure from outside attacks. For example, the security of ICS and Smart Grids relies on the assumption that the systems are isolated from the outside world, and they are controlled and monitored locally [11, 32, 92]. Even, the IMDs were also secured based on the assumption that they are isolated from the outside world [53] the same as the ECUs in smart cars [78]. But the ongoing development in CPS applications is no more restricted to the isolation concept. In fact, they are introducing more connections. With more connections, more access points are getting introduced to those systems which is making them more vulnerable.

- **Increased Connectivity:** With time, the connections inside a CPS are increasing at a significant rate. Unlike before, they are no more isolated from the external environment. Nowadays, they mostly rely on the open networks and wireless technologies. For example, control centers which are directly connected to the ICS and Smart Grids are also connected to the Internet which increases the chance of external attacks. In fact, it has been analyzed that a maximum number of attacks to an ICS was made locally until 2001, but after that most of them originated from outside sources [8]. This is a definite result of more connectivity. Some field devices are directly connected to the Internet for fast incident responses and more convenience which make them more vulnerable [85, 141].
- **Heterogeneity:** A CPS is built with different kinds of components which are manufactured by different entities. For example, COTS, proprietary, and third-party components are integrated to build a CPS application. Hence, a CPS is a result of more integrated such components rather than designed [32]. Each of the components has its security problems. This integration of those components invites respective inherent vulnerabilities [3]. For example, to access a computer running on Windows OS, one of the steps of Stuxnet attack was to harness the Siemens PLC's default password [101].

RETRACTED CHAPTER

8.4.2 *Vulnerabilities in ICS*

8.4.2.1 Cyber Vulnerabilities

- **Communication Vulnerabilities:** Although there have been many studies on the security issues of the TCP/IP and ICCP like popular protocols, they still have security issues as the design of these protocols was not intended to be secured [5, 56, 84]. Besides, the ICCP interconnects the control center, but it lacks basic security measure like authentication and encryption [114]. The well-known Stuxnet Attack uses the security vulnerabilities in Remote Procedure Call (RPC) protocol [99]. Besides this, the RPC has many more vulnerabilities which are used by the attackers to tamper with the ICS. The ICS which uses wired communications usually depends on the fiber optic and Ethernet. Since Ethernet uses the local area network and as a result, the components of an ICS are connected through the same medium, it is vulnerable to a Man-in-the-Middle (MITM) attack [43]. As an example, if attackers manage to access the connection between the components, they can easily intercept and manipulate all the data [118, 156]. In an ICS plant, usually, short-range wireless communications are performed under the assumption that no outsiders can get access to the communication medium. However, a malicious insider can still capture, analyze, or manipulate the traffic or even a well-skilled outsider can break into it [27]. Moreover, if employees connect their devices which are probably unsafe, to the wireless network, an outsider can use their Internet-connected devices as a vector and get into the system [42]. Long-range communications like satellite, microwave, and others are also used in ICS, but their vulnerabilities in the context of ICS have not been studied yet. It concluded that wireless communications are more susceptible to cyber-attacks like unauthorized access, active and passive eavesdropping, replay attacks, and much more discussed rigorously in the literature as in [68, 157].

- **Software vulnerabilities:** The unauthorized access to the database where confidential data are stored is one of the most popular software-related vulnerabilities [118, 168]. Emails are also contributed to spread malware. Many attacks which exploited emails are demonstrated by experiments in [39]. To gain access to a secure ICS network, an attacker usually exploits the Internet connections of the devices (e.g., laptops, smartphones, tablets, etc.) which are connected to the desired network [13].

RETRACTED CHAPTER

8.4.2.2 Cyber-Physical Vulnerabilities

- **Communication Vulnerabilities:** For sending control commands from the control center to different components, ICS uses protocols like Modbus and DNP3. These protocols are used for monitoring also. The de facto standard for communication in the Modbus protocol lacks the basic standard of security like encryption which creates vulnerability for eavesdropping [1, 9, 29]. The lacking integrity in de facto makes the data integrity uncertain [9, 39]. Even, the authorization measures are not feasible enough which may result into the controllers receiving false data or manipulated data could be sent to the actuators [149, 168]. These vulnerabilities are caused by the DNP3 protocol also as it lacks these security measurements like encryption and authorization [31, 61]. At least 23 attacks were made using DNP3's vulnerabilities, such as lack of authorization, authentication, and encryption, which was analyzed by East et al. [31]. If the primary communication between the field devices such as PLCs, RTUs and the control centers is failed, usually there is a secondary connection which is directly connected (e.g., dial-up) to the sensors and the actuators [1]. It makes the system easy to be breached as the attacker does not need to exploit any other advanced communication.
- **Operating System:** In ICS field devices like PLCs and RTUs, the operating systems which are used are Real-Time Operating System, which does not have access control measure. As a result, all users get root access which is the highest privilege. This makes the devices vulnerable to miscellaneous attacks [168]. If the operating systems have vulnerabilities, the systems running them become vulnerable also which in return makes those devices the vector of an attack on the field devices. For example, the Stuxnet attack exploited the vulnerabilities in two operating systems. The first one was exploited in the Print Spooler Service which is a vulnerability in remote code execution over Remote Procedure Call (RPC) [100]. As a result, Stuxnet could copy itself to the vulnerable computer [17]. Similar to this, the other one was Windows Server Service which also used

remote code execution in which specially crafted RPC request was sent [99], and this makes the Stuxnet capable of copying itself to other computers [17]. Some attacks use the buffer overflow vulnerability in the operating system used at the control center [149, 168]. Among the most used vulnerabilities in the operating system, buffer overflow is the most popular according to ICS-CERT [62].

- **Software Vulnerabilities:** Among the programs which are used in the general-purpose operating system to monitor and control the field devices, WinCC is popular which is a Siemens product and used to control PLCs. The Stuxnet attacks the vulnerable computers which run WinCC. At first, the Stuxnet copies itself to the vulnerable computer and then installs a DLL file in the system which is used by both WinCC and the PLC. It allows the DLL to send rogue codes to the PLC. Lack of digital signature is the main vulnerability which allows this critical action [77]. As we discussed earlier, one of the main reasons of increased vulnerabilities is the presence of COTS in CPS, and an example of this in 200 PLC models is revealed in [85].

8.4.2.3 Physical Vulnerabilities

The physical exposure of the ICS field devices, such as PLCs, RTSs, is vulnerable as they can be tampered or stolen due to lack of physical security. For example, a water canal had solar panels as its source of energy which were stolen and as a result, the control center lost all critical data of that canal for necessary operations [2].

8.4.3 Vulnerabilities in Smart Grid

8.4.3.1 Cyber Vulnerabilities

- **Communication Vulnerabilities:** The information infrastructure of a smart grid relies on certain protocols. The smart Grid's components use TCP/IP for the general-purpose Internet. As the vulnerabilities in TCP/IP are known, it is not used for the connection to the control center. However, sometimes due to misconfiguration accidentally the control center gets directly/indirectly connected to the Internet which itself is very vulnerable [25]. ICCP is used for the communication among control centers, but it contains critical buffer overflow vulnerabilities [168].
- **Software Vulnerabilities:** Along with the same software vulnerabilities present in the ICS, smart meters contain some more. Since the widely spread smart meters can be controlled remotely, it provides certain vulnerabilities for the attackers to exploit as they can control smart meters from either the meters individually or the control center. If injecting a software bug into one of the components in a smart grid is used as a vector, creating a wide blackout will become feasible [4]. More accessible smart meters in every household provide

RETRACTED CHAPTER

more access points to the attackers [108] which sometimes are used as backdoors. Santa Marta [135] discovered such backdoor to a smart meter which could allow a capable customer to gain full control over the meter including modification of the utility bill. Additionally, there is a protocol named TELENET which can be used to connect the smart meter. This protocol can be exploited to perform multiple coordinated attacks on different smart meters in a grid.

- **Privacy Vulnerabilities:** The smart meters at the households and the utility companies have two-way communication which creates vulnerabilities. An attacker can intercept the traffic of vast data generated by the smart meters which will compromise the privacy of the customer [21]. Furthermore, they can access the information about the presence/absence and daily habits of the residence.

8.4.3.2 Cyber-Physical Vulnerabilities

- **Communication Vulnerabilities:** The power grid infrastructure has the same kind of vulnerabilities as ICS in the context of the same protocols used in ICS, i.e., Modbus and DNP3. Smart grid has some additional protocols like IEC 61850 which provides some advanced communication between the substations. However, these advanced protocols do not have adequate security measures. Some of these could not provide encryption which creates the vulnerability for eavesdropping which will provide the details of customer's usage pattern to the attacker [96, 108]. The protocols which do not have significant authentication measure could be exploited to inject false data [124, 156]. One more result of this is the over-flooded network by injected bogus data which is an example of DoS attack [143, 162]. The heterogeneous components of a smart grid also create vulnerabilities. The generation plant of a smart grid communicates with the transmission plant which interacts with the distribution sector and this sector delivers the power to the customers. Each of these sectors has their security protocols which integrally are vulnerable to various kind of attacks due to lack of proper communication and collaboration [36, 58, 108].
- **Smart Meter Vulnerabilities:** As discussed earlier, due to two-way communication in smart meters components, many access points are created for the attackers to intercept the interactions [69]. This creates a backdoor in home appliances which could become an entrance for an attacker to the control center. The documentation of a smart meter was analyzed by Santamarta, and a "Factory login" account was discovered [135]. Unlike regular customers' accounts, this account would give any user complete privilege over the device. This may result into (1) Disrupted power supply, (2) attacks to other smart meters in the same network, and (3) tampered data of the collected data such as the utility bill [135].

RETRACTED CHAPTER

8.4.3.3 Physical Vulnerabilities

The field devices of smart grid face similar problems like ICS' components. As they are widespread the physical security to these field devices is inadequate [140]. They are vulnerable to the physical destructions. For instance, the power lines can be easily damaged by malicious, natural, or accidental causes. Once 50 million people suffered from large blackout due to the power line cut by overgrown trees [149].

8.4.4 Vulnerabilities in Medical Devices

8.4.4.1 Cyber Vulnerabilities

- **Obscurity Vulnerabilities:** Some medical device manufacturing company relies on the secrecy of the designing proprietary protocols due to lack of their security measures [82]. This is known as "security through obscurity." Although this has never been enough to thwart the attackers.
- **Communication vulnerabilities:** Medical devices usually communicate with their programmers through a wireless connection which is exploited for different kinds of attacks, such as injection, eavesdropping, replay attacks, and much more. Lack of encryption in the security measures allows replay attacks [52] along with the loss of confidentiality since the ICDs interact with their programmers through wireless channels. Also, patients wearing devices or with IMDs are vulnerable to privacy invasion-related attacks. Moreover, the patient can be tracked down if the unique information of the devices is inferred [53].
- **Software Vulnerabilities:** Along with the growing role of software in the medical devices, their vulnerabilities have also increased. Hence, more devices are recalled due to software-related defects [46, 54]. Since the role of these devices is to monitor and control the health of patients, a simple flaw can result in a critical health situation. The security analysis of the medical devices was publicly analyzed by Hanna et al. [54] for the first time. They discovered that a medical device named Automated External Defibrillator (AED) has four vulnerabilities such as (1) random code execution because of buffer over flow, (2) improper storage for credentials, (3) inadequate authentication mechanism, (4) firmware update without any authorization due to improperly deployed Cyclic Redundancy Check (CRC). Also, Li et al. [87] also showed that how a random CRC check in code can lead to various dangerous attacks like replay attack, unauthorized injection of data, and sending out unapproved commands.

RETRACTED CHAPTER

8.4.4.2 Cyber-Physical Vulnerabilities

- **Communication Vulnerabilities:** The dependency of medical devices, like wearable devices and IMDs, on wireless communication invites more vulnerabilities. If a medical device fails to send or receive accurate data, the patient will suffer from an undesired health condition. The chances of jamming attacks, replay attacks, eavesdropping increase. As an example of jamming attack, if an insulin pump does not receive the periodic updates from the Continuous Glucose Monitoring (CGM) device associated with the patient, the pump may not decide the accurate amount of insulin that needs to be injected, which may cause improper health conditions [87, 125]. Some attacks on computational or communication devices drain out the battery resource and the devices fail to communicate [52, 131]. Another vulnerability is, by exploiting wireless communication, the attacker could inject specially crafted data which result in undesired operations by the medical devices. Halperin et al. [52] and Gollakata et al. [48] explained that the wireless communication vulnerabilities held by ICDs could be utilized for injection attacks. Moreover, Li et al. [87] demonstrated that by intercepting the wireless communication of the insulin pump with its remote control, an attacker could gain the ability to control the device remotely. For authorization, the injected package requires the serial number of the device. Radcliffe et al. [125] showed that an attacker who retrieved the serial number could inject an unauthorized inappropriate command to the device. For the replay attack, the attacker does not have to be knowledgeable about the underlying protocols. All he has to do is capture legitimate command packets which can be retransmitted later. Li et al. [87] showed that the vulnerable insulin pump which allows replay attack may receive incorrect readings of the glucose level which will command the insulin pump to inject wrong amount of insulin to the patient which will cause undesired health problems. It was revealed by Radcliffe et al. [125] that CGM is also vulnerable to replay attacks.
- **Device Authentication:** As a result of implied trust to everyone using commercial programmer, an attacker without any technical knowledge can use those without any authorization [52]. Halperin et al. [52] showed that even Universal Software Radio Peripheral (USRP) is capable to replace a programmer and deliver malicious packet.

RETRACTED CHAPTER

8.4.4.3 Physical Vulnerabilities

Both wearable and implantable devices are vulnerable to physical attacks. For example, an attacker, who can get close to the medical devices, can tamper with those and inject malicious commands which will cause undesired health problems for the patient. The serial number of the device will also be revealed which is convenient for other attacks. Thus, there should be adequate physical security around the medical devices as recommended by Hanna et al. [54]. Nonetheless, since the designer of the devices cannot control the surroundings of the patients' wearing those, the patients, along with the devices, are vulnerable to physical attacks in an insecure location. These types of attacks are usually politically motivated [153].

8.4.5 *Vulnerabilities in Smart Cars*

8.4.5.1 Cyber Vulnerabilities

- **Communication Vulnerabilities:** To enable hands-free operations in a smart car and to provide car's manufacturing company the control to do certain operations remotely like software update, crash report and stolen car recovery, etc., cellular interfaces are used. These cellular communication channels are provided to the cars by TCU. Since Global Positioning System (GPS) and microphone are parts of these TCU, major security concerns regarding TCU are arising. The connection can be used as a vector to track down the vehicle or even become a spying tool for eavesdropping on the conversation going inside the car [15, 155].

  Among the vulnerable vectors used for an attack on a smart car, Bluetooth is the most important one [155]. To pair a device with the smart car via Bluetooth, the Telematics Control Unit (TCU) generates a PIN which has to be entered for authentication. However, this measurement is not enough since an attacker can brute-force the PIN or even inject a modified PIN by faking the Bluetooth Software. If the Bluetooth's Media Access Control (MAC) is extracted by the attackers, the car will be vulnerable to the traceability attacks as the MAC is unique and traceable [15].
- **Software Vulnerabilities:** Smart cars are the result of integration of different types of ECUs which are operated by different software. The reliance of smart cars on the ECUs has increased rapidly and as a result the possibility of a software bug, and other vulnerabilities, in the ECUs have also escalated [59]. Malicious code, injected in a software running ECU, can expose the entire car to various types of attacks. Jo et al. [66] showed that how a TCU running on Android Operating System was exploited to unlock the doors and even the GPS was tracked due to the vulnerabilities in the software. In fact, if the media player has the vulnerability it can be exploited to attack other ECUs as the player has the ability to connect to the CAN bus directly. As identified by Checkoway et al. [15], the media player can be used as vector to attack the other ECUs by injecting a malicious code installed CD and the player is vulnerable to other arbitrary codes because of its ability to resolve different media files.

RETRACTED CHAPTER

8.4.5.2 Cyber-Physical Vulnerabilities

- **Communication Vulnerabilities:** Due to inadequate security mechanisms, smart cars are vulnerable to different types of attacks [78]. Among the in-car communication protocols, Controller Area Network (CAN) and Local Interconnect Network (LIN) are used the most. However, we will review the vulnerabilities of CAN since it is used more than LIN. CAN lacks proper encryption, authentication, and authorization measurements. Due to lack of encryption, Tire Pressure Monitoring System (TPMS) is vulnerable to attacks like eavesdropping, data injection, and spoofing [130]. Using the unique ID stored in the TPMS, tracing a car becomes possible. Even more, the broadcasting nature of CAN creates vulnerabilities for DoS attacks [73]. DoS exploits the error handling mechanism of CAN bus network [22]. Another vulnerability in the security property is non-repudiation which makes it difficult to trace the source of the attack [60].
- **Vulnerabilities in ECUs:** The ECUs are getting equipped with advanced technologies for the betterment of safety and comfort. ECUs like Collision Prevention, Adaptive Cruise Control, etc., provide safety. And Comfort is delivered by the ECUs like RKE and Comfort Part Assist. These are all parts of AN network which is vulnerable to many attacks. For example, if a ECU is attacked then the attacker can also attack the other vulnerable ECUs in the same network at the same attempt [155]. ACC is the next-generation Cruise Control Driving. If the ECU is tampered externally or even internally by exploiting other vulnerable ECUs such as RKE, TPMS, and TCU, incorrect data can be provided to the ACC, as a result the car will change its speed unexpectedly which can turn into a collision.
- **Vulnerabilities in X-by-wire technology:** Nowadays, there is a trend called X-by-wire in smart cars. This technology replaces the components like steering, brakes which are controlled mechanically by electronic and electromagnetic components. It allows the driver to control the mechanical and electromechanical components by pushing some buttons. For example, Steer-, Shift-, Break- are used in this trend [145]. However, this implies more threats to the vehicle. This technology counts on FlexRay protocol which is very costly and doubtful to be widely used in the near future [145].

8.4.5.3 Physical Vulnerabilities

A car is physically vulnerable to various types of attacks. Such as if the TPMS part of a car is destroyed, the designated ECU will not receive the air pressure from the TPMS. A mechanic has physical access to a car. This opportunity makes many internal parts directly accessible to an attacker through OBD-II port [160]. Even the exterior mirror is exploited sometime as the backdoor to the internal parts [60].

RETRACTED CHAPTER

8.5 Real-World CPS Attacks

In this section, we have reviewed the attacks reportedly made on each of these applications, using the vulnerabilities discussed in Sect. 8.4. The attacks have been categorized into cyber, cyber-physical, and physical attacks based on the locations of the damages made by these attacks. The attacks which do not have impact on the actuators/sensors are considered as cyber-attacks while the attacks which directly strike the physical components are contemplated as physical attacks. Finally, the attacks which hit the physical components exploiting cyber components are considered as cyber-physical attacks. Generally, the attacks which are publicly known are very rare [121] and to find the attacks utilizing all the above-mentioned vulnerabilities is infeasible. With the brief review of real-world attacks on CPS applications, we have also provided four different taxonomy proposed by Yampolskiy et al. [164] based on attacks on ICS, Smart Grids, Medical Devices, and Smart Cars. Tables 8.1, 8.2, 8.3, and 8.4 demonstrates the real-life attacks on ICS, Smart Grids, Medical Devices, and Smart Cars, respectively. Here are some brief definitions of items used in the taxonomy:

- **Influenced object:** The object on which is attacked.
- **Influence:** The resulting changes on the attacked object.
- **Affected Elements:** Elements which got affected indirectly.
- **Impact:** Changes in the entire CPS.
- **Method:** The way the attack took place.
- **Precondition:** The pre-attacks made to make the attack successful.

RETRACTED CHAPTER

8.5.1 Attacks on Industrial Control System (ICS)

8.5.1.1 Cyber-Attacks

- **Communication Protocols:** Most of the attacks on ICS are made exploiting the vulnerabilities in communication protocols. An example of Address Resolution Protocol being spoofed was demonstrated on Supervisory Control and Data Acquisition (SCADA) system [42, 151].
- **Espionage:** Many attacks have been made to the ICS with motive of spying. DuQu and Flame are two examples of these kind of attacks [20, 110]. Flame had targeted many ICS in the Middle East world and was not discovered till 2012. The objective of this malware is to collect private data like emails, network traffic of the corporations [110]. Similarly, a group of hackers called Dragonfly attacked many corporations in the USA and Europe in 2003. Their motive was to collect classified information of those corporations. They sent fishing emails containing malware PDFs to the employees of those organizations. After opening these emails, the vector changed into water hole vulnerabilities which

RETRACTED CHAPTER

Table 8.1 ICS cyber-physical attacks

Name	Influenced element	Influence	Affected element	Impact	Method	Precondition	Reference
Web-based attacks and field devices	Web interface of the field devices	Components which are controlled by the attacked devices	Field devices become unable to be controlled properly by the authorized users	Disable the connection of the control center to the field devices	The Internet connections of the devices are exposed.		[150]
Web-based attacks and field devices	Web interface of the field devices	Components which are controlled by the attacked devices	The configurations of the field devices are lost	Inject malicious code into the devices	Induced vulnerabilities into the TCP/IP protocol due to COTS implementation		[150]
Maroochy	Sewage pumps	Malfunction in the pumps	The configuration of the pump station	Polluted environment and monetary loss due to sewage flood	The configurations of the pumps are manipulated	Well informed insider who is familiar with the system	[141]
Modbus worm	Communication network of ICS	Damage to the communication network	Components connected to the network	False data injection and even rebooting the entire system	Inject malicious code into the system	Communication traffic of ICS is accessible	[39]
Stuxnet	Centrifuges of PLCs	Exaggerated rotation of centrifuges	Rotors attached to the centrifuges	Physically damaged for a long term	Unauthorized commands sent to the centrifuges from the PLCs	Installation of Stuxnet in PLCs	[17, 77, 111, 164]

RETRACTED CHAPTER

Table 8.2 Smart grid cyber-physical attacks

Name	Influenced element	Influence	Affected element	Impact	Method	Precondition	Reference
Cyber extortion	Smart meter attached to the household	No power supply to the household	Residence of the house	Extortion in exchange for power supply	Control the smart meters through its Internet connection	Intercepted two-way communication with the utility company through Internet	[112]
Aurora experiment	Circuit breakers of generators	Explosion of the generator	Power Generators and utilities fed by those generators	Power cut due to explosion of the generators	Rapidly open and close circuit breakers	Ability to communicate with the device	[134, 165]
False data injection	Smart meters	Manipulated billing information	Utility companies	Financial loss	Inject false data to the smart meters installed in the household	Physical access to smart meters	[156]
Theft	Metal and copper wire	Theft of equipment	Smart grid	Disconnection of the field devices	Steal the metallic parts from the field devices	Physical access to the field devices	[122]
Jamming attack	Wireless communication layer	Delay of communication	Smart grid	Malfunction of various components	Inject many unnecessary unauthorized packets in the communication channel	Access to the communication channel.	[90, 91]
Vandalism	Transformers	Damage to transformers	Smart grid	Wide blackout	Damage transformers	Physical exposure of transformers	[41]

RETRACTED CHAPTER

Table 8.3 Medical devices cyber-physical attacks

Name	Influenced element	Influence	Affected element	Impact	Method	Precondition	Reference
DoS	A certain medical device	Shutting down of the device or inability to function accurately	Patients with those attached medical devices	Unhealthy condition of the patient due to miss-treatment	Replay the previously intercepted commands	Intercept the commands sent to the attached medical devices from the control device	[52]
Replay attack	Continuous glucose monitoring (CGM) device	Incorrect measurement of glucose delivered to the pump	Patients along with the attached insulin pumps	Delivery of incorrect amount of insulin to the patient	Replay the previously intercepted commands	The communication between the CGM and insulin pump gets intercepted	[125]
False data injection	Insulin pump	Manipulated data transferred to the insulin pump	Patient's wrong treatment	Patients' health conditions	Imitate the CGM to send the inject false data to insulin pump	The communication between the CGM and insulin pump gets intercepted	[87]
Unauthorized commands injection	Insulin pump	Improper actions by the insulin pump	Patient's wrong treatment	Patients' health condition	Inject unauthorized commands to the insulin pump	The communication between the insulin pump and its remote controller gets intercepted	[87]

RETRACTED CHAPTER

Table 8.4 Smart cars cyber-physical attacks

Name	Influenced element	Influence	Affected element	Impact	Method	Precondition	Reference
DoS	Body control module	Random drop in speedometer	Instrument panel cluster (IPC)	The whole IPC freezes	Disabling the communication of CAN from/to the BCM	Physical access to controller area network (CAN) bus	[73]
DoS	Windows of car	Unable to control open/close windows	ECUs connected to the windows controlling ECU	Passengers' safety is compromised, and discomfort	Send back previously eavesdropped packet, and reverse engineering	Physical access to controller area network (CAN) bus	[60, 73]
Malware injection	Bluetooth ECU	Ability to connect to other ECUs	Transmission control unit (TCU) with other ECUs with cyber and physical capabilities	The entire vehicle safety	Exploiting Bluetooth ECU, send malware to another ECU	Control over the Bluetooth paired devices	[15]
Malware injection	Telematics control unit	Ability to track the vehicle	Other ECUs which are connected to the TCU through cellular channel	Safety of the entire vehicle can be compromised due to possible large-scale accidents	Connection of the Bluetooth paired device is exploited, and a malicious payload is sent to the TCU	Vulnerabilities in the connection of the Bluetooth paired device	[15]

(continued)

RETRACTED CHAPTER

Table 8.4 (continued)

Name	Influenced element	Influence	Affected element	Impact	Method	Precondition	Reference
Malware injection	Any specific ECU	Packets containing malware are spread to the other ECUs	CAN bus which is connected to the ECU	Other ECUs in the same CAN bus network	Spread malware through CAN bus network	Access to the wireless connections	[60, 73]
Replay attack	Lights of the vehicle	Unexpected turn-off/on of the lights	The targeted vehicle with its passengers along with the other surroundings	Life-risking consequences	Retransmit previously eavesdropped packets	Ability to access the CAN bus network	[73]
Spying attack	TCU	Eavesdropping the in-car communications	All other ECUs connected to TCU	Compromised privacy of the passengers	Injecting malware to the TCU exploiting wireless connections	Vulnerabilities in the cellular network of the car	[15]
Relay attack	RKE system	Ability to open the car without using the key fob	Entire vehicle	Theft of the entire vehicle	Relaying the captured LF beacon signals sent from vehicle to key fob and resulting UHF signal sent from key fob to vehicle	Attacker must be equipped with tools such as antennas and amplifiers to relay	[45]

would redirect the readers to a malicious website hosted by those attackers. This malware allowed the attackers to access confidential information stored in those systems [147].

- **Accidental Attack:** Software updates in the systems are necessary to maintain less vulnerabilities. However, if a software is updated with rebooting the system and the system has not completed the backup, all the critical data stored in that system will be erased. If that system is one of the control center systems, other components will also suffer from this and operate abnormally which may even cause plant shutdown [11].
- **Web-based Attacks:** In 2011, a number of oil and energy companies were attacked by Night Dragon which extracted private information from these plants. The attack exploited many vulnerabilities and combined different types of web-based attacks like SQL and malware injection [1, 101].

8.5.1.2 Cyber-Physical Attacks

- **Communication Channels:** As mentioned above, dial-up connections connect the field devices directly which give the attackers direct access to the devices through the dial-up connection. Once in 2005, billing documentation of a water utility pump was modified by exploiting this dial-up connection in the canal system [150]. Although no physical damage was made, if intended, the attacker could have done critical physical damage also.
- **Resentful Insiders:** The workers of a company are familiar with the architecture and networking of the system. Once an ex-employee disrupted the functions intentionally of a sewage treat system of Maroochy Water Services located in Australia in 2000. The attacker used the knowledge as an ex-employee and exploited the vulnerabilities. As a result, the company faced a huge financial loss and the environment got tainted as many streets were flooded [141].
- **Modbus Worm:** Fovino et al. [39] did a tremendous work targeting the malware which is very alarming. A malware was crafted by them which could exploit the vulnerabilities like lack of authentication and integrity present in the Modbus protocol. This worm performs two kinds of attacks: (1) Identify the actuators and sensors, and then DoS including message, and (2) send unauthorized commands to the actuators and the sensors.
- **Malware:** Software vulnerabilities are exploited as a vector to target the physical devices. Stuxnet will be a better example for this. It targets the physical devices through software vulnerabilities [164]. Stuxnet's attack is categorized into two phases: (1) identify the object to target, and (2) hijack the PLC [77]. The first step is achieved with the help of two vulnerable computers running on Windows OS, i.e., shared printing server and Windows Server Service. Remote code execution using RPC would be possible through both vulnerabilities. The first one helps Stuxnet to install itself, whereas the next one allows it to spread to another computer. This process could affect millions of computers. However, because of specific targeted PLCs, the computers which are connected to that specific PLC

RETRACTED CHAPTER

will be influenced. Once the Stuxnet is installed it looks for the software which monitors and controls the PLCs, and that would be Siemens WinCC. To find the accurate Siemens WinCC for the targeted PLC, a thorough analysis is done by the Stuxnet [77]. Once the software is determined, the next step is injecting malware to disrupt the operations of the PLCs. We would refer [111] for detailed analysis on Stuxnet.

- **Web-Based Attacks:** A web-based interface is exploited by attackers as a vector to attack the PLCs. They open up multiple connections and leave them open until they cannot be accessed by the authorized users which results in DoS attacks. Sometimes they send a link to the authorized users which contains malicious Java script which injects bug into the TCP/IP protocols and the controller gets affected as a result [150].

8.5.1.3 Physical Attacks

- **Unintended Attack:** Zotob Worm is not intended to attack ICS, although it caused several manufacturers to shut down their plants. Once, the US company, Daimler Chrysler, was forced to shut down their 13 plants as a side effect of the attack by this worm [149]. This influenced a lot of researchers to analyze the detailed consequences of this attack. Among those, Fovino et al. [39] showed how critical could be the collateral damages of this attack. The consequences include rebooting of ICS servers, creation of vulnerabilities of arbitrary code injection, stimulating DoS attacks, and infecting personal computers.

RETRACTED CHAPTER

8.5.2 Attacks on Smart grids

8.5.2.1 Cyber-Attacks

- **DoS Attacks:** In a smart grid, time is a critical variable. If there is too much delay in the flow of instructions, the components will operate undesirably. If different layers of the network of a smart grid are flooded, it will result in a DoS attack. Lu et al. [90] have analyzed the effect of a DoS attack in a smart grid. In addition, the deployment of wireless communication in the physical layer of smart grid has significantly increased which opens up the vulnerabilities for jamming attacks as shown in [91].
- **False Data Injection:** Injecting false data in the smart grid components leads to disrupted operations by the components. Liu et al. [88] have demonstrated a simulation in which they injected a set of false data and analyzed the consequences. They assumed that the attack had the pre-intrusion of the attackers to the control center and injected false data into the system and as a result, various components operate improperly. Moreover, the operating utilities will also face significant economic loss [156].

- **Untargeted Malware:** Sometimes, other components also get affected because of attacks to the targeted components. In 2003, the traffic between the substations and the field devices got disrupted by the Slammer worm and consequently the energy sector had the impact [8].
- **Customer's information:** Analyzing the interaction between a smart meter located at a house and the control center, the attackers can extract classified information of the customer. Such as the attackers can predict the lifestyle of the customer, when the customer is present at home, when they sleep, which house appliances are preferred, and many more [109].

8.5.2.2 Cyber-Physical Attacks

- **Cyber Extortion:** Taking control over a smart meter, the attacker can extort money from the customer in return of not doing any large-scale damage to his households [112].
- **Blackouts:** If a smart grid is targeted for a DoS attack, mostly the consequence will be a blackout. Idaho National Laboratory experimented on a generator in 2007. The purpose of the experiment was to see what will be the impact on the generator due to a cyber-attack, and the results were infeasible [26]. In 2003, Ohio and Florida had experienced a wide-scale blackout which is believed to be the consequence of attacks done by the People's Liberation Army [55]. The USA had experienced over 800 blackouts in 2014 but the reasons are still unknown [122]. Although it is suggested by some speculation that such blackouts were the results of some cyber-physical attacks on the smart grids [55].

8.5.2.3 Physical Attacks

- **Natural Incidents:** The physical exposure of the field devices is the reason behind physical attacks. Natural calamities are unpredictable and uncontrolled which can cause widespread damage to smart grid's field devices. For example, an ice storm in Philadelphia had caused a broad blackout for several days which affected over 500,000 people [122]. Growing trees, wild animals, and severe storms can easily damage the field devices and since the power transmission is widely spread, the consequences will be affected on a vast population. In 2014, wild animals caused around 150 blackouts in the USA by damaging the power cables [122].
- **Theft:** The field devices are made of metal and copper wires which have a good value in the market. Thieves steal those equipment which cause disconnection and as a result people suffer from blackouts. As an example, over 3000 people in Virginia had suffered from a blackout due to theft of equipment [122].
- **Car Accidents:** There were 356 outages due to car accidents which damaged transmission towers, power poles, or transformers [122].

RETRACTED CHAPTER

- **Vandalism:** Attackers can intentionally damage the field devices of smart meters. Once a sniper shot over 100 rounds at a substation in California damaging around 17 transformers [41].
- **Terrorist Attacks:** A group of terrorists can attack a transmission control of smart grid to cut off communication due to lack of power. As an example, in 2014, terrorists blew a large section of transmission control in Yemen using a rocket launcher which resulted in a nationwide blackout affecting over 24 million people [64].

8.5.3 Attacks on Medical Devices

8.5.3.1 Cyber-Attacks

The attacks on the medical devices are mostly performed in an experimental environment. We have reviewed the attacks on some limited medical devices such as insulin pump, IMDs. The successful attacks made on the insulin pump could be a possible case for the other medical devices due to the similar hardware components and communication channels.

- **Privacy Invasion:** For a successful attack on a medical device, the attacker should be equipped with the device type, its PIN, and the authorized commands to disrupt the device. The authors of [87] have implemented a successful attack and showed that three factors must be known by the attacker: existence of the device, it's type, and PIN. Halperin et al. [52] have also revealed the classified information of the patient along with the device unique number by experimenting an attack on an ICD medical device.
- **Replay Attacks:** If the PIN of a medical device is intercepted by an attacker, it can be exploited in the future to replay the eavesdropped packet [87]. As a result, the insulin pump will operate based on misinformed decisions [125].

8.5.3.2 Cyber-Physical Attacks

- **Replay Attacks:** An ICD was turned off when it was supposed to be working accurately, by Halperin et al. [52]. They replayed the "turn off" command which was used earlier as the commands to turn the device off. Any replay attack can retransmit the previously given commands to the CGM and insulin pump if the software vulnerabilities for replay are exploited by the attacker [87, 125].
- **False Data Injection (FDI):** Li et al. [87] experimented to inject false data into an insulin pump and they could control the pump remotely such as shutting down and resuming the pump.

RETRACTED CHAPTER

8.5.3.3 Physical Attacks

It is not a challenging task to physically access medical devices. The type and unique serial number of the devices can be obtained by a third party which is an example of physical attacks to medical devices [125].

8.5.4 Attacks on Smart Cars

8.5.4.1 Cyber-Attacks

Most of the researchers have done theoretical or simulation-based experiments on smart cars. Only a few have experimented on the actual real cars [15, 60, 73, 102]. To attack a car's internal network an attacker must go through the OBD port II, media player, or wirelessly connected devices, like smartphones. Once the attacker can access the internal network of the car, a lot of opportunities to launch an attack successfully are open.

- **DoS Attack:** A demonstration of DoS attack was done by Koscher et al. [73]. They disabled the interaction of CAN with the Body Control Module (BCM), resulting in the speedometer to drop from 40 to 0 mph instantly and also freeze the whole Instrument Panel Cluster. The freezing of IPC is like, if the driver increases the speed of the vehicle it will not be shown in the speedometer. As a result, the driver will be unaware of the increased speed and the chances of a severe accident will rise critically.
- **False Data Injection (FDI):** The BCM constantly sends the package to the speedometer containing updated speed of the vehicle which keeps the driver aware of the accurate velocity of the car. An attacker might intercept the data transmission between the BCM and the speedometer, which would modify those and forward the incorrect speed [73]. Another possibility is the correct status of the airbags installed in the car can be modified and, even if they are not in the correct state, they may appear healthy due to data modification [60]. In [51] the authors have shown how a customer can manipulate the data received by the insurance dongle to estimate the rate so that it will show lower insurance price.
- **Privacy Invasion:** The in-car conversation can be eavesdropped if the cellular interface in the TCU is exploited by an attacker as demonstrated by Checkoway et al. [15]. They can extract many other private information regarding the vehicle and its owner. Also as Ed Markey, a US senator, had reported, the manufacturing companies store many private information such as driving history and the performance of the car [95].

RETRACTED CHAPTER

RETRACTED CHAPTER

8.5.4.2 Cyber-Physical Attacks

- **DoS Attack:** As examples of DoS attacks, passengers are not able to close any open windows, the theft alarm system of the car doesn't work when it is needed [60], etc. Jamming RKE signals is an example of DoS attacks on the wireless communication.
- **Malware Injection through Bluetooth:** Exploiting the wirelessly connected devices, an attacker can control the other ECUs which are connected through the same network to which the ECU of the Bluetooth connectivity is connected. A successful attack via Bluetooth was conducted by Checkoway et al. [15] in which they compromised a connected smartphone device. The connectivity of the device with the smart car's TCU, which is the Bluetooth ECU, was exploited as a malware named Trojan horse that was injected in the smartphone. After the connection is compromised, the malware sends a malicious payload to the TCU and in result the attacker gets the ability to control other connected ECUs such as Antilock Braking System (ABS). Another attack was shown by Woo et al. [161] that how a mobile device app can be exploited to attack a car's OBD-II port.
- **Malware Injection through OBD-II port:** The OBD-II port is the gateway for the attacker to control the internal networks of various ECUs. For example, Hoppe et al. [60] demonstrated that if an attacker equipped with the OBD-II port of a car injects malicious command, it will develop into DoS attack. The consequences are preventing passengers from opening or closing windows, showing the incorrect status of the airbags, false information regarding air pressure of the tires, and many more.
- **Replay Attacks:** This attack requires the attacker to intercept the CAN network traffic when certain functions are being done by specific ECUs so that those can be replayed to reactivate those functions. Koscher et al. [73] could disable the interior and the exterior lights of a vehicle by delivering previously eavesdropped packets.
- **Packet Injection:** The first step for this attack is to get access to the CAN network. Once an attacker gets access to the CAN network, an enormous number of attacks become feasible. For example, many functions of the car's engine can be disrupted by exploiting the OBD-II port such as increasing the Revolution Per Minute (RPM), disabling the engine's cylinder or even the whole engine. Electronic Brake Control Module controls releasing and locking of the brake. If random modified packets are sent to EBCM, the driving will become unsafe [73]. By injecting arbitrary packets, Lee et al. [83] was able to disrupt many functions of multiple vehicles by performing fuzzing attack. This attack is about capturing the CAN ID and flooding the network by sending arbitrary packets having the same ID.

8.5.4.3 Physical Attacks

- **Relay Attacks:** Many cars have keyless entry nowadays which is like unlocking/locking the car from the key fob. In this attack, the RKE is being targeted

where the vehicle communicates with the key fob. At first the periodical LF Beacon signal, sent by the vehicle to its key fob, is exploited by the attacker to know if the key fob is in close range or not. The attacker relays the communication to send an "Open" Ultrahigh-Frequency signal to unlock the car and in this way the attacker can even start the engine. Eight different manufacturers have implemented this attack successfully on ten different vehicles [45]. This is also an example of Man-in-The-Middle (MITM) attack [158]. Garcia et al. [47] have also implemented these successful attacks by exploiting simple cryptographic measures in the physical layer communication to access the vehicle by coning the car key.
- **ABS Spoofing:** Shoukrey et al. [139] have demonstrated such successful attacks where the target is ABS wheel speed sensor. They have installed a malicious actuator which produces a different magnetic field disrupting the original magnetic field generated by the ABS wheel speed sensor and sends incorrect information to the ABS ECU.

RETRACTED CHAPTER

8.6 Security Control and Solutions

In this section, we describe different solutions in CPS controls. The different solutions can be classified into three different types. Some are application-specific solutions, some are general solutions regardless of application, and some solutions are cross-domain.

8.6.1 General CPS Controls

In this, we review general solutions to secure CPS regardless of the application. The first step of each solution is addressing the causes of vulnerability.

- **Superfluous Connectivity:** Security measures should be taken to prevent unauthorized access to the access point. The protocols used for these communications are well-known proprietary protocols (Modbus, DNP3) or open protocols such as TCP/IP. The proprietary protocols are full of vulnerabilities because of isolation from public testing [3].
- **Communication:** Improved security solutions at communication level in ICS. Intrusion Detection System (IDS) should be designed in such a way that long-delays become intolerable. Mitchell and Chen [103, 106, 107] focus on designing improved IDS which are time-critical. **Device Verification:** The software running on CPS should be authentic. One such verification process is Trusted Platform Module (TPM). TPM is hardware-based solutions providing physical security, which is infeasible to provide in some ICS and smart grids. Therefore, there is the need for revised TPMs considering limited CPS resources.

8.6.2 Application-Specific Controls

8.6.2.1 ICS Controls

- **Modern design:** ICS needs security solutions which are specific to a system. For such solutions, numerous factors should be taken into consideration, such as cyber-physical interactions, and heterogeneity of components and protocols. Most ICS aims at providing reliability to the system during non-malicious failures as suggested by Cardenas et al. [12], but in the current scenarios, cyber-attacks are more common than before. Therefore, security should be taken into consideration besides reliability when designing innovative solutions.
- **Add-on security for Protocols:** Various modifications have been proposed to modify current protocols such as Modbus, DNP, and ICCP to improve the prior security measurements of the traditional IT solutions. For providing non-repudiation, authentication, and preventing replayed attacks, Secure Modbus framework was proposed by Fovino et al. [40]. To add integrity, authenticity, and confidentiality to the security measures, DNPSec has been suggested by Majdalawieh et al. [94].
- **IDS:** It is less complex to design an IDS for ICS compared to traditional security framework for IT. The ability to predict the traffic and the static networking is the reason behind this [75]. A set of goals to be monitored by IDS in ICS is presented by Zhu et al. [167] which are (1) ability to detect any access to the communication links of sensor/actuators and controllers, (2) detection of any kind of customization in the settings of sensors, and (3) physical tampering of actuators. Also, WildCat, a solution to control the physical exposure of ICS plants' wireless network, is presented by D'Amico et al. [27]. This WildCat should be installed in the security guard's car to detect any suspicious wireless activities going on in the perimeter of a CPS plant. The collected information is sent to the control center where it will be analyzed and will send the location of the activity source to the guards. For further details about current IDS solutions for a ICS plant, we will recommend [6, 16, 75, 76, 107, 126, 167].
- **Remote Access:** The field devices must be controlled by only authorized personnel remotely, as suggested by Fernandez et al. [35]. To secure the field device, a designated laptop should constantly be operating through VPN to detect any unauthorized activity. To avoid web-based DoS attacks, Turk et al. [150] suggested that any idle connection should be closed which also helps to reduce the complexity of multiconnection.
- **Encryption and Key Management:** Encryption is a fundamental requirement for ICS systems and the delay in it could be very crucial in a time-sensitive environment. To solve this, a new key management was designed by Choi et al. [23] for specifically ICS which does not cause any delay. ICS environments are widely spread and to protect them, Cao et al. [10] have come up with a new layered security protocol which is based on Hash Chains. This layered security protocol (1) divides the ICS into two different zones based on high-security and

RETRACTED CHAPTER

low-security levels, and (2) manages a lightweight key mechanism. This way, even though an attacker can break through the security of low-level security-based ICS components, accessing the high-level security-based components would not be possible.

- **Software Control:** To continuously update the modified security measurements into the system is a very rigorous and complex process. To prevent the Stuxnet attack, Windows have released a security patch which focuses on Stuxnet-related attacks [77]. Similarly, the manufacturers of ICS components must keep up with modification of security measures of the system and then manufacture the compatible devices. This way it will be ensured that no old vulnerabilities are there in the system [67].
- **Standardization:** The leading bodies like the National Institute of Standards and Technology should focus on the security measures of ICS significantly as both the technical and operational controls are critical. Neglecting either one can be very critical for the entire system. Stouffer et al. [144] have provided a solution regarding this issue. They proposed guidelines for technical problems, like IDS, firewalls; and operational control such as awareness, security, and training of the employers. The operational control is as important as technical problems. For example, as per the report by ICS-CERT, most of the attacks made to ICS are done by phishing [1]. If the employers, without awareness, open those malicious emails, the entire system could become vulnerable [114]. According to the comparison done by Sommestad et al. [142], standardization bodies normally focus on either technical or operational problem, but it is highly required to be focused on both.

RETRACTED CHAPTER

8.6.2.2 Smart Grid Controls

- **DoS Controls:** Attacks like DoS at the network layer are prevented by filtering malicious packets, rate-limiting, and reconfiguring network architecture. Unlike the first two, due to the static nature, the third one will not be easy for smart grids. Also, security techniques in smart grids usually focus on the wireless jamming kind of attacks. The techniques which prevent DoS attacks are divided into four categories: packet-based, signal-based, hybrid, and proactive detection [156].
- **IDS:** Due to the enormous size of smart grids and the heterogeneous components, designing IDS for smart grids is very difficult [143]. The design of IDS for the smart grids must be different from the ones built for traditional IT systems to reduce the possibility of false data injection. An IDS is proposed by Jin et al. [65] which is anomaly-based and uses artificial ants and invariant detection, with Bayesian reasoning approach, to detect any malicious activity. In addition, another IDS was suggested by Mitchell and Chen [105] that works on behavior rule which protects the cyber-physical devices of smart grids, such as subscriber energy meters, data aggregation points, etc. Another significant contribution made by Liu et al. [89], who presented an IDS, which prevent the ICS from false data injection.

- **Authorization and authentication:** Employees usually have access to certain field devices with authorization and authentication. The problem is that the smart grid is spread vastly and most of the field devices share the same authorization credentials. This makes any malicious employee capable of tampering with any of those field devices, and the identity of the attacker could not be tracked as other employees also have the authorized access. Hence, Vaidya et al. [154] came up with a mechanism which strengthens the authentication and authorization of field devices. This mechanism provides legitimate employees the ability to access the field devices remotely from the automation systems in the smart grids, and it relies on elliptic curve cryptography.
- **Modern designs:** Each of the aspects of a CPS needs to be approached differently due to constantly evolving security issues. Mo et al. [108] have proposed the area "cyber-physical security" for the first time. This approach considers the details of both cyber and physical aspects of security. They have demonstrated their approach on two different kinds of attacks: stealthy deception and replay attack. The importance of each of the two aspects, cyber and physical, has been emphasized in the above-mentioned literature. However, the approaches are enhancing the existing protocols which are a temporary solution. Hence a whole bottom-up redesign of the system is desired.
- **Add-on Security:** To prevent the advanced attacks, the trend is about merging the required additional security with the existing one. For example, secure DNP3, which has basic security measurements, such as authentication, confidentiality services, and encryption, is an advanced version of simple DNP3. In the simple version, the add-on security is added by placing another layer of security in the communication level of these protocols [156].
- **Privacy-preserving Controls:** When the data flow from the smart meter to the utility company, due to lack of confidentiality, the usage and patterns of the consumer can be intercepted as well as the data can be modified due to lack of integrity in the security protocols which may result in disrupted billing information [97, 143]. To solve these problems, a certain number of techniques have emerged to provide better privacy when the data is in transit between smart meters and the utility companies [34, 156]. Attacking the smart meters attached to a household, the occupancy of the house can be predicted to break in successfully. As a solution to this problem, Chen et al. [19] have proposed a mechanism named combined heat and privacy (CHP) which makes the usage data look like the house is always occupied by tricking the occupancy detection techniques.
- **Standardization:** To secure the communications among the smart grids, certain standardizations have been introduced by several bodies like NIST and IEC. For example, such guidelines for smart grids are developed by NIST in the report 7268 [116]. In addition, standards like TC57, 6235 are developed by IEC [25].
- **Preventing disabling of smart grids:** To prevent the exploitation of disabling feature of a smart grid, Anderson and Fuloria [4] have suggested that the manufacturers should program smart meters in this way that they could let the customer know, in enough time, in advance before the malicious command takes

RETRACTED CHAPTER

effect and the meters get disabled. This may help in the detection of DoS attack also.

- **Physical Security:** To prevent the physical tampering with smart meters, NIST standard states that all the meters should have cryptographic access to the meter and must be sealed inside tamper-resistant units [116].

8.6.2.3 Medical Devices Control

- **Authentication:** Authentication: To prevent unauthorized access to the IMDs, Halperin et al. [52] have proposed a cryptographic-based mechanism along with a key exchange procedure which improves the authentication. Both mechanisms rely on external radio frequency, as a source of energy, instead of batteries. In addition, another protocol named Out of Band (OOB) was deployed to improve the authentication measurements. This authentication protocol uses a different channel than the one which is used for communication [131]. For advanced key generation in encrypted communication, heart rate, glucose level, electrocardiograms can also be used in Body Sensor Network (BSN) [131, 136]. The movement of a patient can also be used for key generation [117].
- **Intrusion Detection System:** A mechanism that alarms the patient whenever it detects any unauthorized attempts to interact with IMDs was proposed by Halperin et al. [52]. Similarly, Gollakota et al. [48] also proposed a mechanism named Shield which detects and prevents any unauthorized attempt to connect IMDs wirelessly. In addition, there was an attempt by Mitchell and Chen [104] on how to prevent any posed threats by disrupted actuators and sensors. The mechanism proposed by them can detect the affected actuators and sensors by behavior rule-based Intrusion Detection System but it is not designed for the IMDs or wearable devices. Their technique is applicable for stand-alone devices which work solely such as cardiac device and vital sign monitor.
- **Location-Based Control:** Some security technique relies on protocols based on distance bounding. This protocol prevents an attacker to attack remotely. Various techniques such as received signal strength, ultrasound signals, electrocardiography, etc. determine the limit of distance [166]. However, since these techniques do not provide any authorization, other mechanisms are needed to be incorporated [131].
- **Thwarting Active and Passive Attacks:** Body Coupled Communication thwarts most of the active and passive attacks made on the insulin pump as stated by Li et al. [87]. They have experimented with this communication and showed that since this communication of an insulin pump uses the human body as their medium to communicate, instead of any wireless communication, it thwarts the possible attacks by exploiting the wireless channel. To tamper the insulin pump, the attacker needs to reach very close to the patient which is a bar for most of the attackers.
- **Shifting Security to Wearable Devices:** The IMDs and wearable devices have their risk management security measurements, and this can be challenging for

RETRACTED CHAPTER

shifting the security measurements to another device. For example, to replace a patient's IMD with a more secure device, the process can be life-risking at first. Even if it is not life-risking, regarding battery and computational resources, the shifting of security techniques could be still expensive. Hence, the optimal solution is to deploy another device which will solely operate on the security issues. Xu et al. [163] have designed a device called IMD Gaurd which defends the medical devices against spoofing and jamming attacks. Similarly, as previously discussed, Gollakota et al. [48] proposed the shield device which will defend the wearable device from any unauthorized attempt to interact.

- **Cross-Domain Solutions:** Here is a certain similar limitation in both smart cars and medical devices such as constraints of data and power. Hence to defend from eavesdropping and replay attacks, the rolling code encryption of smart cars is implemented in medical devices as suggested by Li et al. [87].
- **Standardization and recommendations:** The leading body in the standardization of medical devices is the Food and Drug Administration (FDA). There are several standards and guidelines issue by the FDA for the manufacturers of the medical devices. They have suggested in 2005 that the usage of COTS creates the maximum number of vulnerabilities since it has the capability to be accessed remotely [37]. Another standard regarding cyber security was posted by them in 2014 [38]. However, they lack the intensity that mandates following of these guidelines which allow the manufacturers to follow their preferred guidelines. To resolve this issue, the latest BAN standard, IEEE 802.15.6, has been implemented to stop the manufacturers from the production of less secure medical devices [63].
- **Allowing vs. disallowing remote functionalities:** To prevent the attackers from intercepting the channel between the patients' medical devices and the remote physicians, the manufacturers should limit this remote access of the medical devices. So, it is suggested the medical device should not receive remote commands from the physician but should only send the patients' log and health status to the physician. Although this will prevent the medical devices from unauthorized commands, it will also limit the complete usability of the device [82]. Hence, Hayajneh et al. [57] came up with a cryptographic system named Rabin public key which prevents the medical system from unauthorized commands even if they are passed to the medical devices.

RETRACTED CHAPTER

8.6.2.4 Smart Cars Controls

- **Unimplemented promising controls:** There are several promising controls which have not been implemented yet. For example, Wolf et al. [160] have proposed authentication gateway, firewalls, and encryption to secure the bus network. Another security paradigm named defense-in depth, i.e., detection, prevention, countermeasures, deflections, and recovery, was suggested by Larson et al. [78] as the replacement design of the security measure in the cars.
- **Cryptography:** Although, cryptography adds advanced authorization, integrity, and authentication, the computational cost of these will be high due to the

limited functionalities of cars' components. Thus Wolf et al. [159] presented Hardware Security Module which is cost-efficient as it is hardware based. This mechanism secures the communication channels of the ECUs in a car along with V2V communication channel. In addition, a standard for equipping the car with better security measurements, Escherich et al. [33] designed Secure Hardware Extension which adds secure boot and secret key protection to the cars' ECUs.

- **Redefining Trust:** To disable the arbitrary ECUs from performing operations to diagnose and reflash, a trust-related control was presented by Koscher et al. [73]. They also implemented another trust-related control which requires authentication and authorization for the ECUs which are allocated for the reflashing and diagnostic operations. For the successful implementation of these, trusted platforms along with remote verification are required [70].
- **Restricted Critical Commands:** Physical access to the cars can be a gateway for attackers. There are certain commands which require physical access to cars for implementation, and this could be critical as any benign malicious command could be a serious attack. Koscher et al. [73] emphasized on this part that physical access to the car is always dangerous. If the number of commands requiring physical access is restricted the convenience and flexibility of the car will be affected. So, such security mechanism should be implemented which will balance both sides.
- **Bluetooth:** The TCU controls Bluetooth connectivity of the cars which is also connected to the other ECUs. Hence, attackers can exploit connected electronic devices, which are connected to the cars via Bluetooth, and attack other ECUs of the car through TCU as well [15]. For the need for extra security layer to secure Bluetooth connectivity, Dardanelli et al. [28] proposed a mechanism which is applicable for two-wheeler vehicles but should be efficient for cars also. To process thorough authentication of the smartphones before connecting to cars via Bluetooth, a mechanism was also suggested by Woo et al. [161]. This helps to reduce the number of attacks exploiting vulnerabilities in Bluetooth connected smartphones.
- **IDS:** Most of the Intrusion Detection Systems are designed for CAN network protocols, whereas a very few are designed for other protocols such as LIN and FlexRay. A specification-based IDS is designed by Larson et al. [79] which is installed in every single ECU. Another behavior-based IDS is designed for both FlexRay and CAN network by Stefan and Roman [137]. As cost is an important factor for the implementation of security mechanism, a very cost-efficient mechanism of anomaly-based IDS is designed by Miller and Valasek[155]. Another anomaly-based IDS which uses time as a constraint is very effective for detecting intrusion or any anomaly. It is designed by Cho and Shins [22], and this mechanism utilizes the measurements of the time intervals of periodic messages to uniquely identify each of the ECUs. Taylor et al. [148] have proposed an IDS mechanism which compares the frequency of currently sent packets with the historically sent packet which had strict frequencies. This way it can detect anomalies in the frequency of delivered packets.

RETRACTED CHAPTER

8.7 Security Challenges

8.7.1 Challenges in General CPS

- **Security by Design:** Most of the CPS model is not secured enough in their design model because they are not considered enough due to their isolation from other systems in a physically secured environment, such as no Internet connection which makes the physical security measure the most important one [144].
- **Cyber-Physical Security:** To provide optimal cyber-physical security, the cyber and physical aspects have to be considered separately with the same importance. This way the cyber-attacks with physical consequences will be better predicted and prevented [49]. The solutions of the attacks on CPS will be focused on cyber only unless the fundamental differences between the physical and cyber aspects are properly contemplated as suggested by Neuman et al. [113]. A new field named "Cyber-Physical Security" was proposed by Mo et al. [108]. They have also described some novel solutions regarding cyber-physical security, especially for smart grids. The systems' ability to survive under an attack carries the same importance as the security challenges. A set of security solutions including the systems' survivability are discussed in [12].
- **The Real-Timeliness Nature:** The absence of real-time requirement affects the security model [14, 113] since the real-time decision is very crucial for the attacked CPS system. Hence, contemplation of the interactions between cyber and physical aspects gives the full picture of the CPS model with which arises the importance of risk assessment [14].
- **Uncoordinated Change:** A CPS usually have many stakeholders among which most of them are somehow related to the system such as manufacturers, operators, and implementers. Hence, while implementing any changes in the system, the coordination among them is necessary. Otherwise, due to lack of coordination in security measures, the heterogeneous components of a CPS will become vulnerable [3, 92].

In addition, with the above mentioned general challenges with the CPS security, we have briefed about the challenges with each of the four applications.

RETRACTED CHAPTER

8.7.2 Challenge in ICS

- **Change Management:** The components of ICS are diversely spanned geographically which are needed to be updated, repaired, removed, or replaced at some point. For example, a perfect planning is required to update any component of ICS, or else other components can experience unexpected failure. Once, in a nuclear plant, an unexpected failure occurred due to an update in the computer system [12]. Moreover, the large number of stakeholder can also cause unexpected failure unintentionally. Hence the coordinated change management is very crucial to managing the security-related changes in the system [92, 144].

- **Insider Threat:** The insiders of a system have the detailed knowledge about the components. They can attack the system intentionally or unintentionally exploiting the trust given to them. The Maroochy incident is an example of this. They can also help the remote attackers by giving them the access or confidential information. This kind of threat needs more serious considerations [75].
- **Secure Integration:** ICS is inherently vulnerable by the vulnerabilities of its legacy systems. Thus, the integration of the components with their legacy vulnerabilities must be done very securely so that they do not create any new vulnerabilities. However, since there are many components in an ICS it is practically infeasible to replace all of them at one time due to financial concerns [75], but, meanwhile, short-term security updates must be implemented to reduce the potential risks [12].

8.7.3 *Challenges in Smart Grids*

- **Two-Way Communication:** The advanced metering system allows the smart meters attached to the households to communicate to the utility companies directly which increases the physical attack. Unlike power grid, smart meters are physically accessible which is a threat to the utility companies also [69].
- **Access Control Mechanism:** As smart grid is widely spread, the mechanism for access control to the field devices must be considered strictly [3]. There must be proper control and mechanisms at every possible access point.
- **Privacy Concerns:** The communication traffic contains consumers' privileged information also. Besides the encryption of data, there must be an anonymization technique induced to prevent several types of attacks from deducing patterns of the encrypted information [72, 109]. A homomorphic encryption was proposed by Li et al. [86]. This mechanism protects the privacy of the consumers while the low overhead of the smart grids is also maintained. However, this encryption is not enough to prevent an attacker from injecting false data or impersonating a legitimate smart meter [156].
- **Explicit Trust:** There must be proper mechanisms and security measures to detect false data. Since the size of smart grid is large, it is very difficult to detect false data injection and unauthorized commands by the security measure which are designed to detect faults only [29, 88].
- **Comprehensive Security:** The security levels at the lower levels of smart grids, like field devices, are less compared to high-level components, such as control centers, due to the less capabilities of the smart grid. Because of the additional maintenance cost, the security solutions should be lightweight and cost-effective [71].
- **Change Management:** The management of changes in a smart grid is as challenging as ICS or even more as smart grids are more diverse and the number of its stakeholders are also more. Since the capabilities of change management are very limited in smart grids, it is intensely required to make the grids more secure [143].

RETRACTED CHAPTER

8.7.4 Challenges in Medical Devices

- **Usability vs. Security:** Too much security can be a serious problem for medical devices. For example, if a patient with critical health condition needs urgent care by IMD, but the IMD needs assistance from another person, who does not have the access privileges or the cryptographic credentials, the unavailability could be dangerous for the patient [53, 129]. So, it is required to focus on the usability along with security. The ideal solution would be allowing usability during emergencies while providing security as much as possible. Denning et al. [30] have proposed an optimal solution which uses fail-open/safety wristband. The patient wears a wristband which prevents any unauthorized person to interact with the IMDs, and when the patient removes the band, the IMD can be accessed by unauthorized persons.
- **Increased code for add-on security:** The limited power of the medical devices could be affected if addition functions are required due to additional codes of security. This may kill the original purpose of the device [131]. Hence, it is advisable that the medical devices should be focusing on their priority operation where the security measurements will be managed by some external device [48].
- **Limited Resources:** The power resources are critical for these small devices which require limited energy. The additional mechanism for security requires extra energy [53, 129]. The power of these devices must be maintained for several years. As one of the first efforts, Halperin et al. [52] proposed a security which has battery-free power consumption. It solely relies on RF as the energy source.

To drain the battery resources of these medical devices, attackers can flood the network with unnecessary commands which result in DoS attack [131]. Although if a medical device refuses to interact with unauthorized components, sending and receiving unnecessary commands will consume a certain amount of energy. Hence, new security controls must be developed to prevent the devices to respond to any illegitimate activity.

RETRACTED CHAPTER

8.7.5 Challenges in Smart Cars

- **Secure Integration:** In a smart car, the COTS and the third-party components are integrated by the manufacturer. Sometimes the integrated components mismatch due to lack of detailed information about the COTS and the third-party components. According to Sagstetter et al. [133], it is advisable that we should use the formal techniques, like a model-based design, where in every step the correctness of the information about the COTS and the third-party components are verified. Also, the measurements of access control need to be improved to prevent any unauthorized access to the components which are usually originated from the mismatch between the COTS and the third-party components [115].

- **Effective Separation:** The traffic of CAN network is separated into high and low frequencies by the gateway ECUs; however, many attacks were still able to bypass these gateways and attack various ECUs [73]. As a solution, some manufacturers deployed some techniques where the critical ECUs are in a totally separated network [155]. Another solution is to replace the simple ECUs with Master-ECUs [133], though it is very costly.
- **Heterogeneity of Components:** It is very normal that different components of a car cannot be manufactured by only car manufacturing companies. So, the distinct types of components are normally manufactured by Original Equipment Manufacturers (OEM). So, the accord among different parties must be maintained as the security measurements and capabilities are different for each component. Hence, security engineers who are familiar with early design phase must be incorporated by the manufacturers [70].
- **In-Car Communication:** Due to the assumption of isolation, CAN network is vulnerable inherently. Hence, there is a need for new protocols which assumes that there are potential attackers who can exploit these vulnerabilities. Therefore, a highly secure platform was proposed by the OVERSEE project [50] which will revolutionize the CAN network by replacing it. In addition, firewall and IDS kind of temporary solutions can be used as a part of the gateway ECU or even a separated ECU. Currently, there is a potential project going on state-full IDS which helps to detect the legitimacy of each packet sent to the vehicle during its different states as driving, parking, and much more [146].
- **New Vulnerabilities:** In the near future, there will be more challenges regarding the new security issues, V2V, and V2I communications as discussed in [119].

8.8 Conclusion

This chapter builds a good reference for those who need to get an overview of the recent studies and real-life issues of the CPS' security measures. We have discussed various possible threats to CPS according to different motives of the attacker. This helps to emphasize the awareness of the popularly used security measures of the CPS applications and can nurture great danger upon us. This chapter contains what are the common vulnerabilities in CPSs that can be exploited by the attackers and will allow the readers to learn about areas of the CPS that need more emphasis. For a better understanding of the exploitation of such vulnerabilities, we have presented several attacks that have taken place in the real world and succeeded. A taxonomy of these real-world attacks is also included for a quick study about successful attacks exploiting existing vulnerabilities. Some of the previous and current studies which are done on the security issues of CPS are covered in this chapter which will assist the readers having a desire to pursue further research in this field.

RETRACTED CHAPTER

References

1. Alcaraz C, Zeadally S (2013) Critical control system protection in the 21st century. Computer 46(10):74-83
2. Amin S, Litrico X, Sastry SS, Bayen AM (2010) Stealthy deception attacks on water scada systems. In: Proceedings of the 13th ACM international conference on hybrid systems: computation and control. ACM, New York, pp 161–170
3. Amin S, Schwartz GA, Hussain A (2013) In quest of benchmarking security risks to cyber-physical systems. IEEE Netw 27(1):19–24
4. Anderson R, Fuloria S (2010) Who controls the off switch? In: 2010 first IEEE international conference on smart grid communications (SmartGridComm). IEEE, Piscataway, pp 96–101
5. Bellovin, SM (1989) Security problems in the TCP/IP protocol suite. ACM SIGCOMM Comput Commun Rev 19(2):32–48
6. Briesemeister L, Cheung S, Lindqvist U, Valdes A (2010) Detection, correlation, and visualization of attacks against critical infrastructure systems. In: 2010 eighth annual international conference on privacy security and trust (PST). IEEE, Piscataway, pp 15–22
7. Brooks RR, Sander ST, Deng J, Taiber J (2008) Automotive system security: challenges and state-of-the-art. In: Proceedings of the 4th annual workshop on cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead (CSIIRW '08). ACM, New York, pp 26:1–26:3
8. Byres E, Lowe J (2004) The myths and facts behind cyber security risks for industrial control systems. In: Proceedings of the VDE Kongress, vol 116
9. Byres E, Franz M, Miller D (2004) The use of attack trees in assessing vulnerabilities in scada systems. In: Proceedings of the international infrastructure survivability workshop
10. Cao H, Zhu P, Lu X, Gurtov A (2013) A layered encryption mechanism for networked critical infrastructures. IEEE Netw 27(1):12–18
11. Càrdenas AA, Amin S, Sastry S (2008) Research challenges for the security of control systems. In: Proceedings of the 3rd conference on hot topics in security (HOTSEC)
12. Càrdenas A, Amin S, Sinopoli B, Giani A, Perrig A, Sastry S (2009) Challenges for securing CPSs. In: Workshop on future directions in cyber-physical systems security
13. Cardenas AA, Roosta T, Sastry S (2009) Rethinking security properties, threat models, and the design space in sensor networks: a case study in SCADA systems. Ad Hoc Netw 7(8): 1434–1447
14. Càrdenas AA, Amin S, Lin ZS, Huang YL, Huang CY, Sastry S (2011) Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM symposium on information, computer and communications security. ACM, New York, pp 355–366
15. Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, Koscher K, Czeskis A, Roesner F, Kohno T (2011) Comprehensive experimental analyses of automotive attack surfaces. In: USENIX security symposium
16. Cheminod M, Durante L, Valenzano A (2013) Review of security issues in industrial networks. IEEE Trans Ind Inf 9(1):277–293
17. Chen TM, Abu-Nimeh S (2011) Lessons from Stuxnet. Computer 44(4):91–93
18. Chen M, Gonzalez S, Vasilakos A, Cao H, Leung VC (2011) Body area networks: a survey. Mobile Netw Appl 16(2):171–193
19. Chen D, Kalra S, Irwin D, Shenoy P, Albrecht J (2015) Preventing occupancy detection from smart meters. IEEE Trans Smart Grid 6(5):2426–2434
20. Chien E, OMurchu L, Falliere N (2012) W32.duqu: the precursor to the next Stuxnet. In: Presented as part of the 5th USENIX workshop on large-scale exploits and emergent threats. USENIX, Berkeley
21. Cho S (2014) Privacy and authentication in smart grid networks. Doctoral dissertation, Ph. D. dissertation, Department of Computer Science, State University of New York, Incheon, South Korea

RETRACTED CHAPTER

22. Cho KT, Shin KG (2016) Error handling of in-vehicle networks makes them vulnerable. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, New York, pp 1044–1055
23. Choi D, Kim H, Won D, Kim S (2009) Advanced key-management architecture for secure SCADA communications. IEEE Trans Power Delivery 24(3):1154–1163
24. Chow R, Uzun E, Càrdenas AA, Song Z, Lee S (2011) Enhancing cyber physical security through data patterns. In: Workshop on foundations of dependable and secure cyber-physical systems (FDSCPS), p 25
25. Cleveland FM (2012) IEC 62351 security standards for the power system information infrastructure. http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf
26. CNN (2007) Sources: staged cyber-attack reveals vulnerability in power grid. http://www.cnn.com/2007/US/09/26/power.at.risk/
27. D'Amico A, Verderosa C, Horn C, Imhof T (2011) Integrating physical and cyber security resources to detect wireless threats to critical infrastructure. In: 2011 IEEE international conference on technologies for homeland security (HST), pp 494–500
28. Dardanelli A, Maggi F, Tanelli M, Zanero S, Savaresi SM, Kochanek R, Holz T (2013) A security layer for smartphone-to-vehicle communication over bluetooth. IEEE Embed Syst Lett 5(3):34–7
29. Das SK, Kant K, Zhang N (2012) Handbook on securing cyber-physical critical infrastructure. Elsevier, Amsterdam
30. Denning T, Kramer DB, Friedman B, Reynolds MR, Gill B, Kohno T (2014) CPS: beyond usability: applying value sensitive design based methods to investigate domain characteristics for security for implantable cardiac devices. In: Proceedings of the 30th annual computer security applications conference. ACM, New York, pp 426–435
31. East S, Butts J, Papa M, Shenoi S (2009) A taxonomy of attacks on the DNP3 protocol. In: Palmer C, Shenoi S (eds), Critical infrastructure protection III. IFIP advances in information and communication technology, vol 311. Springer, Berlin, pp 67–81
32. Ericsson, GN (2010) Cyber security and power system communication 2014; essential parts of a smart grid infrastructure. IEEE Trans Power Delivery 25(3):1501–1507
33. Escherich R, Ledendecker I, Schmal C, Kuhls B, Grothe C, Scharberth F (2009) SHE: secure hardware extension-functional specification, version 1.1. Hersteller Initiative Software (HIS) AK Security
34. Fang X, Misra X, Xue G, Yang D (2012) Smart gridthe new and improved power grid: a survey. IEEE Commun Surv Tutorials 14(4):944–980
35. Fernandez JD, Fernandez AE (2005) SCADA systems: vulnerabilities and remediation. J Comput Sci Coll 20(4):160–168
36. Fleury T, Khurana H, Welch V (2008) Towards a taxonomy of attacks against energy control systems. In: Papa M, Shenoi S (eds) Critical infrastructure protection II. The international federation for information processing, vol 290. Springer, New York, pp 71–85
37. Food and Drug Administration (FDA) (2005) Cybersecurity for networked medical devices containing off-the-shelf (OTS) software. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf
38. Food and Drug Administration (FDA) (2014) Cybersecurity for networked medical devices containing off- the-shelf (OTS) software. www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
39. Fovino IN, Carcano A, Masera M, Trombetta A (2009) An experimental investigation of malware attacks on SCADA systems. Int J Crit Infrastruct Prot 2(4):139–145
40. Fovino IN, Carcano A, Masera M, Trombetta A (2009) Design and implementation of a secure Modbus protocol. In: Critical infrastructure protection III. Springer, Berlin, pp 83–96
41. FOX News Network (2014) Threat to the grid? Details emerge of sniper attack on power station. http://www.foxnews.com/politics/2014/02/06/2013-sniper-attack-on-power-grid-still-concern-in-washington-andfor-utilities/

RETRACTED CHAPTER

42. Francia G III, Thornton D, Brookshire T (2012) Wireless vulnerability of SCADA systems. In: Smith RK, Vrbsky SV (eds), ACM southeast regional conference. ACM, New York, pp 331–332
43. Francia III G, Thornton D, Brookshire T (2012) Wireless vulnerability of SCADA systems. In: Proceedings of the 50th annual southeast regional conference, 2012 Mar 29. ACM, New York, pp 331–332
44. Francia III GA, Thornton D, Dawson J (2012) Security best practices and risk assessment of SCADA and industrial control systems. In: Proceedings of the international conference on security and management (SAM), 2012 Jan 1. The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), Las Vegas, p 1
45. Francillon A, Danev B, Capkun S (2011) Relay attacks on passive keyless entry and start systems in modern cars. In: Proceedings of the network and distributed system security symposium (NDSS)
46. Fu K, Blum J (2013) Controlling for cybersecurity risks of medical device software. Commun ACM 56(10):35–37
47. Garcia FD, Oswald D, Kasper T, Pavlid'es P (2016) Lock it and still lose it–on the (in) security of automotive remote keyless entry systems. In: 25th USENIX security symposium (USENIX Security 16)
48. Gollakota S, Hassanieh H, Ransford B, Katabi D, Fu K (2011) They can hear your heartbeats: non-invasive security for implantable medical devices. SIGCOMM Comput Commun Rev 41(4):2–13
49. Gollmann D (2013) Security for cyber-physical systems. In: Mathematical and engineering methods in computer science. Springer, Berlin, pp 12–14
50. Groll A, Holle J, Ruland C, Wolf M, Wollinger T, Zweers F (2009) Oversee a secure and open communication and runtime platform for innovative automotive applications. In: 7th embedded security in cars conference (ESCAR)
51. Guan L, Xu J, Wang S, Xing X, Lin L, Huang H, Liu P, Lee W (2016) From physical to cyber: escalating protection for personalized auto insurance. In: Proceedings of the 14th ACM conference on embedded network sensor systems CD-ROM (SenSys '16). ACM, New York, pp 42–55
52. Halperin D, Clark SS, Fu K, Heydt-Benjamin TS, Defend B, Kohno T, Ransford B, Morgan W, Maisel WH (2008) Pacemakers and implantable cardiac defibrillators: software radio attacks and zeropower defenses. In: IEEE symposium on security and privacy (SP 2008), pp 129–142
53. Halperin D, Heydt-Benjamin TS, Fu K, Kohno T, Maisel WH (2008) Security and privacy for implantable medical devices. IEEE Pervasive Comput 7(1):30–39
54. Hanna S, Rolles R, Molina-Markham A, Poosankam P, Fu K, Song D (2011) Take two software updates and see me in the morning: the case for software security evaluations of medical devices. In: Proceedings of the 2nd USENIX conference on health security and privacy, health (SEC '11). USENIX Association, Berkeley, p 6
55. Harris S (2008) China's cyber militia. National Journal Magazine, 31 May
56. Harris B, Hunt R (1999) TCP/IP security threats and attack methods. Comput Commun 22(10):885–897
57. Hayajneh T, Mohd BJ, Imran M, Almashaqbeh G, Vasilakos AV (2016) Secure authentication for remote patient monitoring with wireless medical sensor networks. Sensors 16(4):424
58. Hieb JL (2008) Security hardened remote terminal units for SCADA networks. University of Louisville, Louisville
59. Hoglund G, McGraw G (2004) Exploiting software: how to break code. Pearson Education India, New Delhi
60. Hoppe T, Kiltz S, Dittmann J (2011) Security threats to automotive can networks — practical examples and selected short-term countermeasures. In: Proceedings of the 27th international conference on computer safety, reliability, and security (SAFECOMP '08). Springer, Berlin, pp 235–248

RETRACTED CHAPTER

61. Huitsing P, Chandia R, Papa M, Shenoi S (2008) Attack taxonomies for the modbus protocols. Int J Crit Infrastruct Prot 1:37–44
62. ICS-CERT (2010) Common cybersecurity vulnerabilities in industrial control systems. http://ics-cert.us-cert.gov/sites/default/files/recommendedpractices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf
63. IEEE 802.16 Working Group et al (2004) IEEE standard for local and metropolitan area networks. part 16: air interface for fixed broadband wireless access systems. IEEE Std 802: 16–2004
64. Investment Watch (2014) First time in history, a terrorist attack on the electric power grid has blacked-out an entire nation in this case Yemen. http://investmentwatchblog.com/first-time-in-history-a-terrorist-attack-onthe-electric-power-grid-has-blacked-out-an-entire-nation-in-thiscase-yemen
65. Jin X, Bigham J, Rodaway J, Gamez D, Phillips C (2006) Anomaly detection in electricity cyber infrastructures. In: Proceedings of the international workshop on complex networks and infrastructure protection (CNIP '06)
66. Jo, HJ, Choi W, Na SY, Woo S, Lee DH (2016) Vulnerabilities of android OS-based telematics system. Wirel Pers Commun 92(4):1511–1530
67. Johnson RE (2010) Survey of SCADA security challenges and potential attack vectors. In: 2010 international conference for internet technology and secured transactions (ICITST). IEEE, Piscataway, pp 1–5
68. Karygiannis T, Owens L (2002) Wireless network security. NIST special publication, 800:48
69. Khurana H, Hadley M, Lu N, Frincke DA (2010) Smart-grid security issues. IEEE Secur Priv 8(1):81–85
70. Kleidermacher D, Kleidermacher M (2012) Embedded systems security: practical methods for safe and secure software and systems development. Elsevier, Amsterdam
71. Knapp ED, Samani R (2013) Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure, Newnes
72. Komninos N, Philippou E, Pitsillides A (2014) Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tutorials 16(4):1933–1954
73. Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S (2010) Experimental security analysis of a modern automobile. In: 2010 IEEE symposium on security and privacy (SP), pp 447–462
74. Krishnamurti T et al (2012) Preparing for smart grid technologies: a behavioral decision research approach to understanding consumer expectations about smart meters. Energy Policy 41:790–797
75. Krotofil M, Gollmann D (2013) Industrial control systems security: what is happening? In: 2013 11th IEEE international conference on industrial informatics (INDIN). IEEE, Piscataway, pp 670–675
76. Krotofil M, Larsen J, Gollmann D (2015) The process matters: ensuring data veracity in cyber-physical systems. In: Proceedings of the 10th ACM symposium on information, computer and communications security (ASIA CCS '15). ACM, New York, pp 133–144
77. Langner R (2011) Stuxnet: dissecting a cyberwarfare weapon. Secur Priv IEEE 9(3):49–51
78. Larson UE, Nilsson DK (2008) Securing vehicles against cyber-attacks. In: Proceedings of the 4th annual workshop on cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead (CSIIRW '08). ACM, New York, pp 30:1–30:3
79. Larson UE, Nilsson DK, Jonsson E (2008) An approach to specification-based attack detection for in-vehicle networks. In: 2008 IEEE intelligent vehicles symposium. IEEE, Piscataway, pp 220–225
80. Lee EA (2008) CPSs: design challenges. In: 2008 11th IEEE international symposium on object oriented real-time distributed computing (ISORC). IEEE, Piscataway
81. Lee EA, Seshia SA (2011) Introduction to embedded systems: a cyber-physical systems approach. University of California, Berkeley

RETRACTED CHAPTER

82. Lee I, Sokolsky O, Chen S, Hatcliff J, Jee E, Kim B, King A, Mullen-Fortino M, Park S, Roederer A et al (2012) Challenges and research directions in medical cyber–physical systems. Proc IEEE 100(1):75–90
83. Lee H, Choi K, Chung K, Kim J, Yim K (2015) Fuzzing can packets into automobiles. In: 2015 IEEE 29th international conference on advanced information networking and applications. IEEE, Piscataway, pp 817–821
84. Leverett EP (2011) Quantitatively assessing and visualising industrial system attack surfaces. University of Cambridge, Darwin College
85. Leverett E, Wightman R (2013) Vulnerability inheritance in programmable logic controllers. https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
86. Li F, Luo B, Liu P (2010) Secure information aggregation for smart grids using homomorphic encryption. In: 2010 first IEEE international conference on smart grid communications (SmartGridComm). IEEE, Piscataway, pp 327–332
87. Li C, Raghunathan A, Jha NK (2011) Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system. In: 2011 13th IEEE international conference on e-health networking applications and services (Healthcom), pp 150–156
88. Liu Y, Ning P, Reiter MK (2011) False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur 14(1):13
89. Liu T, Sun Y, Liu Y, Gui Y, Zhao Y, Wang D, Shen C (2015) Abnormal traffic-indexed state estimation: a cyber-physical fusion approach for smart grid attack detection. Futur Gener Comput Syst 49:94–103
90. Lu Z, Lu X, Wang W, Wang C (2010) Review and evaluation of security threats on the communication networks in the smart grid. In: Military communications conference (MILCOM' 10). IEEE, Piscataway, pp 1830–1835
91. Lu Z, Wang W, Wang C (2011) From jammer to gambler: modeling and detection of jamming attacks against time-critical traffic. In: Proceedings IEEE INFOCOM. IEEE, Piscataway, pp 1871–1879
92. Luallen, ME (2011) Critical control system vulnerabilities demonstrated - and what to do about them. A SANS Whitepaper
93. MacDonald D, Clements SL, Patrick SW, Perkins C, Muller G, Lancaster MJ, Hutton W (2013) Cyber/physical security vulnerability assessment integration. In: 2013 IEEE PES innovative smart grid technologies (ISGT). IEEE, Piscataway, pp 1–6
94. Majdalawieh M, Parisi-Presicce F, Wijesekera D (2006) DNPSEC: distributed network protocol version 3 (DNP3) security ramework. In: Advances in computer, information, and systems sciences, and engineering. Springer, Berlin, pp 227–234
95. Markey E (2015) Tracking and hacking: security and privacy gaps put American drivers at risk. http://www.markey.senate.gov/imo/media/doc/2015-02-06MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf
96. Mashima D, Càrdenas AA (2012) Evaluating electricity theft detectors in smart grid networks. In: Proceedings of the 15th international conference on research in attacks, intrusions, and defenses (RAID'12). Springer, Berlin, pp 210–229
97. McDaniel P, McLaughlin S (2009) Security and privacy challenges in the smart grid. Secur Priv IEEE 7(3):75–77
98. Metke AR, Ekl RL (2010) Security technology for smart grid networks. IEEE Trans Smart Grid 1(1):99–107
99. Microsoft Security Tech Center (2008) Microsoft security bulletin ms08-067 - critical. https://technet.microsoft.com/library/security/ms08-067
100. Microsoft Security TechCenter (2010) Microsoft security bulletin summary for September 2010. https://technet.microsoft.com/library/security/ms10-sep
101. Miller B, Rowe D (2012) A survey scada of and critical infrastructure incidents. In: Proceedings of the 1st annual conference on research in information technology. ACM, New York, pp 51–56
102. Miller C, Valasek C (2013) Adventures in automotive networks and control units. A SANS whitepaper

RETRACTED CHAPTER

103. Mitchell R, Chen IR (2011) Survivability analysis of mobile CPSs with voting-based intrusion detection. In: 2011 7th international wireless communications and mobile computing conference (IWCMC), pp 2256–2261
104. Mitchell R, Chen R (2012) Behavior rule based intrusion detection for supporting secure medical CPSs. In: 2012 21st international conference on computer communications and networks (ICCCN). IEEE, Piscataway, pp 1–7
105. Mitchell R, Chen R (2013) Behavior-rule based intrusion detection systems for safety critical smart grid applications. IEEE Trans Smart Grid 4(3):1254–1263
106. Mitchell R, Chen IR (2013) Effect of intrusion detection and response on reliability of CPSs. IEEE Trans Reliab 62(1):199–210
107. Mitchell R, Chen IR (2014) A survey of intrusion detection techniques for cyber-physical systems. ACM Comput Surv 46(4):55
108. Mo Y, Kim THJ, Brancik K, Dickinson D, Lee H, Perrig A, Sinopoli B (2012) Cyber-physical security of a smart grid infrastructure. Proc IEEE 100(1):195–209
109. Molina-Markham A, Shenoy P, Fu K, Cecchet E, Irwin D (2010) Private memoirs of a smart meter. In: Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building. ACM, New York, pp 61–66
110. Munro K (2012) Deconstructing flame: the limitations of traditional defences. Comput Fraud Secur 2012(10):8–11
111. Falliere N, Murchu LO, Chien E (2011) W32. stuxnet dossier. White Paper (Symantec Corporation, Security Response) 5(6):29
112. Nakashima E, Mufson S (2008) Hackers have attacked foreign utilities, CIA analyst says. Washington Post, 19 January
113. Neuman C (2009) Challenges in security for cyber-physical systems. In: DHS workshop on future directions in cyber-physical systems security, Citeseer
114. Nicholson A, Webber S, Dyer S, Patel T, Janicke H (2012) SCADA security in the light of cyber-warfare. Comput Secur 31(4):418–436
115. Nilsson DK, Phung PH, Larson UE (2008) Vehicle ECU classification based on safety-security characteristics. In: Road transport information and control-RTIC 2008 and ITS United Kingdom members' conference. IET, Stevenage, pp 1–7
116. NIST (2010) NISTIR. 7628: guidelines for smart grid cyber security. Technical report
117. Oberoi D, Sou WY, Lui YY, Fisher R, Dinca L, Hancke GP (2016) Wearable security: key derivation for body area sensor networks based on host movement. In: 2016 IEEE 25th international symposium on industrial electronics (ISIE). IEEE, Piscataway, pp 1116–1121
118. Paukatong T (2005) SCADA security: a new concerning issue of an inhouse egat-scada. In: Transmission and distribution conference and exhibition: Asia and pacific, IEEE/PES, pp 1–5
119. Petit J, Shladover SE (2015) Potential cyberattacks on automated vehicles. IEEE Trans Intell Transp Syst 16(2):546–556
120. Pfleeger CP, Pfleeger SL (2006) Security in computing, 4th edn. Prentice Hall PTR, Upper Saddle River
121. Piètre-Cambacèdès L, Tritschler M, Ericsson GN (2011) Cybersecurity myths on power control systems: 21 misconceptions and false beliefs. IEEE Trans Power Delivery 26(1): 161–172
122. Bauman K, Tuzhilin A, Zaczynski R (2017) Using social sensors for detecting emergency events: a case of power outages in the electrical utility industry. ACM Trans Manag Inf Syst (TMIS) 8(2–3):7
123. Quinn, EL (2009) Privacy and the new energy infrastructure. SSRN 1370731
124. Rad AHM, Leon-Garcia A (2011) Distributed internet-based load altering attacks against smart power grids. IEEE Trans Smart Grid 2(4):667–674
125. Radcliffe J (2011) Hacking medical devices for fun and insulin: breaking the human scada system. In: Black Hat Conference presentation slides, vol 2011
126. Barbosa RR (2014) Anomaly detection in SCADA systems: a network based approach
127. Rahman MA, Bera P, Al-Shaer E (2012) Smartanalyzer: a noninvasive security threat analyzer for AMI smart grid. In: Proceedings IEEE INFOCOM, pp 2255–2263

RETRACTED CHAPTER

128. Rajkumar RR et al (2010) Cyber-physical systems: the next computing revolution. In: Proceedings of the 47th design automation conference. ACM, New York
129. Rostami M, Burleson W, Koushanfar F, Juels A (2013) Balancing security and utility in medical devices? In: Proceedings of the 50th annual design automation conference. ACM, New York, p 13
130. Roufa RMI, Mustafaa H, Taylora SOT, Xua W, Gruteserb M, Trappeb W, Seskarb I (2010) Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. In: 19th USENIX security symposium, Washington, pp 11–13
131. Rushanan M, Rubin AD, Kune DF, Swanson CM (2014) SoK: security and privacy in implantable medical devices and body area networks. In: IEEE symposium on security and privacy
132. Ryu DH, Kim HJ, Um K (2009) Reducing security vulnerabilities for critical infrastructure. J Loss Prev Process Ind 22(6):1020–1024. Papers presented at the 2007 and 2008 international symposium of the Mary Kay O'Connor process safety center and papers presented at the fWCOGIg 2007
133. Sagstetter F, Lukasiewycz M, Steinhorst S, Wolf M, Bouard A, Harris WR, Jha S, Peyrin T, Poschmann A, Chakraborty S (2013) Security challenges in automotive hardware/software architecture design. In: Proceedings of the conference on design, automation and test in Europe, EDA Consortium, San Jose, pp 458–463
134. Salmon D et al (2009) Mitigating the aurora vulnerability with existing technology. In: Proceedings of the 36th annual western protective relay conference
135. Santamarta R (2012) Here be backdoors: a journey into the secrets of industrial firmware. https://media.blackhat.com/bh-us-12/Briefings/Santamarta/BH_US_12_Santamarta_Backdoors_WP.pdf
136. Seepers RM, Weber JH, Erkin Z, Sourdis I, Strydis C (2016) Secure key-exchange protocol for implants using heartbeats. In: Proceedings of the ACM international conference on computing frontiers. ACM, New York, pp 119–126
137. Seifert S, Obermaisser R (2014) Secure automotive gateway– secure communication for future cars. In: 12th IEEE international conference on industrial informatics (INDIN). IEEE, Piscataway, pp 213–220
138. Miciolino EE, Bernieri G, Pascucci F, Setola R (2015) Communications network analysis in a SCADA system testbed under cyber-attacks. In: Telecommunications Forum Telfor (TELFOR), 2015 23rd-2015 Nov 24. IEEE, New York, pp 341–344
139. Shoukry Y, Martin P, Tabuada P, Srivastava M (2013) Non-invasive spoofing attacks for anti-lock braking systems. In: Cryptographic hardware and embedded systems-CHES 2013. Springer, Berlin, pp 55–72
140. Shoukry Y, Martin P, Yona Y, Diggavi S, Srivastava M (2015) PYCRA: physical challenge-response authentication for active sensors under spoofing attacks. In: Proceedings of the 22nd ACM SIGSAC conference on computer and communications security. ACM, New York, pp 1004–1015
141. Slay J, Miller M (2007) Lessons learned from the maroochy water breach. In: Critical infrastructure protection, pp 73–82
142. Sommestad T, Ericsson GN, Nordlander J (2010) SCADA system cyber security—a comparison of standards. In: 2010 IEEE power and energy society general meeting. IEEE, Piscataway, pp 1–8
143. Sridhar S, Hahn A, Govindarasu M (2012) Cyber– physical system security for the electric power grid. Proc IEEE 100(1):210–224
144. Stouffer KA, Falco JA, Scarfone KA (2011) SP 800-82. Guide to industrial control systems (ICS) security: supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC). Technical report, Gaithersburg
145. Studnia I, Nicomette V, Alata E, Deswarte Y, Kaˆaniche M, Laarouchi Y (2013) Survey on security threats and protection mechanisms in embedded automotive networks. In: 43rd annual IEEE/IFIP conference on dependable systems and networks workshop (DSN-W). IEEE, Piscataway, pp 1–12

RETRACTED CHAPTER

146. Studnia I, Nicomette V, Alata E, Deswarte Y, Kaaniche M, Laarouchi Y (2013) Security of embedded automotive networks: state of the art and a research proposal. In: SAFECOMP 2013-workshop CARS (2nd workshop on critical automotive applications: robustness & safety) of the 32nd international conference on computer safety, reliability and security
147. Symantec Security Response (2014) Dragonfly: western energy companies under sabotage threat. http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat
148. Taylor A, Japkowicz N, Leblanc S (2015) Frequency based anomaly detection for the automotive can bus. In: 2015 world congress on industrial control systems security (WCICSS). IEEE, Piscataway, pp 45–49
149. Tsang R (2010) Cyberthreats, vulnerabilities and attacks on scada networks. University of California, Berkeley
150. Turk RJ (2005) Cyber incidents involving control systems. Idaho National Laboratory (INL), Idaho Falls
151. Urias V, Leeuwen BV, Richardson B (2012) Supervisory command and data acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed. In: Military communications conference, 2012 - MILCOM, pp 1–8
152. US-CERT (2009) Cyber threat source descriptions. https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
153. Vaas L (2013) Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking. https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/
154. Vaidya B, Makrakis D, Mouftah HT (2013) Authentication and authorization mechanisms for substation automation in smart grid network. IEEE Netw 27(1):5–11
155. Valasek C, Miller C (2014) A survey of remote automotive attack surfaces. Black Hat USA 2014
156. Wang W, Lu Z (2013) Cyber security in the smart grid: survey and challenges. Comput Netw 57(5):1344–1371
157. Welch D, Lathrop S (2003) Wireless security threat taxonomy. In: IEEE systems, man and cybernetics society information assurance workshop. IEEE, Piscataway, pp 76–83
158. Wetzels J (2014) Broken keys to the kingdom: security and privacy aspects of rfid-based car keys. Preprint arXiv:1405.7424
159. Wolf M, Gendrullis T (2012) Design, implementation, and evaluation of a vehicular hardware security module. In: Information security and cryptology-ICISC 2011. Springer, Berlin, pp 302–318
160. Wolf M, Weimerskirch A, Paar C (2004) Security in automotive bus systems. In Proceedings of the workshop on embedded security in cars (ESCAR'04)
161. Woo S, Jo HJ, Lee DH (2015) A practical wireless attack on the connected car and security protocol for in-vehicle can. IEEE Trans Intell Transp Syst 16(2):993–1006
162. Xie L, Mo Y, Sinopoli B (2010) False data injection attacks in electricity markets. In: 2010 first IEEE international conference on smart grid communications (SmartGridComm). IEEE, Piscataway, pp 226–231
163. Xu F, Qin Z, Tan CC, Wang B, Li Q (2011) Imdguard: securing implantable medical devices with the external wearable guardian. In: Proceedings IEEE INFOCOM, pp 1862–1870
164. Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y, Sztipanovits J (2013) Taxonomy for description of cross-domain attacks on CPS. In: Proceedings of the 2nd ACM international conference on high confidence networked systems. ACM, New York, pp 135–142
165. Zeller M (2011) Myth or reality? Does the aurora vulnerability pose a risk to my generator? In: 2011 64th annual conference for protective relay engineers. IEEE, Piscataway, pp 130–136
166. Zheng G, Fang G, Shankaran R, Orgun MA (2015) Encryption for implantable medical devices using modified one-time pads. IEEE Access 3:825–836

RETRACTED CHAPTER

167. Zhu B, Sastry S (2010) Scada-specific intrusion detection/prevention systems: a survey and taxonomy. In: Proceedings of the 1st workshop on secure control systems (SCS)

168. Zhu B, Joseph A, Sastry S (2011) A taxonomy of cyber-attacks on scada systems. In: Proceedings of the 2011 international conference on internet of things and 4th international conference on cyber, physical and social computing (ITHINGSCPSCOM '11). IEEE Computer Society, Washington, pp 380–388

RETRACTED CHAPTER