EXAMPLE CHAPTER – Contributed chapter

Chapter 5: Security Methods for Critical Infrastructure Communications

Author(s):
*T. J. Bihl (Wright State University, United States, Trevor.Bihl@wright.edu)
A. F. Zobaa (Brunel University London, United Kingdom, email: azobaa@ieee.org)

5.1 Introduction

Critical infrastructure (CI) includes any systems and assets that are so vital that their destruction or disruption threatens lives, governments, economies, ecologies, or the social/political structure of nations (Moteff & Parfomak, 2004) (Luiijf & Klaver, 2004). Thus, CI includes, but is not limited to, power grids, water and sewage, hospitals, and transportation systems (Luiijf & Klaver, 2004). To enable monitoring and control of CI systems, industrial control networks are often used (Galloway & Hancke, 2013). Industrial control networks, conceptualized in Figure 5.1, are systems that monitor and control physical devices. Conservatively, eighty percent of US electric power utilities employ industrial control networks for monitoring and control (Fernandez & Fernandez, 2005). Of interest in industrial control networks is preventing unauthorized access to CI systems and overall reliability of the networks.

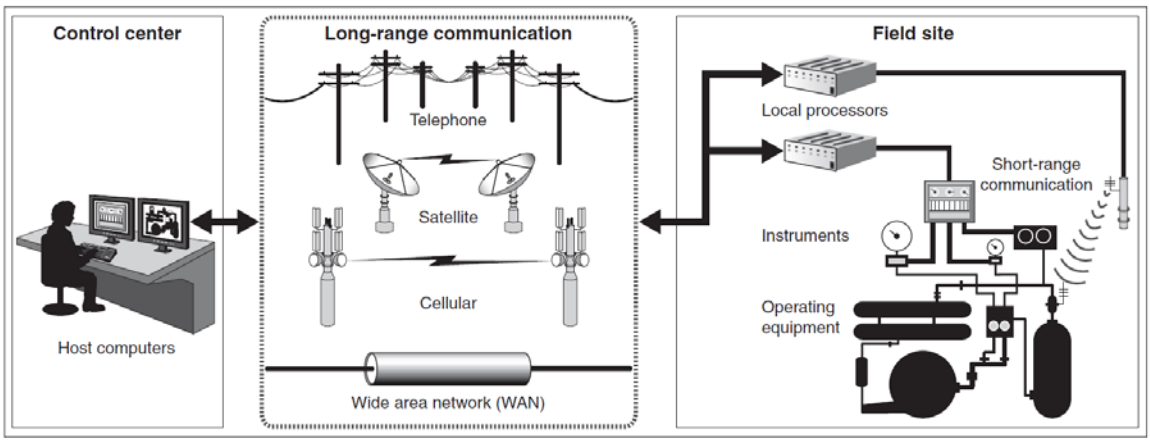

Figure 5.1: Conceptualization of an Industrial Control Network (from (Goverment Accountability Office (GAO), 2008))

Increasingly, commercial network technologies are being used in industrial control networks; this increases internet pathways and cyber security risks. In many ways, extending the Internet

of Things (IoT) to include CI components can be seen as logical since IoT enabled devices can be used to monitor all components in a system, e.g. wireless enabled structural health monitoring of bridges (Hu, Wang, & Ji, 2013). However, to be useful, communication networks used for CI need to balance performance, security, reliability, availability, and survivability (Snow, Varshney, & Malloy, 2000) (Ellison, Fisher, Linger, Lipson, & Longstaff, 1997). Thus, beyond introducing vulnerabilities, security concerns can both limit user confidence in communications networks (Liao, Luo, Gurung, & Shi, 2015) and reduce their functionality (McMaster, 2003).

Communication security is only as strong as the weakest link, e.g. one insecure device in a large and otherwise security network can compromise the entire network (Yang, Luo, Ye, Lu, & Zhang, 2004). To secure networks, monitoring for anomalous behavior and vetting the identify of devices that aim to gain access to the network is critical. With the IoT expanding the volume and variety of devices connected to CI networks, the proliferation of communication devices and standards in CI applications thus presents security challenges. To understand how to vet the identity of communication devices, this chapter first reviews communications operations, then the types of devices used in industrial communication networks, the various threats to networks, and then the various security measures available.

5.2 Effects of Successful Communication System Threats

A variety of possible outcomes exists for successful CI communication system incidents. To this end, risk analysis of the various threats can be conducted concerning a communication system and the possible consequences if the threat occurs (Peltier, 2005). To evaluate what risks should be mitigated, security analysis can consider the likelihood of successful attack (L_{AS}) as a function of the threat (T), vulnerabilities (V), and target attractiveness (A_T) (Byres & Lowe, 2004). In conjunction with L_{AS}, of interest is also the consequence (C) of an attack (Byres & Lowe, 2004). While each communication system has various specific threats and

possible consequences, the consequences can be generally binned as follows, where a malicious party could (Miller & Rowe, 2012): *distort* or modify files and information, *disrupt* access to the network, *disclose* information, *destroy* files or systems, or cause the *death* of humans. Additionally, some effects are *unknown* incidents, where the results and goals were not be discovered by investigators (Miller & Rowe, 2012). With effective security analysis, the estimated financial, environmental and health consequences of attacks can be estimated and used to allocate security resources (Byres & Lowe, 2004).

5.3 General Communication System Operations

In operation, industrial control networks are used for communication, monitoring and controlling of devices and processes. For instance, instruments and operating equipment can record their states and transmit this as a message over the network. Similarly, an operator monitoring the equipment could send a message to change a state, e.g. opening a valve. However, to function, industrial control networks need a software and protocol framework to enable communications and routing of messages.

In general, to communicate over any network, first a software application (such as an operator clicking on a symbol for a valve he wishes to open) initiates the transmission of a data packet, which is the data or commands that are to be transmitted (Frenzel, 2013) (Couch, 1993). This process is conceptualized in Figure 5.2 where the layers are conceptualized as the layers of the Open Systems Interconnection (OSI) model; consistent with (Frenzel, 2013) (Couch, 1993). Table 6.1 provides general descriptions of each OSI layer. In general, all layers are software-related and indicate how data is handled; the exception is the physical layer which involves the physical components to transmit/receive data.

In Figure 5.2, as the packet proceeds through layers of software and hardware, more information is added to format the message, in the form of headers, addresses and etc. (Frenzel,

2013) (Couch, 1993). These are added to describe the properties of devices, bit-level identification characteristics, communication properties, details for appropriate packet data handling, and etc. (Frenzel, 2013) (Couch, 1993). Once addresses, headers and other details are added as data is conceptually passed through the OSI layers, the final message is is transmitted over the communication medium (wired or wireless). Another device then receives the signal and the process is reversed to remove addresses and headers whereby it is determined how to handle and process the received data (Frenzel, 2013) (Couch, 1993).

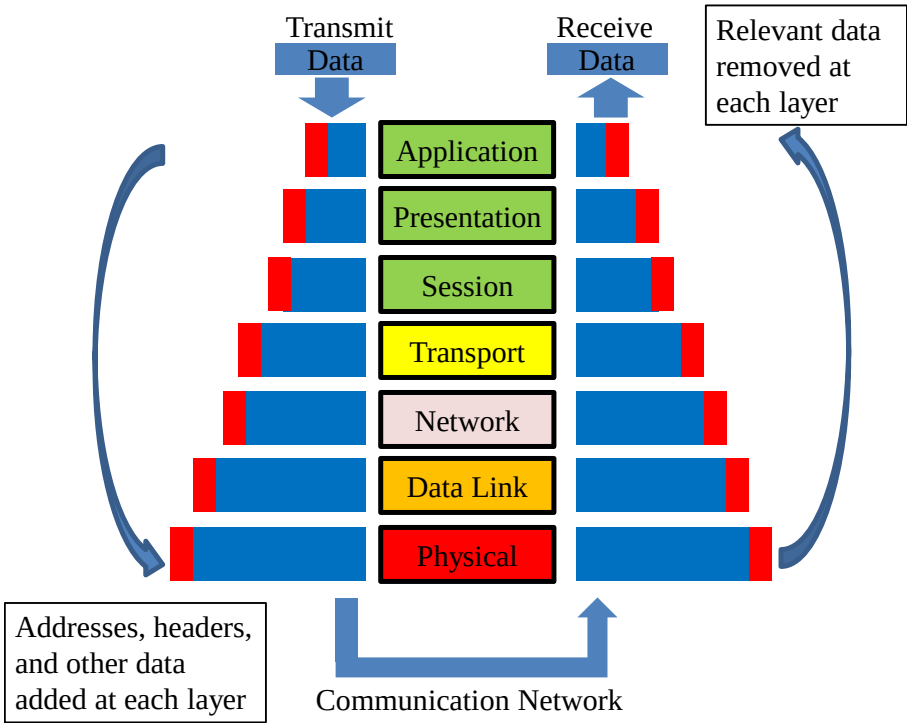

Figure 5.2: General digital communication operation. (From (Bihl T. J., 2015))

Table 6.1: Communication Layers per the OSI Stack with Descriptions and Examples

	Data	Layer	Description	Example
Host Layers	Data	Application	Software to access network	End User
		Presentation	Applies formatting to data, encrypts data, facilitates application layer interaction.	Syntax, data manipulation
		Session	Interhost connections, session establishment	Synching
	Segments	Transport	Connection protocols	TCP, host-to-host
Media Layers	Packets	Network	Determines physical path for data routing	Packets, routing
	Frames	Data Link	Transfer of signal between nodes via physical devices	Frames, MAC Addresses
	Bits	Physical	Signals, transmission, communication, and reception over a medium; physical components/devices	Cables, devices, physical mediums, transmission methods

5.4 Industrial Control Networks and Operations

Industrial control networks operate by linking devices to operators via an infrastructure (wired, wireless, or a combination) (US Government Accountability Office, 2004) (Slay & Miller, 2007). Human machine interfaces (HMI) feature prominently in industrial control networks and enable the presentation of interactive animations of devices and sensors, graphics of systems, and schematic diagrams to operators (Higgs, 2000) (Gomez Gomez, 2005). Oversight and management for data acquisition in industrial control networks are provided by software layers including Distributed Control Systems (DCSs), Supervisory Control And Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Cyber-Physical Systems (CPS) (Galloway & Hancke, 2013) (Cárdenas, Amin, & Sastry, 2008). Appropriate and effective design of SCADA and DCS is key since industrial control networks are connected to physical equipment, they differ from commercial networks, e.g. wifi and internet, by having high reliability requirements and the necessity of very short communication times but in small packets (Galloway & Hancke, 2013).

5.4.1 Industrial Control Network Operations and Components

Broadly, the structure in an industrial control network has four layers, as seen in Figure 5.1 and described in Table 5.2: processes and field equipment, devices, the station/substation of interest and the enterprise (Slay & Miller, 2007) (Schneider Electric, 2012) (Dolezilek & Schweitzer, 2000). Processes include the industrial system itself and field equipment, such as sensors, instrumentation, and actuators (Schneider Electric, 2012). Devices include both Remote Telemetry Units (RTUs) and Programmable Logic Controllers (PLCs) (Galloway & Hancke, 2013) (Kang & Robles, 2009). PLCs serve to control processes, perform digital and analog input/output, and provide control logic (Galloway & Hancke, 2013) and RTUs serve as sensor data collection devices (Slay & Miller, 2007) (Galloway & Hancke, 2013). Due to ongoing developments in controllers, the function of RTUs and PLCs is frequently performed by an RTU/PLC device that can serve both functions as needed (Schneider Electric, 2012). The enterprise level includes the end user (Dolezilek & Schweitzer, 2000).

Table 5.2: Integration and Control (I&C) System Levels, per (Dolezilek & Schweitzer, 2000)

Level	**Description**	**Example**
Enterprise	Highest level, includes all end users who are inside or outside the substation.	Workstation at the corporate office.
Station/Substation	3rd level, performs data acquisition and local input/output for the entire station.	Human machine interfaces, controller software, and decision support systems running on a local PC.
Device	2nd level, contains PLCs and RTUs that collect and react to data.	Protective relays, meters, fault recorders, load tap changers, VAR controllers, RTUs, PLCs
Process	Lowest level, connected to physical components for monitoring control.	Current transformers, Voltage Transformers, Resistance thermal detectors, Transducers

Bridging the gap between the station and enterprise level are the communication network and medium, host software, and the communication medium itself, as well as the protocols used to transmit data from RTUs and PLCs over the network (Galloway & Hancke, 2013). Finally, the host software layer includes software components, such as SCADA, whereby information is routed and presented effectively between clients, servers and the field devices (Queiroz,

Mahmood, Hu, Tari, & Yu, 2009) (Galloway & Hancke, 2013). The client components refer to the end users, or operators, who monitor the system and the human-machine interface components (Daneels & Salter, 1999). Additional components can include firewalls and intrusion detection systems to protect the network from unauthorized access.

In practice, different RTU and PLC devices can be in use in a single installation and operate using different protocols; the languages used to exchange information (Schneider Electric, 2012) (Daneels & Salter, 1999). Varying ages of devices in use exist in industrial control networks because outdated yet useful devices are rarely discarded while they continue to function correctly (Dolezilek & Schweitzer, 2000). Thus, one network could possibly contain many devices from many different manufacturers, and thus a variety of protocols can be found in use in any given industrial control network and stations. Additionally, proprietary versions of protocols can exist, making integration a further challenge (Schneider Electric, 2012); however, digital forensics investigations can aid in understanding proprietary protocol operations (Badenhop, Ramsey, Mullins, & Mailloux, 2016). Before being able to transmit over a network, one must understand and integrate effectively with the protocol. If proprietary protocols are used, this may require an operator to agree to a non-disclosure agreement (Badenhop, Ramsey, Mullins, & Mailloux, 2016), or to simply rely on the protocol to operate effectively. To facilitate communication, servers that aggregate information at the station-level for communication over the network can generally handle multiple protocols (Daneels & Salter, 1999).

5.4.2 Commercial Technology Inroads Into Industrial Control Networks

Commercial technology has made inroads into industrial control networks via two vectors: increased numbers of internet pathways and increased use of Commercial Off the Shelf (COTS) communication devices in industrial control networks. Industrial control networks saw widespread use decades before the internet (Robles & Choi, 2009). Since there were no initial

pathways to commercial networks during this period, many industrial control networks regarded security as an afterthought (Cárdenas, Amin, & Sastry, 2008). However, widespread internet connectivity has resulted in both indirect and direct pathways between it and industrial control networks (Patton, et al., 2014); take for instance proposed industrial control interaction via direct internet portals (Khatib, Dong, Qiu, & Liu, 2000) or cell phone applications (Ozdemir & Karacor, 2006). Additionally, recent advances in communication networks, such as Wireless Networks and the Internet of Things (IoT), are increasingly finding use in CI systems (Jiang, et al., 2014).

IoT advances and technologies, whereby communication abilities and links to everyday objects and devices (Wortmann & Flüchter, 2015), are increasingly finding use in CI systems to enable communication and monitoring of a wide number of devices. For example, smart grids might contain commercial wireless devices and protocols to enable meter or substation monitoring (Jiang, et al., 2014). Traditionally, CI security focused on SCADA systems and protocols, while the IoT has expanded the number and types of devices and standards CI communication networks must consider (Mo, et al., 2012). One type of IoT technology with increasing use in CI systems is the IEEE 802 standard subgroup (area networks) (IEEE, 2004). For instance, area networks have been, or been proposed for, use in CI, including the smart grid (Güngör, et al., 2011), smart cities and e-government (Chang, Kannan, & Fellow, 2003) (Harmon, Castro-Leon, & Bhide, 2015) and CI applications such as hospitals (Cao, Leung, Chow, & Chan, 2009). However, notable security deficiencies exist in many commercial communication standards, c.f. (Badenhop, Ramsey, Mullins, & Mailloux, 2016) (Melaragno, Bandara, Wijesekera, & Michael, 2012), thus including commercial communications devices introduces additional vectors for malicious agents to leverage.

Additionally, and naturally, connecting more and more CI devices through IoT advances results in big data concerns due to expanding volume, variety and the velocity of signals transmitted.

Due to the expanding variety and volume of devices in IoT CI implementations, future CI networks themselves have characteristics seen in the 3 V's (volume, variety, and velocity) of big data (Bihl, Young, & Weckman, 2016). Thus, monitoring logs and transmissions of communication devices to find threats can involve big data analytics due the massive amount of events logged (Samuelson, 2016) (Gutierrez, Bauer, Boehmke, Saie, & Bihl, 2017).

5.5 High Level Communication System Threats

Understanding cyber security involves understanding key characteristics of communication system threats. With an understanding of threats, one can develop and select appropriate security measures. Although a wide variety of threats exist, these can be grouped loosely by the approach taken, as conceptualized in the general taxonomy presented in Figure 5.3. In Figure 5.3, example threats include those related to the source (physical versus cyber), insider versus outsider (agent), and etc.; this representation was adapted from Nawir et al. (2016) by removing redundant groupings (information damage and access were synonymous) and introducing additional fields (e.g. supply chain related). A robust security approach mitigates these threats through a combination of both technological and non-technological methods.

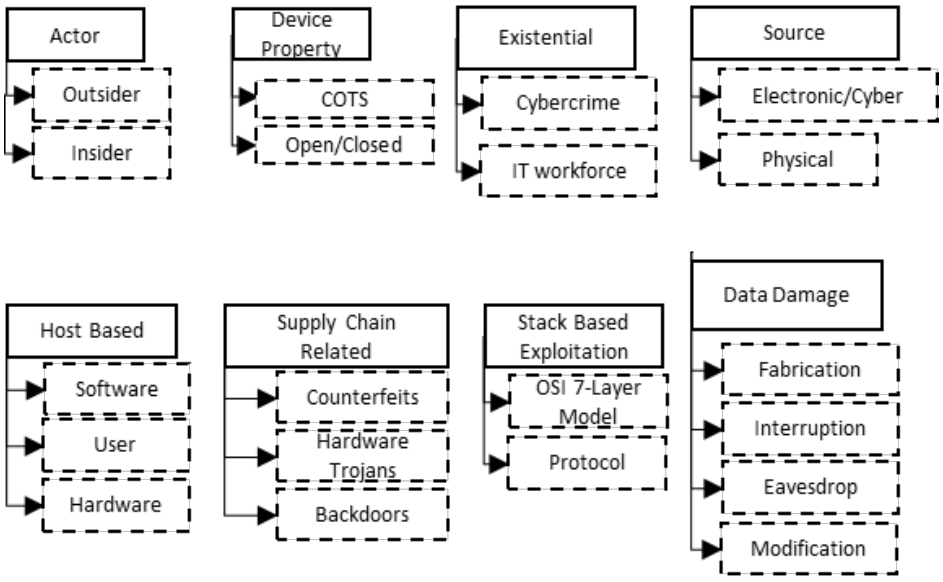

Figure 5.3: General taxonomy of communication system threats. (Adapted and Extended From (Nawir, Amir, Yaakob, & Lynn, 2016))

5.5.1 Actor-based Threats: Insider versus Outsider

From a system perspective, threats emanate from inside or outside malicious actor(s), which dictate different courses of action to prevent and mitigate (Walton & Limited, 2006). Historically, most security breaches in corporations and industrial control networks threats were internal in nature; however, external (cyber) threats and breaches have become more common due to increasing internet pathways within industrial control networks (Byres & Lowe, 2004).

Outsider threats are the work of hackers and malicious parties who wish to gain unauthorized access to a network and possibly disrupt its abilities (Walton & Limited, 2006). These threats inherently require technical approaches to mitigate and resolve (Walton & Limited, 2006). Conversely, insider threats are related to employees (past and present) and knowledgeable associates whose work is associated with the CI and communication system in question (Walton & Limited, 2006). Thus, insider threats are possibly immune to cyber security measures since malicious parties might know appropriate passwords, account details, etc. needed to achieve access.

Disaffected employees, and employees under the sway of blackmail, bribery, or ideology, way wish to disrupt or damage the network (Walton & Limited, 2006). Logically, one would desire to minimize insider threats completely and focus on outsider threats since insider threats are difficult to detect (Walton & Limited, 2006). However, three general approaches exist to detect and deter insider threats (Walton & Limited, 2006): 1) mitigating possible damages by compartmentalization; 2) early detection via authentication and auditing, and 3) proper management and ownership to reduce disaffection. Thus, a combination of proper security procedures, technology to find suspicious actions, and management all have roles in mitigating insider threats.

5.5.2 Device Property and Existential Related Issues

Various properties of the communication devices related to proprietary and non-proprietary designs can be exploited. If a communication network uses COTS devices, then any system using these devices inherits their known and unknown vulnerabilities (Cárdenas, Amin, & Sastry, 2008). Prior to wide spread use of COTS devices in CI implementation, industrial control networks used mostly highly customized software and hardware components and thus had the advantage of "security by obscurity" (Stuttard, 2005). The open versus closed nature of protocol designs can also be related to vulnerabilities; closed/proprietary protocols have the advantage of "security by obscurity." Security by obscurity means that closed and proprietary protocols benefit from their obscurity, where malicious actors find difficulty learning the particulars to exploit. Open designs with public protocols do not benefit from security by obscurity, however, such networks are generally safer since security professionals can fix and augment security issues as they become known (Cárdenas, Amin, & Sastry, 2008).

Vulnerabilities also exist due to existential issues related the expanding pool of skilled IT professionals throughout the world with the skills to attack communication systems (Cárdenas, Amin, & Sastry, 2008). Additionally, the amount of freely available cybercrime tools is expanding and available for use by even less skilled malicious actors (Cárdenas, Amin, & Sastry, 2008). However, it should be noted that while a certain pool of skilled IT professionals can be malicious, it is also advantageous to security to find flaws and develop solutions (Rescorla, 2005).

5.5.3 Host-based Threats

The host of the system can be compromised through various means as discussed by Nawir et al. (2016). For instance, an authorized user might not effectively protect credentials and so a malicious actor could gain access to a network via those authentic credentials. Alternatively,

an attacker could compromise software by overloading resource buffers or pushing devices to exhaustion. Finally, hardware can become compromised if malicious code is injected into it; for example, contact with infected flash drives was sufficient for the Stuxnet worm to infect computers which were not directly connected to the internet (Chen & Abu-Nimeh, 2011).

5.5.4 Physical versus Electronic Threats and Mitigation

Outsider threats involve attacks on a communication network by parties who are remote and not directly connected to the organization that manages the network (Walton & Limited, 2006). Broadly, outsider threats can be physical, like the 2013 assault on PG&E's Metcalf transmission station (Smith, 2014) for example; or electronic, like cyber attacks on CI (Miller & Rowe, 2012). Electronic threats broadly include all other software and protocol exploitation methods. Here, the communication medium is used as a vector to infect, restrict access, or damage network operating conditions. Physical attacks on CI systems can be seen in the form of terrorists and criminals who gain in-person access to a site to physically attack it (Smith, 2014). While these attacks might not aim specifically at the communication system, damages and reduced capabilities could result. While a physical attack on infrastructure can be mitigated by site security, physical attacks via hardware trojans are stealthy in nature and could result from an insecure electronic supply chain.

5.5.5 Supply Chain Related Threats and Mitigation

While electronic/cyber is the primary security concern in communication systems, supply chain concerns also exist since CI communication systems interact with physical objects and have many components, possibly at long distances from monitors. Outsourcing electronic production has introduced weaknesses in supply chain security for electronics and introduced various issues (Jang-Jaccard & Nepal, 2014). Physical threats exist in the form of counterfeit electronics, which can fail quicker (Guin U. , et al., 2014) (Tehranipoor, 2015), integrated

circuits which have hardware trojans, integrity circuits, or malignant logic can compromise the security of a network (Di & Smith, 2007) (Jang-Jaccard & Nepal, 2014), and compromised circuits can include backdoors to facilitate future attacks (Jang-Jaccard & Nepal, 2014). Collectively, robust physical security to limit unauthorized site access is necessary and includes secured integrated circuit supply chains (Karri, Rajendran, Rosenfeld, & Tehranipoor, 2010) (Guin U. , et al., 2014).

5.5.6 Information Damage Related Threats

In addition to the specific effects discussed in Section 5.2, data damage actions are possible, as discussed by Nawir et al. (2016). Once an actor or virus/worm has gained access to a network, various possible actions could happen to the data being collected. This data involves either the sensor readings from a substation and actions sent by an observer--so, data integrity is key to reliable operations. Threats exist to data in the interception of communications, whereby data might be monitored passively (eavesdropping) or even modified before it reaches its indented recipient. Data can also be fabricated to allow for situations where an attacker floods a system with data that shows normal conditions while the actual system is in an out of control state. Additionally, an attacker could interrupt data, which might cause the communication network to shut down or merely replay the last observations received.

5.5.7 Stack-Based Exploitations

Additional threats exist due to the exploitation of protocol characteristics and different functionalities of communication operations. Knowledge of protocol specifics can lend itself to the exploitation of weaknesses in a given protocol. Additionally, the operations and characteristics associated with each of the OSI 7-layers are associated with particular weaknesses. From a security and device identification standpoint, different layers of the OSI stack also correspond to different information, e.g. Network-level encryption keys are

"something you know," MAC-level MAC addresses are "something you have" and Physical-layer characteristics are "something you are" (Ramsey, Temple, & Mullins, 2012). With this understanding, one can further understand attacks and issues per layer and determine appropriate cyber security measures.

5.6 Cyber Threats and Security

Focusing primarily on the electronic/cyber threats found in the Stack-based Exploitation and Data Damage threats in Figure 5.3, requires understanding the specific threats employed and protection methods. Table 5.3 presents various threats and protection measures in reference to the 7-layer OSI model of Table 6.1 with threats and protections per (Nawir, Amir, Yaakob, & Lynn, 2016). Broadly, we will characterize these threats and security measures as: Component-Specific, e.g. PLC security issues, Physical Layer related, e.g. hardware threats, and then Software and Protocol-based, e.g. most of the issues found in Table 5.3.

Table 5.3: OSI 7 Layer Model with Example Threats and Protections Available Per Layer

Layer	Threats	Protection
Application	Clock Skewing, Selective Message Forwarding, Data Aggregation Distortion, Clone Attacks	High-level firewalls
Presentation	SSL to tunnel HTTP attacks	Applications delivery platform (ADP)
Session	Hijacking	Packet analysis, encryption, limiting packets
Transport	Renegotiation, port scans, DoS, misdirection, Flooding, De-synchronization	Handshake protocol
Network	False Routing, Packet Replication, Blackhole, Wormhole, Sinkhole, Sybil, Selective Forwarding, HELLO flood, Acknowledgement spoofing	Firewalls, encryption keys
Data Link	MAC Flooding, MAC spoofing, ARP Cache Poisoning, Traffic Manipulation, Identity Spook, Collision, Exhaustion, Unfairness	Intrusion detection/prevention systems (IDPS)
Physical	Device Tampering, Eavesdropping, Jamming, Counterfeits	RF Fingerprinting, PUFs, COAs

5.5.1 Component-Specific Related Threats and Mitigation

Security threats can exist due to weaknesses in specific components. Due to the large number of PLCs in an industrial control network, weaknesses found in these devices can be a critical vector for compromises to occur. Since PLCs monitor and control physical devices, realized threats related to PLCs can result in devices being driven out of safety margins and possibly to system damaging outcomes, e.g. Stuxnet (Chen & Abu-Nimeh, 2011). Threats to PLCs include worms that can infect and change memory values to arbitrary values resulting in a given PLC operating its control logic via incorrect values (Sandaruwan, Ranaweera, & Oleshchuk, 2013). Many PLCs also have forcing output functionalities which enable an operator to force an output to be a specific value; thus, any PLC with direct links to the internet could be compromised if an attacker gains direct access (Sandaruwan, Ranaweera, & Oleshchuk, 2013). Finally, protocol exploitations, e.g. the malformed packets (Ultes-Nitsche & Yoo, 2004), can be used as a further software vector to PLC attacks (Sandaruwan, Ranaweera, & Oleshchuk, 2013).

5.5.2 Software and Communication Threats and Mitigation

A wide variety of communication devices and standards exist in CI implementations, including a variety of SCADA protocols, e.g. Modbus®, RP-570, Profibus, Conitel, IEC 61850, T101, IEC 60870-5-101 (104), DNP V3.0, ISO-TSAP, and UCA (Utility Communications Architecture) (Robles, Choi, & Kim, 2009). While not all of these protocols employ the 7 OSI layers as described in Table 6.1, the same broad operations are still performed per protocol operations and thus all are generally susceptible to the various attacks lists in Table 5.3. All of these standards are associated with various advantages and weaknesses. For example, the ISO-TSAP protocol used by many Siemens PLCs does not provide for data encryption (Sandaruwan, Ranaweera, & Oleshchuk, 2013). Limitations in specific protocols have also led to the development of secured versions of protocols, e.g. “Secure MODBUS” (Fovino, Carcano, Masera, & Trombetta, 2009).

Incorporating intrusion detection and prevention systems (IDPS) into industrial control networks can mitigate MAC related attacks and provide a log of events which violate access rules (Zhu & Sastry, 2010)(Xing, Srinivasan, Jose, Li, & Cheng, 2010). However, IDPS systems generally rely on coded rules, which are limited against new and novel attacks (Gutierrez, Bauer, Boehmke, Saie, & Bihl, 2017). A variety of network based routing attacks exist and these can take the form of attackers flooding, or corrupting routing information or flooding the network with replicated packets to consume bandwidth and cause communication termination (Xing, Srinivasan, Jose, Li, & Cheng, 2010). Network attacks can be mitigated by routing access restrictions and detection methods that watch for false routing and other types of attacks (Xing, Srinivasan, Jose, Li, & Cheng, 2010). Higher level attacks can exist at the application level and influence the software used by the operator. For instance, clock skewing can desynchronize operations and cause communications to be unstable in protocols that require synchronization, e.g. wireless sensor networks operating under IEEE 802.11 (Xing, Srinivasan, Jose, Li, & Cheng, 2010). Authentication methods and data integrity approaches can be adopted to mitigate against these risks (Xing, Srinivasan, Jose, Li, & Cheng, 2010).

5.5.3 Physical Layer Threats and Security Measures

At the physical layer, a variety of threats can exist. For instance, devices can be tampered with, and counterfeit integrated circuits (IC) exist in the supply chain for many communication devices (Guajardo J. , Kumar, Schrijen, & Tuyls, 2008). Subsequently, various economic, security and safety issues can exist; for example: counterfeit IC results in millions to billions of dollars in lost revenue to developers, security issues exist in that counterfeit ICs could be designed to learn operating keys, thereby allowing unauthorized access, and further issues exist for users since counterfeit ICs are more prone to failure (Guajardo J. , Kumar, Schrijen, & Tuyls, 2008). While software-based security often receives the majority of the emphasis, all software-based security is hackable as seen in Table 5.3. Thus, determining the authenticity of

devices or individual ICs is also of interest for CI protection.

5.5.3.1 Biometric-like Security with Physical Layer Security Measures

Biometric security involves selecting using discriminating qualities that are *universal*, *distinct*, *permanent*, and *collectable* (Cobb, Garcia, Temple, Baldwin, & Kim, 2010). Biometric-like security for communication devices involves examining the intended and unintended communication and radiation are useful for device identification between disparate devices (Weng, et al., 2005) (Cobb, Laspe, Baldwin, Temple, & Kim, 2012). When devices from the same production run are considered, communication signal fingerprinting approaches enable production-induced variations to be discriminable (Cobb, Laspe, Baldwin, Temple, & Kim, 2012). Physical layer features and identification methods can be employed as an additional level of security whereby claimed identities are vetted for device identity authentication (Cobb, Laspe, Baldwin, Temple, & Kim, 2012). Physical layer features aim to characterize communication devices due to production variations whereby minute signal differences can be used to discriminate between individual devices (Cobb, Laspe, Baldwin, Temple, & Kim, 2012).

Because physical layer characteristics are associated with the intrinsic physics-based properties of devices, they provide inherent benefits in preventing spoofing attacks common with security at other OSI levels (Tomko, Rieser, & Buell, 2006). Desirable Physical layer characteristics are those that are identifiable and possess biometric-like qualities, see (Jain, Ross, & Prabhakar, 2004) (Ryer, Bihl, Bauer, & Rogers, 2012), of *universality*, *distinctiveness*, *permanence*, and *collectability* (Cobb, Garcia, Temple, Baldwin, & Kim, 2010). Two general approaches of physical layer security exist for this purpose: 1) adding physically traceable objects to devices (Grau, Zeng, & Xiao, 2012) (Majzoobi, Koushanfar, & Potkonjak, 2009) (DeJean & Kirovski, 2007), and 2) the exploiting inherent features present in device signals, e.g. through RF Fingerprinting (Suski, Temple, Mendenhall, & Mills, 2008) (Cobb, Garcia,

Temple, Baldwin, & Kim, 2010) (Ellis & Serinken, 2001) (Scanlon, Kennedy, & Liu, 2010).

5.5.3.2 Physically Traceable Objects

Three identification methods have been proposed to verify the identity of communication devices using physically traceable objects: Radio Frequency Identification (RFID), Physical Unclonable Functions (PUFs), and RF Certificates of Authenticity (RF-COA). While there are various benefits to each approach, all are limited in their ability to be applied to equipment already in use.

RFID is a tracking technology which involves placing an identifier antenna 'tag' on a device for tracking (Roberts, 2006) (Landt, 2005). To identify devices, the RFID tag either actively emits (powered RFID tags), or emits only when scanned (unpowered RFID tags) (Grau, Zeng, & Xiao, 2012). Due to the ability to remotely track objects, RFID has seen extensive use in commercial and warehouse applications for products tracking (Landt, 2005). RFID does have known issues, including: interference (Holland, Young, & Weckman, 2011), placement (RFID antennas must be located on each device), and type-level issues (multiple identical objects typically receive the same RFID tag).

Both PUFs and RF-COAs are an extension of the RFID process whereby uniquely identifiable components or antenna are added to an integrated circuit. However, whereas RFID tags operate at a type-level, PUFs and RF-COAs operate at a serial-number level. PUFs include two techniques for authentication: 1) adding internal measurement circuitry to integrated circuit (IC), and 2) adding capacitive sensors on top of ICs in a grid form (Cobb, Laspe, Baldwin, Temple, & Kim, 2012). PUFs work by incorporating a randomized component to these augmentations, to ensure uniqueness (Cobb, Laspe, Baldwin, Temple, & Kim, 2012).

RF-COAs essentially take the RFID concept and make small, unique, and three-dimension antennae using randomly shaped conductors and dielectric components which are placed onto ICs to create a uniquely identifiable RF signal (DeJean & Kirovski, 2007). In

essence, RF-COAs combine PUFs and RFID into a single IC identification approach (Cobb, Laspe, Baldwin, Temple, & Kim, 2012).

Both PUFs and RF-COAs can be employed to ensure ICs are authentic in a similar way that product keys are used to ensure authorized installation of software (Guajardo J. , Kumar, Schrijen, & Tuyls, 2008). While PUFs can provide increased security, both PUF approaches require physical IC manipulations and thus are prohibitive for use with legacy devices. RF-COAs have similar, and obvious, impediments to their use on legacy devices, in addition to extra design considerations needed in the manufacturing and design process. Finally, RF-COAs are further limited in utility due to the existence of spoofing mechanisms (DeJean & Kirovski, 2007).

5.5.3.3 Communication Signal Exploitation

RF Fingerprinting is the characterizing a communication device from minute differences in emanated signals to extract biometric-like features (Weber, Birkel, Collmann, & Engelbrecht, 2010) (Candore, Kocabas, & Koushanfar, 2009). RF Fingerprinting implies systematic signal collection, processing, sampling, statistical feature extraction methods, and classifier model development (Harmer, 2013). When considering intentional emissions, RF Fingerprinting has been successful in discriminating inter-device variations, e.g. similar devices from different manufacturers (Klein, 2009), and intra-device variations, e.g. devices from the same manufacturer that differ only by serial number (Bihl, Bauer, & Temple, 2016).

After collecting signals, a region of interest, e.g. the preamble which should be consistent for a protocol, is isolated (Bihl, Bauer, & Temple, 2016). Instantaneous amplitude, phase, and frequency response are then computed for each region of interest (Bihl, Bauer, & Temple, 2016). These responses are then divided into bins, from which RF Fingerprinting features are then extracted. The considered RF Fingerprinting features are generally the 2nd, 3rd, and 4th

mathematical moments (variance, skewness, and kurtosis), which are used to quantify distributional properties of the signal for identification (Cobb, 2011)(Thirukkonda, 2009) (Lohweg, et al., 2013). Figure 5.4 presents a visualization of the RF-DNA fingerprints from sampled-time ZigBee preamble data.

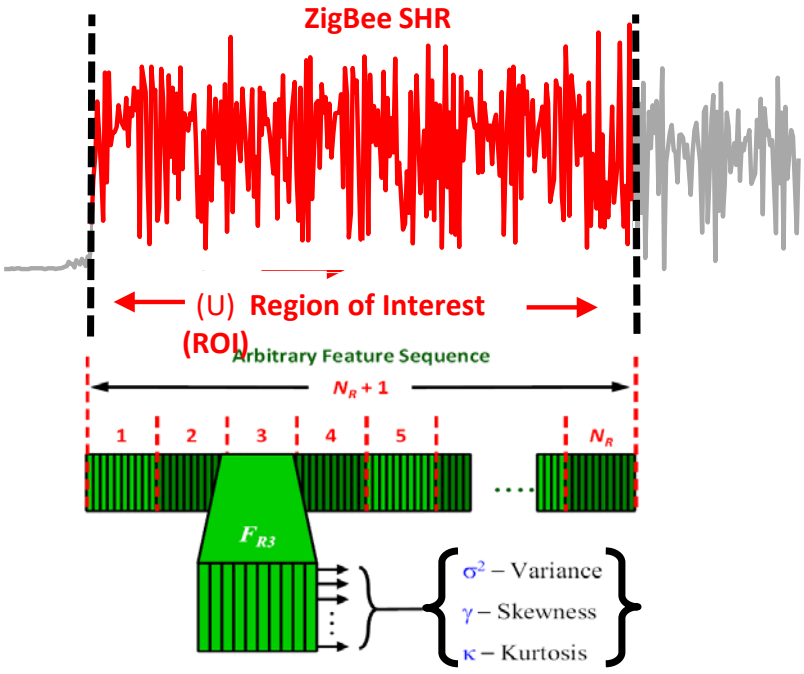

Figure 5.4: General RF Fingerprinting Process, Example Using with ZigBee Signal. (From (Bihl T. J., 2015))

Applicability of RF Fingerprinting methods includes wireless and wired communications, c.f. (Bihl, Bauer, & Temple, 2016) (Carbino, Temple, & Bihl, 2015). Recent advancements in adapting RF Fingerprinting to wired communication include the works of (Lopez, Temple, & Mullins, 2014) (Ross, Carbino, & Stone, 2017), both of which explored CI related communication device discrimination. Outside of laboratory research, commercial devices have begun to provide physical layer authentication ability, e.g. (PFP Cybersecurity, 2016).

5.6 Conclusions

To have a reliable industrial control network, one must consider effective security measures. Security primarily involves authenticating the identity of devices and operators and thus restricting unauthorized access to networks. Given the severity of intrusions in CI networks, preventing unauthorized access and limiting internet pathways are necessary. However, the expansion of IoT into CI systems, e.g. the Smart Grid, precludes the ability to successfully rely on security through obscurity for industrial control networks and thus and effective cyber security strategy is necessary. Although much research and work exists in cyber security and authentication, these tend to be related to preventing certain types of attacks or focusing on one layer of the OSI stack. In operation, one would desire to create a systematic security and authentication scheme whereby a claimed identity is vetted through physical layer authentication.

5.7 References

Agrawal, D., Archambeault, B., Rao, J. R., & Rohatgi, P. (2003). The EM Side—Channel(s). *Cryptographic Hardware and Embedded Systems - CHES 2002, 2523*, 29-45.

Ahmed, I., Obermeier, S., Naedele, M., & Richard III, G. (2012). Scada systems: Challenges for forensic investigators. *Computer, 45*(12), 44-51.

Alsiherov, F., & Kim, T. (2010). Research trend on secure SCADA network technology and methods. *WSEAS Transactions on Systems and Control, 8*(5), 635-645.

Badenhop, C. W., Ramsey, B. W., Mullins, B. E., & Mailloux, L. O. (2016). Extraction and analysis of non-volatile memory of the ZW0301 module, a Z-Wave transceiver. *Digital Investigation, 17*, 14-27.

Bihl, T. J. (2015). *Feature Selection and Classifier Development for Radio Frequency Device Identification.* Air Force Institute of Technology: Ph.D. Dissertation.

Bihl, T. J., Bauer, K. W., & Temple, M. A. (2016). Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions. *IEEE Transactions on Information Forensics and Security, 11*(8), 1862-1874.

Bihl, T. J., Young, W. A., & Weckman, G. R. (2016). Defining, Understanding, and

Addressing Big Data. *International Journal of Business Analytics (IJBAN), 3*(2), 1-32.

Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. *Proceedings of the VDE Kongres*, 213-218.

Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. *Proceedings of the VDE Kongress*, 213-218.

Candore, A., Kocabas, O., & Koushanfar, F. (2009). Robust stable radiometric fingerprinting for wireless devices. *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST)*, 43-49.

Cao, H., Leung, V., Chow, C., & Chan, H. (2009). Enabling technologies for wireless body area networks: A survey and outlook. *IEEE Communications Magazine, 47*(12), 84-93.

Carbino, T. J., Temple, M. A., & Bihl, T. J. (2015). Ethernet card discrimination using unintentional cable emissions and constellation-based fingerprinting. *International Conference on Computing, Networking and Communications (ICNC)*, 369-373.

Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. *HotSec*.

Chang, A.-M., Kannan, P. K., & Fellow, S. (2003). Preparing for wireless and mobile technologies in government. *E-government* , 345-393.

Chen, T., & Abu-Nimeh, S. (2011). Lessons from stuxnet. *Computer, 44*(1), 91-93.

Clarke, G. R., Reynders, D., & Wright, E. (2004). *Practical modern SCADA protocols: DNP3, 60870.5 and related systems.* Newnes.

Cobb, W. E. (2011). *Exploitation of Unintentional Information Leakage from Integrated Circuits.* Air Force Institute of Technology: PhD Dissertation.

Cobb, W. E., Garcia, E. W., Temple, M. A., Baldwin, R. O., & Kim, Y. C. (2010). Physical layer identification of embedded devices using RF-DNA fingerprinting. *Military Communications Conference (MILCOM)*, 2168-2173.

Cobb, W. E., Laspe, E. D., Baldwin, R. O., Temple, M. A., & Kim, Y. C. (2012). Intrinsic physical-layer authentication of integrated circuits. *IEEE Transactions on Information Forensics and Security, 7*(1), 14-24.

Couch, L. W. (1993). *Digital and Analog Communication Systems* (4 ed.). New York: MacMillan.

Creery, A., & Byres, E. (2005). Industrial cybersecurity for power system and SCADA networks. *Industry Applications Society 52nd Annual Petroleum and Chemical Industry Conference*, 303-309.

Daneels, A., & Salter, W. (1999). What is SCADA? *International Conference on Accelerator and Large Experimental Physics Control Systems*, 339-343.

DeJean, G., & Kirovski, D. (2007). RF-DNA: Radio-Frequency Certificates of Authenticity. *Cryptographic Hardware and Embedded Systems (CHES)*, 346-363.

Di, J., & Smith, S. (2007). A hardware threat modeling concept for trustable integrated circuits. *IEEE Region 5 Technical Conference*, 354-357.

Dolezilek, D., & Schweitzer, E. O. (2000). *SEL communications and integration white paper.* Schweitzer Engineering Laboratories .

Ellis, K. J., & Serinken, N. (2001). Characteristics of radio transmitter fingerprints. *Radio Science , 36*(4), 585-597.

Ellison, R. J., Fisher, D. A., Linger, R. C., Lipson, H. F., & Longstaff, T. (1997). *Survivable network systems: An emerging discipline.* Carnegie-Mellon Univ. Pittsburgh, PA: Software Engineering Ins.

Fernandez, J., & Fernandez, A. (2005). SCADA systems: Vulnerabilities and remediation. *Journal of Computing Sciences in Colleges, 20*(4), 160-168.

Fovino, I., Carcano, A., Masera, M., & Trombetta, A. (2009). Design and Implementation of a Secure Modbus Protocol. *Critical Infrastructure Protection*, 83-96.

Frenzel, L. (2013, Mar. 22). *What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?* Retrieved Nov. 11, 2014, from Electronic Design: http://electronicdesign.com/what-s-difference-between/what-s-difference-between-ieee-802154-and-zigbee-wireless

Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control networks. *IEEE Communications Surveys and Tutorials, 15*(2), 860-880.

Gomez Gomez, J. A. (2005). *Survey of SCADA SYSTEMS and visualization of a real life process.* Linköping University: MS Thesis.

Goverment Accountability Office (GAO). (2008). *TVA Needs to Address Weaknesses in Control Systems and Networks, GAO-08-526.* Washington DC: US Government.

Grau, D., Zeng, L., & Xiao, Y. (2012). Automatically tracking engineered components through shipping and receiving processes with passive identification technologies. *Automation in Construction, 28*, 36-44.

Guajardo, J., Kumar, S. S., Schrijen, G. J., & Tuyls, P. (2008). Brand and IP protection with physical unclonable functions. *IEEE International Symposium on Circuits and Systems (ISCAS)*, 3186-3189.

Guajardo, J., Kumar, S. S., Schrijen, G.-J., & Tuyls, P. (2008). Brand and IP protection with physical unclonable functions. *IEEE International Symposium on Circuits and Systems (ISCAS)*, 3186-3819.

Guin, U., Huang, K., DiMase, D., Carulli, J. M., Tehranipoor, M., & Makris, Y. (2014).

Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. *Proceedings of the IEEE, 102*(8), 1207-1228.

Guin, U., Huang, K., DiMase, D., Carulli, J., Tehranipoor, M., & Makris, Y. (2014). Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. *Proceedings of the IEEE, 102*(8), 1207-1228.

Güngör, V., Sahin, D., Kocak, T., Ergüt, S., Buccella, C., Cecati, C., & Hancke, G. (2011). Smart grid technologies: communication technologies and standards. *IEEE Transactions on Industrial Informatics, 7*(4), 529-539.

Gutierrez, R. J., Bauer, K. W., Boehmke, B. C., Saie, C. M., & Bihl, T. J. (2017). Cyber Anomaly Detection: Using Tabulated Vectors and Embedded Analytics for Efficient Data Mining. *Journal of Algorithms and Computational Technology*.

Harmer, P. K. (2013). *Development of a Learning from Signals Classifier for Cognitive Software Defined Radio Applications.* Wright Patterson AFB, OH: Ph Dissertation (DRAFT), Air Force Institute of Technology.

Harmon, R. R., Castro-Leon, E. G., & Bhide, S. (2015). Smart cities and the Internet of Things. *Portland International Conference on Management of Engineering and Technology (PICMET)*, 485-494.

Higgs, M. (2000). Electrical SCADA systems from the operators perspective. *International Conference on Human Interfaces in Control Rooms, Cockpits and Command Centres*, 458-461.

Holland, W. S., Young, W. A., & Weckman, G. R. (2011). Facility RFID localization system based on artificial neural networks. *International Journal of Industrial Engineering: Theory, Applications and Practice, 18*(1), 16-24.

Hu, X., Wang, B., & Ji, H. (2013). A wireless sensor network-based structural health monitoring system for highway bridges. *Computer-Aided Civil and Infrastructure Engineering, 28*(3), 193-209.

IEEE. (2004). *Overview and Guide to the IEEE 802 LMSC.* Institute of Electrical and Electronics Engineers.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol., 14*(1), 4-20.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993.

Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., & Shen, X. S. (2014). Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology, 19*(2), 105-120.

Kang, D.-j., & Robles, R. J. (2009). Compartmentalization of protocols in SCADA communication. *International Journal of Advenced Science and Technology, 8*, 27-36.

Karri, R., Rajendran, J., Rosenfeld, K., & Tehranipoor, M. (2010). Trustworthy hardware: Identifying and classifying hardware trojans. *Computer, 43*(10), 39-46.

Khatib, A.-R., Dong, Z., Qiu, B., & Liu, Y. (2000). Thoughts on future Internet based power system information network architecture. *IEEE Power Engineering Society Summer Meeting*, 155-160.

Klein, R. W. (2009). *Application of dual-tree complex wavelet transforms to burst detection and RF fingerprint classification.* Air Force Institute of Technology: PhD Dissertation.

Landt, J. (2005). The history of RFID. *IEEE Potentials, 24*(4), 8-11.

Liao, Q., Luo, X. R., Gurung, A., & Shi, W. (2015). A holistic understanding of non-users' adoption of university campus wireless network: An empirical investigation. *Computers in Human Behavior, 48*, 220-229.

Liu, C.-C., Stefanov, A., Hong, J., & Panciatici, P. (2012). Intruders in the grid. *IEEE Power and Energy magazine, 10*(1), 58-66.

Lohweg, V., Hoffmann, J. L., Dörksen, H., Hildebrand, R., Gillich, E., Hofmann, J., & Schaed, J. (2013). Banknote authentication with mobile devices. *IS&T/SPIE Electronic Imaging*, 1-14.

Lopez, J., Temple, M. A., & Mullins, B. E. (2014). Exploitation of HART Wired Signal Distinct Native Attribute (WS-DNA) Features to Verify Field Device Identity and Infer Operating State. *International Conference on Critical Information Infrastructures Security*, 24-30.

Luiijf, E. A., & Klaver, M. H. (2004). Protecting a nation's critical infrastructure: The first steps. *IEEE International Conference on Systems, Man and Cybernetics*, 1185-1190.
Majzoobi, M., Koushanfar, F., & Potkonjak, M. (2009). Techniques for design and implementation of secure reconfigurable PUFs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS), 2*(1), 1-33.

Mardiguian, M. (2001). *Controlling Radiated Emissions by Design.* Springer.

McMaster, H. R. (2003). *Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War*. Carlisle, PA: US Army War College.

Melaragno, A., Bandara, D., Wijesekera, D., & Michael, J. (2012). Securing the ZigBee Protocol in the Smart Grid. *Computer, 45*(4), 92-94.

Miller, B., & Rowe, D. C. (2012). A Survey of SCADA and Critical Infrastructure Incidents. *1st Annual conference on Research in information technology*, 51-56.

Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE, 100*(1), 195-209.

Montrose, M. I. (2004). *EMC and the Printed Circuit Board: Design, Theory, and Layout Made Simple.* John Wiley & Sons.

Moteff, J., & Parfomak, P. (2004). *Critical infrastructure and key assets: definition and identification.* Washington DC: Congressional Research Service.

Nawir, M., Amir, A., Yaakob, N., & Lynn, O. (2016). Internet of Things (IoT): Taxonomy of security attacks. *3rd International Conference on Electronic Design (ICED),* 321-326.

Ozdemir, E., & Karacor, M. (2006). Mobile phone based SCADA for industrial automation. *ISA transactions, 45*(1), 67-75.

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. (2014). Uninvited connections: a study of vulnerable devices on the internet of things (IoT). *IEEE Joint Intelligence and Security Informatics Conference (JISIC),* 232-235.

Peltier, T. R. (2005). *Information Security Risk Analysis.* CRC Press.

Pennesi, S., & Sebastiani, S. (2005). Information security and emissions control. *International Symposium on Electromagnetic Compatibility, 3*, 777-781.

Perry, T. S., & Geppert, L. (1996). Do portable electronics endanger flight? The evidence mounts . *IEEE Spectrum, 33*(9), 26-33.

PFP Cybersecurity. (2016). Embedding Security in the Internet of Things. *White Paper*.

Queiroz, C., Mahmood, A., Hu, J., Tari, Z., & Yu, X. (2009). Building a SCADA security testbed. *Third International Conference on Network and System Security*, 357-364.

Ramsey, B., Temple, M., & Mullins, B. (2012). PHY foundation for multifactor ZigBee node authentication. *Global Communication Conference (GLOBECOM)*, 795-800.

Reaves, B., & Morris, T. (2012). Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. *International Journal of Critical Infrastructure Protection, 5*(3), 154-174.

Rescorla, E. (2005). Is finding security holes a good idea? *IEEE Security & Privacy, 3*(1), 14-19.

Roberts, C. M. (2006). Radio frequency identification (RFID). *Computers & Security, 25*(1), 18-26.

Robles, R. J., & Choi, M.-k. (2009). Assessment of the vulnerabilities of SCADA, control systems and critical infrastructure systems. *International Journal of of Grid and Distributed Computing Assessment, 2*(2), 27-34.

Robles, R. J., Choi, M.-k., & Kim, T.-h. (2009). The Taxonomy of SCADA Communication Protocols. *Proceedings of KIIT Summer Conference,* 116-119.

Robyns, P., Quax, P., & Lamotte, W. (2017). PHY-layer security is no alternative to cryptography. *10th ACM Conference on Security and Privacy in Wireless and Mobile Networks* , 160-162.

Ross, B. P., Carbino, T. J., & Stone, S. J. (2017). Physical-Layer Discrimination of Power Line Communications. *International Conference on Computing, Networking and Communications (ICNC)*, 341-345.

Ryer, D. M., Bihl, T. J., Bauer, K. W., & Rogers, S. K. (2012). QUEST hierarchy for hyperspectral face recognition. *Advances in Artificial Intelligence*.

Samuelson, D. A. (2016). Using big data in cybersecurity. *ORMS-Today, 43*(5).

Sandaruwan, G. P., Ranaweera, P. S., & Oleshchuk, V. A. (2013). PLC security and critical infrastructure protection. *8th IEEE International Conference on Industrial and Information Systems (ICIIS)*, 81-85.

Scanlon, P., Kennedy, I. O., & Liu, Y. (2010). Feature extraction approaches to RF fingerprinting for device identification in femtocells. *Bell Labs Technical Journal, 15*(3), 141-151.

Schneider Electric. (2012). *SCADA Systems* . Schneider Electric.

Slay, J., & Miller, M. (2007). Lessons learned from the maroochy water breach. *Critical infrastructure protection*, 73-82.

Smith, R. (2014, 2 2). Assault on California power station raises alarm on potential for terrorism. *Wall Street Journal*.

Snow, A. P., Varshney, U., & Malloy, A. D. (2000). Reliability and survivability of wireless and mobile networks. *Computer, 33*(7), 49-55.

Stuttard, D. (2005). Security & obscurity. *Network Security, 7*, 10-12.

Suski, W. C., Temple, M. A., Mendenhall, M. J., & Mills, R. F. (2008). Using spectral fingerprinting to improve wireless network security. *IEEE Global Commun. Conf. (GLOBECOM)*, 1-5.

Tehranipoor, M. M. (2015). *Counterfeit integrated circuits.* Springer International Publishing.

Thirukkonda, S. (2009). *Correlation in Firm Default Behavior.* M.S. Thesis: Massachusetts Institute of Technology.

Tomko, A. A., Rieser, C. J., & Buell, L. H. (2006). Physical-layer intrusion detection in wireless networks. *IEEE Military Communications Conference (MILCOM)*, 1-7.

Ultes-Nitsche, U., & Yoo, I. (2004). Run-Time Protocol Conformance Verification In Firewalls. *ISSA*, 1-11.

US Government Accountability Office. (2004). *Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems.* Washington, DC: GAO-05-434.

Walton, R., & Limited, W.-M. (2006). Balancing the insider and outsider threat. *Computer fraud & security*, *11*, 8-11.

Weber, M., Birkel, U., Collmann, R., & Engelbrecht, J. (2010). Comparison of various methods for indoor RF fingerprinting using leaky feeder cable. *Workshop on Positioning Navigation and Communication (WPNC)*, 291-298.

Weng, H., Dong, X., Hu, X., Beetner, D. G., Hubing, T., & Wunsch, D. (2005). Neural network detection and identification of electronic devices based on their unintended emissions. *International Symposium on Electromagnetic Compatibility, 1*, 245-249.

Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering,*, *57*(3), 221-224.

Xing, K., Srinivasan, S., Jose, M., Li, J., & Cheng, X. (2010). Attacks and countermeasures in sensor networks: a survey. *Network security*, 251-272.

Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. *IEEE wireless communications*, *11*(1), 38-47.

Zhu, B., & Sastry, S. (2010). SCADA-specific intrusion detection/prevention systems: a survey and taxonomy. *Workshop on Secure Control Systems (SCS)* .