https://doi.org/10.48009/1_iis_2019_119-133

INDUSTRIAL INTERNET OF THINGS VULNERABILITIES AND THREATS: WHAT STAKEHOLDERS NEED TO CONSIDER

Fred Hoffman, Mercyhurst University, fhoffman@mercyhurst.edu

ABSTRACT

The Industrial Internet of Things, or IIoT, introduces Internet-enabled devices into industrial process systems operating in the energy, transportation, healthcare, utilities, cities, agriculture, and other critical infrastructure sectors, establishing linkages between previously-air gapped information technology (IT) and operational technology (OT) networks. While the introduction of these Internet-enabled devices creates new efficiencies, improves performance, increases productivity, and increases profitability, it also introduces new security challenges and risks. IIoT is a system of systems; the architecture of a single IIoT system consists of different layers, with each layer performing a distinct function, having unique operational characteristics, and relying upon different devices and communication protocols than other layers of the system. Because of the unique characteristics of these various layers and functions, the vulnerabilities and threats associated with them also differ. Many internal stakeholders are involved in the conceptualization, planning and implementation of an organization's adoption of IIoT; while some may be experienced and knowledgeable technologists, others are not. Regardless of one's technical knowledge, recognition of the potentially-catastrophic consequences of successful exploitation of those vulnerabilities necessitate at least some familiarity with security vulnerabilities and threats associated with the various IIoT layers and sub-systems. The purpose of this article is to identify for IIoT stakeholders some of the vulnerabilities and threats associated with various layers and functions of an IIoT architecture and illuminate the need for a comprehensive, systematic, and layer-appropriate approach to IIoT security.

Keywords: Industrial Internet of Things, Industry 4.0, Industrial Control Systems, SCADA, critical infrastructure, security

INTRODUCTION

For decades, industrial processes and the industrial control systems (ICS) that operate them have been protected, to a large extent, by the fact that these were typically proprietary systems with most or all hardware and software components designed, produced and integrated by a single manufacturer and functioning on a closed operational network that was air-gapped from other networks. Such systems were not designed to be exposed to the Internet over an open network link, communicate via the cloud, or even support bi-directional communications; however, all three of these aforementioned characteristics are central to the Industrial Internet of Things, or IIoT.

The introduction of Internet-enabled devices and systems into industrial operations, critical infrastructure, and other large-scale applications entices stakeholders through the prospect of increased efficiency, reduced cost, improved maintenance, increased profit margins, and competitive advantage. At the same time, IIoT stakeholders must recognize there are vulnerabilities and risks associated with implementing and operating an IIoT system, and ensure such recognition is not only factored into their IIoT security strategy, but also into their equipment acquisition and implementation decisions.

IoT, IIoT, AND INDUSTRY 4.0

Three terms associated with the introduction of Internet-enabled devices into industrial processes are IoT, Industry 4.0, and IIoT. As depicted in Figure 1, these three terms are not interchangeable; they refer to related, but differing, concepts.

Internet of Things (IoT)

First used by Kevin Ashton in 1999 while giving a presentation at Proctor and Gamble (Eigner, 2017), the term Internet of Things (IoT) refers to the cyber networking of physical objects that enables those objects to interact and work together. IoT is where the cyber and physical worlds meet (Mehnen, He, Tedeschi, & Tapoglou, 2017).

Industrial Internet of Things (IIoT)

General Electric first introduced the term *Industrial Internet* in 2012 (Evans & Annunziata, 2012), and in 2014 partnered with AT\&T, Cisco, Intel and IBM to form the Industrial Internet Consortium (IIC), a non-profit organization dedicated to the furtherance of the concept (Bledowski, 2015). IIoT describes a large-scale operation in which data is collected from different sensors, actuators, and devices within an industrial environment, and both data and devices are controlled via the Internet (Aazam, Zeadally, & Harras, 2018). The scope of the Industrial Internet/IIoT is rather broad, encompassing such diverse industrial sectors as energy, transportation, healthcare, utilities, cities, agriculture, and mining (Bledowski, 2015).

Industry 4.0

In contrast to the much broader concept of IIoT, Industry 4.0 focuses on manufacturing and related activities. Whereas IIoT was the brainchild of U.S. corporations, the Industry 4.0 concept arose from the German federal government's desire for Germany industry to become more efficient and productive through the integration of automation information technology. The term Industry 4.0 (or *Industrie 4.0*) was coined by the German government to describe not only the computerization of manufacturing processes (Aazam, Zeadally, & Harras, 2018), but also the integration of activities throughout the value chain, encompassing such distinct functions as design, supply chain, production, distribution, and customer service (Bledowski, 2015). Within the context of Industry 4.0, the Germans also coined the term *cyber-physical systems* (CPS), which refers to the embedding of software into machines and devices and then linking them via the Internet for monitoring and control with the goal of reducing errors and failures while increasing efficiency (Bledowski, 2015). The purpose of CPS is to incorporate machines and devices into an interconnected industrial environment to automate and improve process control and efficiency, while enabling better decision-making (Mehnen, He, Tedeschi, & Tapoglou, 2017).

IoT, IIoT, and Industry 4.0: What's in a name?

Although it is not uncommon to hear Industry 4.0 and IIoT used interchangeably, the two terms differ in significant ways. As shown in Figure 1, both IIoT and Industry 4.0 are actually subsets of IoT. Whereas Industry 4.0 is more narrowly focused on manufacturing, IIoT encompasses critical infrastructure, Smart Cities, Smart Agriculture, and other activities well beyond the scope of Industry 4.0. While both IIoT and Industry 4.0 are business-oriented subsets of the Internet of Things, mainstream news media reporting on the Internet of Things tends to focus on such *consumer*-oriented devices as smart phones, wearable devices, smart TVs, smart appliances, and such smart home functions as remotely-controlled lights and security systems. By contrast, IIoT is *industry*-oriented, with so-called Smart Factories, Smart Grids, Smart Machines, Smart Cities, Smart Vehicles, and Smart Agriculture. Although IoT, Industry 4.0, and IIoT have different origins, describe different concepts, and focus on different activities and consumer targets, what they all have in common is the joining and networking of the cyber and physical worlds via the Internet. Commonalities between IIoT, IoT, and Industry 4.0 include: (1) Internet-enabled devices; (2) Internet connectivity between devices; (3) data management; (4) data processed and secured separately from the device (at the Edge, in the Fog, or in the Cloud). It has been estimated that by 2020, approximately 37 billion different things (Internet-enabled products or devices) will be connected to the Internet via IPv6 (Eigner, 2017).

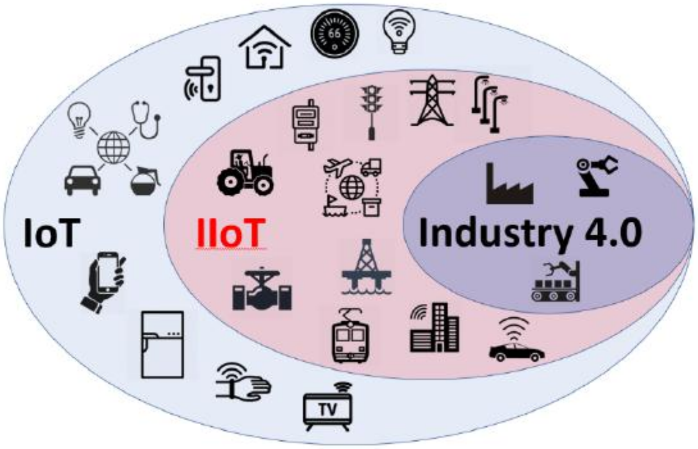


Figure 1. How IoT, IIoT, and Industry 4.0 relate to one another

IIOT AND CRITICAL INFRASTRUCTURE

Presidential Policy Directive 21 (2013) identifies the following 16 national infrastructure sectors as critical to U.S. national security: Chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems. A good business case can be made for the introduction of IIoT into each of these sixteen critical infrastructure sectors. For industrial operations in the petrochemical or energy industries, for example, the introduction of Internet-enabled devices holds forth the prospect of remotely updating, diagnosing, and restarting connected devices and systems without necessitating the dispatch of technicians to remote sites (Asplund & Nadjm-Tehrani, 2016). Unfortunately, the proliferation of low-cost Internet Protocol (IP)-based IIoT devices have increased the vulnerability of these industrial systems to cyberattack (Trautman & Ormerod, 2018). In 2003, a massive power blackout in North America negatively impacted not only electric power distribution, but also transportation, the water supply, communications systems, and also several industries (Andersson et al, 2005). Although the blackout was caused by a software bug in an electric grid control room, rather than by the actions of malicious actors, the incident illustrates the scale of the consequences that can result from critical infrastructure failure. The 2018 SANS Industrial IoT Security Survey report projected that the installed base of IoT devices will triple, from 23 billion in 2018 to 75 billion by 2025, causing increased need for bandwidth and for security-savvy professionals skilled in the design, implementation, and operation of IIoT systems (Filkins & Wylie, 2018).

Security threats to industrial control systems

Industrial Control Systems, or ICS, serve as the central nervous system of critical infrastructure networks ranging from power and water systems to manufacturing and transportation. In the past, ICS have proven to be less susceptible (but not immune) to cyber intrusion because they have traditionally been closed, stand-alone systems employing proprietary control protocols and specialized hardware and software (Trautman & Ormerod, 2018) and were not connected to the Internet. In the past, ICS security was due, in large measure, to obscurity (Bhattacharjee, 2018). Due to the addition to Internet-enabled devices in industrial processes, that situation is rapidly changing, and neither ICS manufacturers nor system operators can rely on obscurity as a mainstay of ICS security (Freemantle & Scott, 2017). The highly-complex nature of these industrial operations, coupled with their high-volume outputs, make them natural candidates for incorporating emerging I-IoT technologies that offer the prospect of improving efficiency and productivity while reducing cost (Filkins &Wylie, 2018). However, the proliferation of low-cost Internet Protocol (IP)-based I-IoT devices designed for use in industrial processes, coupled with their introduction into previously proprietary, stand-alone ICS systems, have increased the vulnerability of these industrial systems to cyberattack (Trautman & Ormerod, 2018). A central security challenge of IIoT is linkage via the Internet of once-separate IT and OT networks. Some common OT networks include proprietary Industrial Control Systems (ICS), Supervisory Control and Data Acquisition systems (SCADA), process control networks (PCN), manufacturing execution systems (MES), telematics, robotics, facilities management and building automation systems (Contu, Middleton, Alaybeyi & Pace, 2018).

Increased connectivity equals increased risk

When a stand-alone ICS was produced by a single manufacturer (such as ABB, Honeywell, Yokogawa, or Siemens), communication protocols were proprietary and exclusive to that particular manufacturer's equipment. Consequently, conducting a cyberattack against such a system made it necessary for an attacker to not only acquire a copy of the proprietary ICS software to develop a malware that would be effective against a that system, but also somehow identify and then exploit an access opportunity and conduit to deliver the malware. The push toward IIoT changes this scenario significantly. In contrast to proprietary and unitary ICS, IIoT devices and systems are now offered by an ever-growing number of manufacturers. In order for these various IIoT components and devices to successfully function in an industrial enterprise, hardware and software produced by those different manufacturers must be able to successfully integrate and communicate with one another. Consequently, there is a push within the IIoT community for standards-based connectivity technology. As industrial protocols become standardized, industrial networks become increasingly susceptible to cyberattacks involving more generic malware that could be employed, with little or no modification, against many different industrial process implementations (Bhattacharjee, 2018). Increased connectivity translates to increased vulnerability. Between 2012 and 2017, the number of cyberattacks targeting ICS in the United States increased a whopping 490 percent (Industrial Control Systems Security, 2017). In March, 2018 the U.S. federal government issued a highly-detailed interagency report (Russian Government Cyber Activity, 2018) describing how Russian government hackers allegedly conducted a sophisticated, seven-stage cyber operation against U.S. energy sector networks and gained access to Supervisory Control and Data Acquisition (SCADA) systems. Although no damage was done to those targeted networks, this provided small consolation to U.S. authorities who are very well aware that peacetime network intrusions and cyber reconnaissance are necessary to lay the groundwork for future cyberattacks on a network.

Attacks on industrial control systems

The 2010 Stuxnet attack demonstrated that cyberweapons could be used to effectively and catastrophically attack physical systems (Hassanzadeh, Modi, & Mulchandani, 2015; Corbò et al, 2018). Stuxnet specifically targeted programmable logic controllers (PLC) that were essential for the operation of centrifuges in a uranium enrichment process performed at a closed facility in Natanz, Iran. The highly-sophisticated malware was designed to operate in three sequential phases: First, it was designed to auto-execute on USB drives, which made it possible for the attacker(s) to target a network that was not connected to the Internet. Second, the malware was designed to identify whether the target was using Siemens PCS7 or Simatic WinCC software and, if so, to alter files essential for controlling programmable logic controllers (PLC). Finally, the malware would not only cause targeted PLCs to modify valve settings, but also deceive system operators by displaying previously-recorded, normal measurements while the targeted centrifuges spun out of control and destroyed themselves (Goodman, 2014; Hassanzadeh, Modi, & Mulchandani, 2015). Other recent, noteworthy cyberattacks on industrial control systems include the Shamoon virus, which in 2012 affected tens of thousands of computers used by energy companies in the Middle East, and the Sandworm attack on Ukraine’s electric power (EP) infrastructure which in 2015 denied electricity to nearly half a million Ukrainians (Gavin, 2018). The attack by pro-Russian hackers on Ukraine's EP grid demonstrated the scale of damage that could be achieved by a cyberattack on critical infrastructure. It is noteworthy that the ability of the Ukrainians to switch over to manual control is believed to have reduced the severity of the attack (Joo & Tan, 2018). Whether such a manual override option would exist within an IIoT-enabled EP system, and how effective it would be as a response to such an attack, would depend on a variety of factors. The consequences of not being able to effectively respond to a cyberattack with sufficient speed was demonstrated in 2014, when hackers targeting a German steel mill first gained remote access to the company's administrative network, then to the steel mill's production management system, which in turn enabled the attackers to take over most of the facility’s control systems (Lee, Assante, & Conway, 2014). Once they gained control, the attackers systematically destroyed human machine interface components and, by preventing a blast furnace from initiating its security settings in a timely manner, caused major damage to the facility (Cyberattack on a German steel mill, 2016).

IOT AS A TARGET

Industry security experts fear that the integration of Internet-enabled devices, systems, and cloud resources create vulnerabilities that put operational capabilities and intellectual property at risk (Hounshell, 2018). Those fears are not unfounded; poorly-secured IoT devices were successfully exploited by malicious individuals to conduct the 12 October 2016 Mirai botnet attack that hijacked IoT devices and conduct a massive distributed denial of service (DDoS) attack that made much of the Internet inaccessible to users on the U.S. East Coast.

VULNERABILITIES AND IIOT LAYERS

Fully 62 percent of industrial participants attending the Industry of Things 2017 conference identified cybersecurity and data privacy as major concerns associated with the adoption of IIoT (Bhattacharjee, 2018). While the introduction of Internet-enabled devices into industrial processes is a defining characteristic of IIoT, there are some unique aspects of the IIoT which make thinking about IIoT system security different from, say, the security of the Internet. These unique qualities derive from the architecture of an IIoT system and the vulnerabilities associated with the devices and communications between them occurring at the various IIoT layers. Large-scale industrial operations are extremely complex and rely on the near-constant availability and reliability of multiple systems, each consisting of myriad components and sub-components produced by multiple manufacturers. In addition, the different roles and functions performed at different layers of an IIoT system means there can be no silver bullet security solution; instead, a cyber security approach involving domain-specific methodologies and tools becomes necessary (Mavropoulos, Mouratidis, Fish, and Panaousis, 2018).

The architecture of IIoT has been characterized in different ways. Above the layer of Things comprising the IoT (devices, machines, tools, cars, buildings, et cetera), Boyes, Hallaq, Cunningham, & Watson (2018) describe a four-stage IoT architecture as consisting of (1) the edge, (2) Internet gateways and acquisition, (3) edge IT, and (4) data center/cloud architecture. Bhattacharjee's five levels are (1) process, (2) basic control, (3) supervisory control, (4), and (5) corporate network. In the most recent release of its Industrial Internet Reference Architecture, the Industrial Internet Consortium (2017) describes a three-tiered IIoT architecture consisting of (1) an edge tier, (2) a platform tier, and (3) an enterprise tier. This article, which focuses on security vulnerabilities of different IIoT architecture functions, takes a *functional* approach to examining IIoT; that is, identifying security threats and vulnerabilities that exist because of the particular nature and characteristics of certain functions within an IIoT system.

The Edge

The field level, or edge, is where the rubber meets the road within an IIoT system. At the edge, the lowest level of an IIoT system, one finds devices with sensors, actuators, and controllers linked to the Internet either directly or via a gateway (Freemantle & Scott, 2017). In an edge device, sensors measure, while actuators are electronically-controlled components that cause something to occur in a device, such as opening or closing a valve. The edge is comprised of machines, physical sensors, actuators, controllers, intelligent and connected edge nodes, which may be wired or connected wirelessly, typically via Bluetooth, WiFi, NRF, or LiFi. Transceivers may convert data protocols or switch between data communication types; this level is considered machine-to-machine (M2M), and there may not be an Internet connection (Mehnen, He, Tedeschi, & Tapoglou, 2017). Machine-to-machine communication, or direct communication between devices without human intervention (Sadeghi, Wachsmann, & Waidner, 2015), can be conducted wired or wirelessly, via a growing number of communications protocols. Many IIoT Edge devices are deployed on so-called low-power and lossy networks (LLN), which have very limited computing power, memory, and energy Alaba, Othman, Hashem, & Alotaib 2017). Because of their role in the industrial process, edge devices may be unattended and remotely deployed at the far geographical reaches of an industrial operation. One example would be a flow monitoring device deployed on a natural gas pipeline (Forsström, Butun, Eldefrawy, Jennehag, & Gidlund, 2018). At the edge level, the greatest security threats to sensors, actuators, controllers, and other edge devices are not cyber, but either electronic (such as jamming) or kinetic, which are physical attacks intended to damage, degrade, disrupt, or destroy the devices. While much of the literature on IIoT security understandably focuses on the risk of cyberattacks, insufficient attention is paid to the threat of electronic and kinetic attacks, despite the fact that devices at the physical edge of IIoT are highly vulnerable to physical attack due to their remote deployment and relative inaccessibility (Mehnen, He, Tedeschi, & Tapoglou, 2017).

Wireless Sensor Networks (WSN)

Wireless Sensor Networks, or WSN, represent a defining feature of the edge layer within an IIoT system. At its lowest layer, an IIoT system is essentially an integrated network of Internet-enabled sensors providing a heretofore unimaginable degree of transparency and insight regarding the status of a complex industrial operation over a geographically-dispersed area that (in the case of a pipeline) could involve hundreds of miles (Huberman, 2016). Within a particular IIoT system, there may be hundreds, or even thousands, of small, dispersed, low-power sensors deployed for such diverse uses as industrial quality control, traffic scrutiny, wildlife monitoring, disaster response, military scrutiny, smart building, battlefield scrutiny, forest fire detection, humidity recording, flood detection, temperature recording, pressure monitoring and light monitoring inside the area of distribution (Acharjya & Ahmed, 2017).

Advances in such communication technologies as Zigbee, Bluetooth Low Energy (BLE), and Internet Protocol version 6 over low-power wireless personal area networks have been key contributors to enabling WSNs to perform as part of IIoT systems (Aazam, Zeadally, & Harras, 2018). Factors contributing to the vulnerability of WSNs include the open nature of wireless channels used by many WSN devices combined with the power, computing, and memory limitations of sensor nodes which make public key cryptography algorithms like RSA unsuitable for employment in WSN environments (Li, Niu, Bhuiyan, Wu, Karuppiah, & Kumari, 2018). Typical Internet security measures like encryption and digital signatures may not work with low power/low bandwidth IIoT devices (Freemantle & Scott, 2017).

Although the sensors, actuators, and controllers found within WSNs are generally less-sophisticated than other devices and equipment found within an IIoT system, that does not mean they are unimportant. For example, the failure of a smart sensor controlling several valves in a refinery could lead to a chain reaction involving other devices, resulting in an overall system failure (Huberman, 2016).

WSN can be targeted for either passive or active attacks. Passive attacks include monitoring and eavesdropping, impersonation, node capturing, and spoofing (Yazdinejad, Nayyeri, & Afshari, 2017). Some of the active attack types that Karlof & Wagner (2003) identified as having been conducted against WSNs include sinkhole attack, sensed data attack, black hole attack, gray hole attack, bogus routing, jamming, selective forwarding attack, wormhole attack, and hello flood attack. Both passive and active attacks against WSN generally require proximate access to the targeted device(s). For example, a malicious actor executing a hello flood attack would get within the communications footprint of the target network to employ a more powerful transceiver and introduce hello packets (Acharjya & Ahmed, 2017). Passive attacks are no less worrisome than active attacks, in part because successful passive attacks can enable subsequent active attacks. For example, node capturing not only makes it possible for attackers to capture encryption keys and protocol states, but then clone captured data to mimic legitimate devices in the network for spoofing and other malicious purposes (Yazdinejad, Nayyeri, & Afshari, 2017).

Gateways
WSN devices communicate with one another using non-IP communication protocols. Raw data from the Edge is generally not aggregated and passed on, unprocessed, to higher levels of the IIoT system. Instead, that Edge passes through a gateway, which contains fieldbus-based interfaces, protocols, and data collection and processing capability.

Middleware and the Fog
Within an IIoT system, middleware is software that links an operating system or database and its applications Freemantle & Scott (2017). One type of middleware used in IIoT systems is referred to as the fog because it exists below the system operator and cloud levels, but above the edge (or device) level. Internet gateways exist between the fog layer and the levels above and below it, and engage in the transfer of communication between them. The amount of data generated by all the devices across an IIoT system is staggering; aggregating all of it in the cloud would be costly in terms of storage, computing capability, and power requirements. This is the rationale behind the fog layer. Like cloud computing, fog computing is also used to store and share data within an IIoT system, but is located closer to the sources of the data in an IIoT system, which enables adequate latency and the efficient processing of time-sensitive data closer to the edge (Fu, Liu, Chao, Bhargava, & Zhang, 2018). Six functions of the fog identified by Aazam, Zeadally, & Harras (2018) include: (1) Real-time industrial big data mining for high performance; (2) concurrent data collection from multiple types of sensors, robots, and machines; (3) fast processing of sensed data to generate instructions for the actuators and robots within some acceptable latency; (4) interfacing incompatible sensors and machines through necessary protocol translation and mapping; (5) managing system power management; (6) data structuring and filtering to avoid sending unnecessary data to the core and the cloud.

SCADA & PLCs
Supervisory Control and Data Acquisition (SCADA) systems function as the central nervous system an industrial control system. Sitting at control room consoles featuring graphical representations of system processes, system operators use SCADA hardware and software to monitor, manage, and control industrial processes. Like ICS, SCADA networks also traditionally relied upon their use of proprietary protocols and separation from other networks to provide security (Choi, Chang, Yun, & Kim, 2015). Asplund and Nadjm-Tehrani (2016) describe attacks against the Modbus, DNP3, and IEC-60870-5-014 protocols commonly found in SCADA systems. As Internet-enabled IIoT devices are incorporated into industrial processes, vulnerability increases as system operators gravitate toward IP-based cyber-physical systems (Mehnen, He, Tedeschi, & Tapoglou, 2017). SCADA systems contained within such IIoT systems as train control (“Smart Train”) or electric power distribution (“Smart Grid”) contain lower-layer sub-controllers called programmable logic controllers (PLC). Integrated with remote terminal units (RTU), human-machine interfaces, and a fieldbus system, PLCs comprise the backbone of a SCADA system. Dick Morley's invention of the PLC in 1968 revolutionized industrial processes; until then, factories relied on dedicated controllers, relays, and fixed circuits to automate the production process; periodically updating each of them was time- and labor-intensive endeavor (Willner, 2018). PLCs are responsible for command disaggregation within an industrial process. For example, if a power grid needs to reduce load by 100 MW across the entire grid, PLCs disaggregate this original command into a succession of sub-commands across the network (Peng, Zhu, Zhu, Hu, Cui & Yan, 2017). Attacks against PLCs can be carried out in a variety of ways. Network intrusions can target communications protocols like UDP, TCP, SIP, DNS, and FTP (Caselli, Zambon, Petit & Kargl, 2015). One known security risk associated with PLCs is the command disaggregation attack, in which attackers modify the disaggregated commands and thereby manipulate the control process in a desired manner (Peng, Zhu, Zhu, Hu, Cui

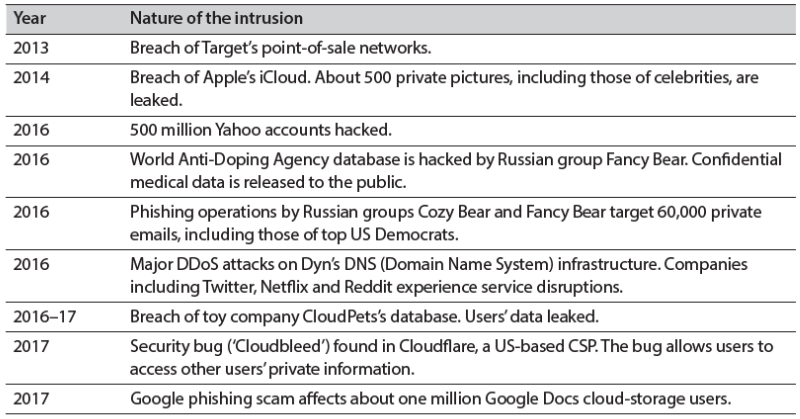
& Yan, 2017). Another method is by inserting malware into devices before they are introduced into the targeted facility, which many believe was the modus operandi used in the 2010 Stuxnet attack targeting Siemens-manufactured PLCs controlling centrifuges in an Iranian uranium enrichment facility, since that facility was not connected to the Internet (Goodman, 2014; Hassanzadeh, Modi, & Mulchandani, 2015).

Distributed storage

Large enterprises continue to migrate away from traditional, on-site data storage in favor of online storage solutions. Distributed and networked storage help IIoT systems handle such huge data sets while enabling system scalability. IIoT systems generate and collect, process, analyze, act upon, and store massive volumes of data. Distributed storage makes it possible for applications to be run from the cloud, and enormous quantities of data to be uploaded and stored there (Shetty & Manjaiah, 2017). Factors contributing to the appeal of distributed storage systems like the Hadoop Distributed File System (HDFS) are reductions in the cost of storage coupled with increases in bandwidth capacity, computing capability, and storage volume. One obvious drawback to distributed storage is that whereas consolidated storage provides a potential attacker with just one target, distributed storage provides a potential attacker with many. To paraphrase bank robber Willie Sutton, distributed and networked storage systems are worthwhile targets for malicious actors because that's where the data is. By means of such techniques as active tap, passive tap, denial of service, faking, replay, and traffic analysis, malicious actors could attack distributed storage devices, systems, associated applications, and networks (Shetty & Manjaiah, 2017).

The Cloud

Even before the emergence of IIoT, companies were attracted to cloud storage as a cost-effective alternative to on-premise storage, eliminating the need to perform their own hardware upgrades, software updates, dedicated database administrators, and so on. Although the Cloud performs a central role in IIoT, one major security vulnerability is that the IIoT system operator transfers responsibility for data security to cloud service providers (CSP). As Figure 2 reflects, CSPs have a less-than-perfect track record when it comes to data security (Joo & Tan, 2018).



Year	Nature of the intrusion
2013	Breach of Target's point-of-sale networks.
2014	Breach of Apple's iCloud. About 500 private pictures, including those of celebrities, are leaked.
2016	500 million Yahoo accounts hacked.
2016	World Anti-Doping Agency database is hacked by Russian group Fancy Bear. Confidential medical data is released to the public.
2016	Phishing operations by Russian groups Cozy Bear and Fancy Bear target 60,000 private emails, including those of top US Democrats.
2016	Major DDoS attacks on Dyn's DNS (Domain Name System) infrastructure. Companies including Twitter, Netflix and Reddit experience service disruptions.
2016–17	Breach of toy company CloudPets's database. Users' data leaked.
2017	Security bug ('Cloudbleed') found in Cloudflare, a US-based CSP. The bug allows users to access other users' private information.
2017	Google phishing scam affects about one million Google Docs cloud-storage users.

Figure 2. Graphic from: Joo and Tan (2018)

Cloud-based services

Not only is the cloud used for data storage, it is also increasingly where software applications, platforms, and virtual infrastructure are housed. Even SCADA can be based in the cloud; one significant risk associated with cloud-based SCADA involves communication with controlled devices. Even SCADA can be based in the cloud; one significant risk associated with cloud-based SCADA involves communication with controlled devices, since those communications may be conducted via unsecured satellite or radio (Gavin, 2018).

INTEROPERABILITY AND SECURITY

In contrast to traditional ICS and SCADA systems, most of whose components were frequently all made by the same manufacturer, IIoT represents not only the aggregation, but also the synchronization, of cyber-physical systems, hardware, and software produced by an ever-expanding number of large and small manufacturers. Another difference between traditional industrial control equipment and IIoT systems is that communication protocols are no longer proprietary. Open platforms like Raspberry Pi and Arduino, and standardized protocols like Modbus, MQTT, REST, WebSocket, and others make it possible for IIoT equipment manufacturers to build devices which can integrate into, and operate within, an IIoT system (Márquez, Herrera, Mejías, Esquembre & Andújar, 2018). While open platforms and standardized protocols facilitate the integration and operation of these diverse IIoT components, they also make life considerably easier for malicious actors due to the economy of scale: An identified vulnerability in one open platform or protocol creates opportunities to target multiple systems that use them.

POTENTIAL THREAT ACTORS AND IIOT

Information security experts generally agree that people, rather than technology, represent the greatest threat to information systems (Ortiz & Matthews, 2016). Human threats to IIoT can be *external* or *internal*. External threats can include malicious actors, bad manufacturers, and bad system operators. External malicious actors who pose a potential threat to IIoT systems include not only the cyberwarfare and foreign intelligence services (FIS) of nation states, but also sub-state actors as organized criminals, terrorists, hacktivists, and even malicious individuals (Ortiz & Matthews, 2016). Manufacturers of IIoT systems and components could also pose security threats by failing to adequately design and build secure IIoT devices, treating security as an afterthought rather than as a core design consideration, or even by intentionally leaving back doors in a product to enable future clandestine access for the purpose of acquiring user data and exposing it to third parties without the system operator's knowledge or consent (Atamli & Martin, 2014). Another external threat could be posed by bad system operators or partners who install insecure devices, fail to adequately train employees on property security practices, or sufficiently vet or monitor contractors and other third parties who have access to the IIoT system facilities and devices.

Internal human threats to an IIoT system, the so-called insider threat, could be either *malicious* or *unintentional*. Malicious actors could range from a disloyal employee acting at the direction of a FIS, terrorist group, or criminal enterprise to a disgruntled or emotionally-unbalanced employee. Unintentional internal threats are posed by otherwise loyal employees who through security policy ignorance, inattention, or laziness unwittingly provide unauthorized access to a malicious actor, or perhaps enable a cyberattack by clicking on a phishing email (Mouton, Leenen, & Venter, 2016). Inadvertent disclosure of sensitive IIoT data can result if the system operator, or someone otherwise legitimately involved with the IIoT system, does something that inadvertently exposes sensitive data or information to unauthorized parties.

POTENTIAL THREAT TYPES & TECHNIQUES VERSUS IIOT

Cyber

As the Stuxnet and German Steel Mill attacks demonstrate, the sophistication of cyberattacks have increased significantly over the last decade; today's attackers employ such techniques as spear phishing and watering holes – social engineering tactics used by malicious actors to trick targeted individual(s) into unwittingly downloading malware onto their system – to carry out sophisticated, multi-phase attacks (Hassanzadeh, Modi, & Mulchandani, 2015). Viruses, worms, Trojan horses, and logic bombs are different types of malware that cause effects ranging from temporary disruption or denial of service to preventing legitimate user access to the system (as in the case of ransomware) or even causing the physical destruction of equipment (as occurred in the 2010 Stuxnet and 2014 German steel mill incidents) (Mehnen, He, Tedeschi, & Tapoglou, 2017).

Radio frequency weapons

Although the defining feature of an IIoT system is its incorporation of Internet-enabled devices, a typical IIoT system will use a variety of communication systems and protocols, to include over-the-air systems like Bluetooth and WiFi. Radio frequency (RF) weapons are devices that could be used to deny, deceive, disrupt, or distort communications involving the targeted device and/or network. One RF technique that could be employed against a wireless sensor network, for example, is *jamming*. Jamming attacks generally exploit the signal strength, packet sending and receiving rate, packet delivery ratio, and certify rate of the targeted device (Acharjya & Ahmed, 2017). A second type of RF attack is *signal injection*. One characteristic of industrial control systems, as compared to most other IT systems, is the consistency and regularity of their communications patterns, which contributes to the stability of controlled processes in power plants, water treatment facilities, electric grids, and other critical infrastructure (Caselli, Zambon, Petit & Kargl, 2015, p. 49). Unfortunately, malicious actors who are knowledgeable of these systems can subvert them by introducing false command messages via so-called semantic attacks. Signal injection involves an attacker introducing fake data into the system, such as by targeting a sensor or sensors electromagnetically. A third type of RF attack, known as *side channel*, is more passive in nature. In this type of attack, the attacker electronically eavesdrops on IIoT system communications, perpetrating a privacy breach, as a result of which private and confidential information can be inferred on the basis of timing analysis of the execution, power consumption, traffic analysis, fault analysis, and electromagnetic analysis of the device (Atamli & Martin, 2014). Such successful eavesdropping enables the malicious actor to employ an active technique called elevation of privileges; this is accomplished by eavesdropping on WSN over-air communications, and joining the network for malicious purposes by pretending to be a legitimate device, thus gaining privileged access to a device or system (Atamli & Martin, 2014).

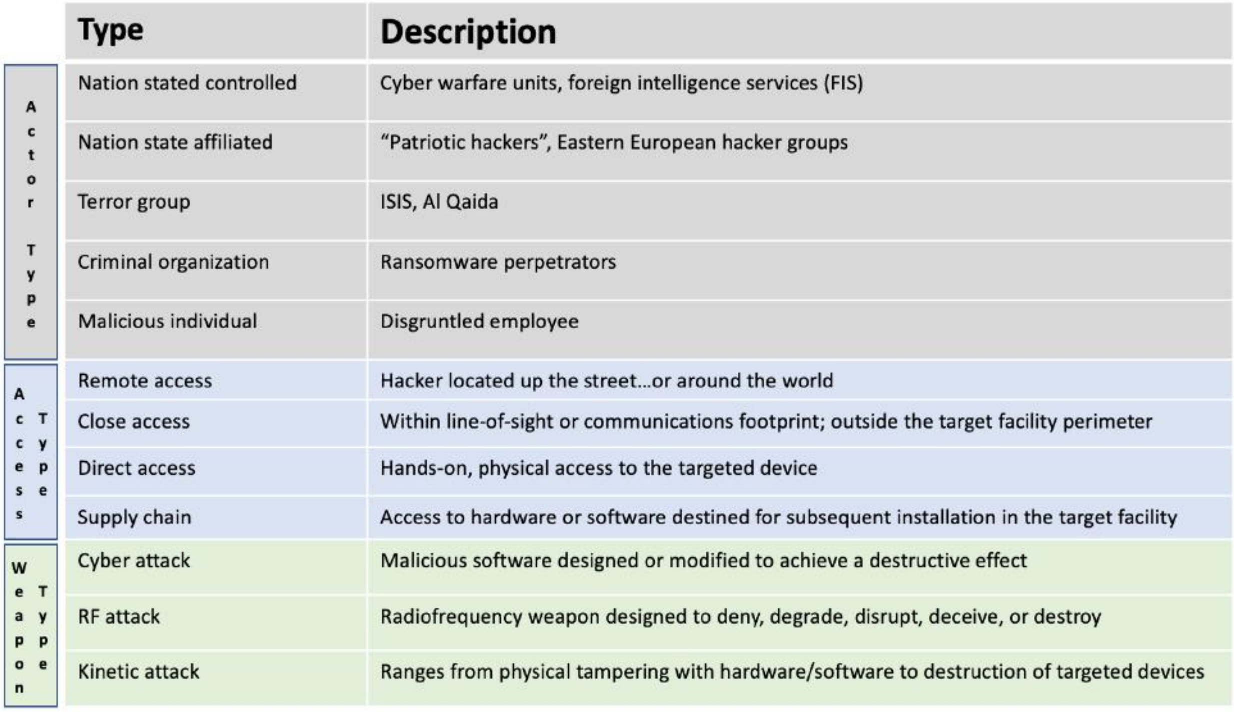
Kinetic

IIoT systems include both cyber and physical components, and in a typical IIoT system physical devices may be geographically dispersed and deployed in unattended and/or unmonitored locations, which could enable malicious (external or internal) actors to physically access, tamper with, or destroy them. Tampering could involve such actions as physically altering or damaging hardware, modifying the device software, or installing a monitoring device, transmitter, or beacon. Device tampering could also be performed on an IIoT device via a supply chain interdiction, either before the device is delivered to the system operator for installation, or when it has been temporarily removed from the system for maintenance or repair. Finally, an attacked could physically destroy a targeted device, either through direct, hands-on access or with a stand-off weapon like a rifle or directed energy weapon.

THREAT ACTOR ACCESS TO IIOT

Attacker and attack determining factors

Some of the factors determining the nature of an attack that could be conducted against an IIoT system include: (1) The type of attacker (nation state, sub-national actor, criminal entity, political activist, disgruntled employee); (2) the resources and capabilities of the attacker; (2) the attacker's objectives; (3) the characteristics of the target and its environment; (4) the nature of the tool or weapon; (5) the attacker's need for anonymity. Figure 3 depicts threat actors, access types, and weapon types.



	Type	Description
Actor Type	Nation stated controlled	Cyber warfare units, foreign intelligence services (FIS)
	Nation state affiliated	"Patriotic hackers", Eastern European hacker groups
	Terror group	ISIS, Al Qaida
	Criminal organization	Ransomware perpetrators
	Malicious individual	Disgruntled employee
Access Type	Remote access	Hacker located up the street…or around the world
	Close access	Within line-of-sight or communications footprint; outside the target facility perimeter
	Direct access	Hands-on, physical access to the targeted device
	Supply chain	Access to hardware or software destined for subsequent installation in the target facility
Weapon Type	Cyber attack	Malicious software designed or modified to achieve a destructive effect
	RF attack	Radiofrequency weapon designed to deny, degrade, disrupt, deceive, or destroy
	Kinetic attack	Ranges from physical tampering with hardware/software to destruction of targeted devices

Figure 3. Threat actors, access types, and weapon types

Attacks can be overt, covert, or clandestine. An overt attack is one in which the attacker makes no effort to conceal its involvement in the attack. A covert attack, like the 2010 Stuxnet attack, is one in which the victim is aware that something has occurred, and may even strongly suspect who perpetrated the attack, but the actual attacker maintains plausible deniability. In a clandestine attack, the attacker gains access to the system and conducts activities against the target system of which the victim remains unaware. A recent example of a clandestine attack was the alleged Russian cyber intrusion against U.S. energy sector networks (Russian Government Cyber Activity, 2018). In that particular instance, however, the perpetrators presumably desired to remain clandestine/undetected, but failed.

Remote, close access, or direct access
Remote access is when the attacker is physically remote from the targeted system, such as a hacking group overseas that sends a phishing email to employees of a targeted U.S. company. A *close access* attack is one where the attacker must get physically close enough to the targeted system to attack it, but not physically touch system devices. An example of a close access attack was the alleged April 2018 attack by Russian military intelligence cyber intelligence operatives against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands, where the suspects traveled to the Netherlands, came within range of the OPCW's WiFi network, and prepared to gain illicit access for the alleged purpose of compromising and disrupting computers before being apprehended (How the Dutch foiled Russian 'cyberattack' on OPCW, 2018). Another example of a close access attack would be someone who is physically outside the security fence of the targeted facility but is able to target a device or network with a radio frequency weapon (jammer). In a *direct access* operation, the attacker has hands-on access to the targeted device; a common example would be a malicious insider who inserts a USB containing malware into a targeted system. Another would be someone who gains hands-on access to a device deployed in a remote, poorly-secured location.

Supply chain operations
One of the earliest, and most spectacular, cyberattacks on an industrial system was actually carried out years before the Internet even existed. In 1982, an alleged Trojan horse attack exploiting a SCADA system vulnerability caused an explosion on a Siberian pipeline in the former Soviet Union that has been described as the first successful cyberattack on a SCADA system in history (Sajid, Abbas, & Saleem, 2016, p. 1377). According to former U.S. Secretary of the Air Force Thomas Reed, during the Cold War the CIA cooperated with Canadian authorities to modify SCADA control system software that they knew was being targeted for illicit acquisition in Canada by the KGB for installation in the Soviet pipeline transporting natural gas from the Urengoi gas fields in Siberia into Western Europe. The covert supply chain operation involved tampering with the software, permitting the Soviets to illegally acquire it in Canada, and then sitting back and waiting after unsuspecting Soviet engineers install the weaponized software. "The pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space" (Reed, 2005, p. 268). Reed claimed that the pipeline explosion had the explosive force of a three-kiloton nuclear weapon and disrupted Soviet supplies of gas and desperately-needed foreign currency income for more than a year (Byrnes & Eng, 2009).

As depicted in Figure 4, the complexity of IIoT systems and the unique operational characteristics of the various functions that comprise it create different types of vulnerabilities.

IIoT Devices
Field devices are low-power units having limited functionality and possessing minimal energy, computing power, memory, and storage capacity; they normally communicate wirelessly and are frequently deployed remotely, are unattended, and have much lower physical security than enjoyed by most IIoT equipment. For these reasons, they are most susceptible to kinetic attack (close or direct access) or attack with RF weapons (close access). Cyberattack, while possible against certain systems, is less likely and would involve direct (as opposed to remote) access. Although supply chain operations pose a comparatively greater threat to high-value IT equipment targets at the higher levels of an IIoT system architecture, easier physical access to these devices by lower-level employees or third-party contractors could serve as an enticement to potential attackers.

Local Application
There are many variables impacting the vulnerability of local applications, access being foremost among them: A trusted insider (such as a malicious employee or third-party contractor) could directly insert malware, as could an unwitting employee who fails to follow security policy and, say, unwittingly inserts an infected drive or permits unauthorized access to a third party. The threat posed by kinetic attack or RF weapons is moderate-to-low.

IIoT Network

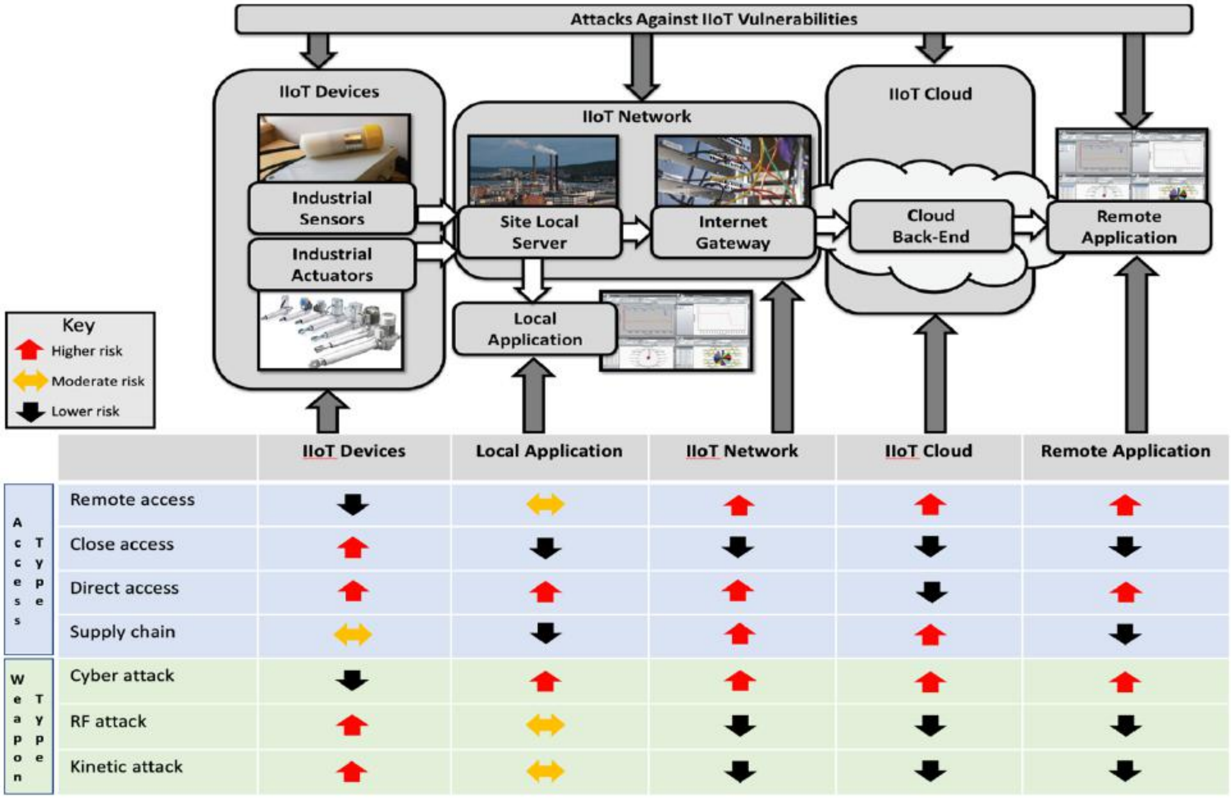
Hardware, software, and/or communications systems contained within the IIoT network represent some of the most lucrative targets for malicious actors not only because of their anticipated direct impact, but also because attacking them would likely cause significant second- and third-order effects elsewhere in the system. Because the IIoT network is such a high-value segment of the IIoT system, and attacking it would likely have such high impact, it would be a strong candidate for a supply chain operation. Because of their physical locations and heightened security, it would be challenging for an external malicious actor to attack them through close access. However, while the threat of kinetic or RF attacks is low, the threat posed by cyber weapons is high because they could either be delivered remotely (such as via phishing emails or a watering hole), or through direct access by a trusted (but malicious) insider who delivers the malware via USB drive. Even a loyal employee could pose a direct access cyber threat by failing to observe security policy and/or falling victim to a malicious actor's social engineering ploy.

IIoT Cloud

Servers located in the IIoT Cloud benefit from good physical and IT security measures, very limited employee access, and system redundancy. These all mitigate against close or direct access attacks, and reduce the potential effectiveness of RF or kinetic attacks. However, as was noted earlier, a risk IIoT operators accept when they contract for Cloud services is reliance upon the Cloud service provider for the provision of adequate and consistent security. The greatest threat to the IIoT Cloud comes in the form of cyber weapons that could be delivered remotely, or via a supply chain operation that introduces an infected Cloud component. The dispersed nature of Cloud servers and facilities reduces the appeal of either kinetic or RF attack.

Remote Application

As with local applications, there are many variables impacting the vulnerability of remote applications. Again, physical access and user adherence to security policy are major factors. RF and kinetic attacks are not major risks, nor is supply chain. By comparison, the direct access cyber threat posed by a malicious or unwitting insider is high, as is the risk of a remotely-conducted cyberattack. Figure 4 depicts the vulnerability types and threat levels across the IIoT value chain.



		IIoT Devices	Local Application	IIoT Network	IIoT Cloud	Remote Application
Access Types	Remote access	⬇	⬌	⬆	⬆	⬆
	Close access	⬆	⬇	⬇	⬇	⬇
	Direct access	⬆	⬆	⬆	⬇	⬆
	Supply chain	⬌	⬇	⬆	⬆	⬇
Weapon Type	Cyber attack	⬇	⬆	⬆	⬆	⬆
	RF attack	⬆	⬌	⬇	⬇	⬇
	Kinetic attack	⬆	⬌	⬇	⬇	⬇

Figure 4. IIoT value chain & vulnerability types. Adapted from Forsström et al. (2018), p. 219

CONCLUSIONS

By identifying some of the vulnerabilities and threats associated with different layers and functions of an IIoT system, this article sought to illustrate to stakeholders involved in IIoT planning and implementation the importance of having a comprehensive, systematic, and well-thought-out security approach to IIoT security. Not all security techniques are equally effective, or even suitable, for all the layers and functions within an IIoT system. For example, encryption solutions developed for the Internet exceed the power, computing, and/or memory capacities of many Edge devices. Similarly, while Blockchain currently receives considerable attention as a security solution for IIoT, some experts remain skeptical of the notion that Blockchain is appropriate for all IIoT devices. One of the identified shortcomings associated with blockchain is scalability (Huberman, 2016).

Given these varied vulnerabilities and threats, an enterprise must not only develop an overarching, macro-level IIoT security strategy, but also have that strategy encompass layer- and system-specific security approaches that have been developed and implemented by suitably-trained and experienced professionals. Finding those IIoT professionals is becoming increasingly difficult; a 2017 survey of executives in the oil, gas, and energy sectors found that more than 20% professed to lacking the skilled workforce needed for growth (Gavin, 2018). The demand for experienced and knowledgeable security practitioners in the IIoT space can only be expected to grow.

Because an IIoT system is comprised of multiple layers, each with its own unique vulnerabilities and security challenges, an IIoT security strategy must adequately take into consideration each of those layer-specific vulnerabilities within the context of a holistic security strategy that takes into account the full spectrum of potential threats to the system. From a security standpoint, an IIoT system is more than just the sum of its parts. One reason a siloed approach to IIoT security is inadvisable is because of the difficulty in clearly delineating who would be responsible for addressing what risks: Information Technology and Operational Technology come together under IIoT, but security strategies, techniques, and solutions for IT and OT differ in significant ways (Gavin, 2018). Therefore, those throughout the enterprise having security responsibilities must communicate, coordinate, and collaborate across functional layers no less effectively than the IIoT system itself was designed to operate.

An effective security strategy for an IIoT system involves more than just highly-trained security professionals and IT security solutions; more than anything, it starts with *imagination*. Who might want to target the system, and under what circumstances? The U.S. military and intelligence communities have long used an approach called red teaming, in which a team is assembled and instructed to “think like the bad guys” in identifying vulnerabilities and dreaming up creatives ways to exploit them. Rather than just leaving security planning to security experts, democratize security by leveraging the knowledge and experience of the workforce. A manager could consult with an experienced field supervisor and ask, “If you were a bad guy, how would *you* attack this process?” Those responsible for IIoT security need to think beyond cyber, take insider threats into account, and prioritize security through good risk management practices. A good place to start would be to develop a threat matrix that takes into account the criticality of a system or component, the consequences of its disruption, and the means and feasibility of various attacks.

REFERENCES

Aazam, M., Zeadally, S., & Harras, K. A. (2018). Deploying fog computing in industrial internet of things and industry 4.0. *IEEE Transactions on Industrial Informatics 14*(10), 4674-4682.

Acharjya, D. P., & Ahmed, N. S. S. (2017). Recognizing Attacks in Wireless Sensor Network in View of Internet of Things. In *Internet of Things: Novel Advances and Envisioned Applications*, 149-172. Springer, Cham.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88*, 10-28.

Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C., & Vittal, V. (2005). Causes of the 2003 major grid blackouts in North America and Europe and recommended means to improve system dynamic performance, *IEEE Transactions on Power Systems 20*(4), 1922 - 1928.

Asplund, M., & Nadjm-Tehrani, S. J. (2016). Attitudes and perceptions of IoT security in critical societal services. *IEEE Access 4*, 2130-2138.

Atamli, A. W., & Martin, A. (2014). Threat-Based Security Analysis for the Internet of Things. In *2014 International Workshop on Secure Internet of Things (SIoT)*, 35-43. IEEE.

Bhattacharjee, S. (2018). *Practical Industrial Internet of Things security: A practitioner's guide to securing connected industries*. Packt Publishing. Kindle Edition.

Bledowski, K. (2015, July). *The Internet of Things: Industrie 4.0 vs. the Industrial Internet*. MAPI Foundation. URL: https://mapifoundation.org/economic/2015/7/23/the-internet-of-things-industrie-40-vs-the-industrial-internet

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The Industrial Internet of Things (IIoT): An analysis framework. *Computers in Industry, 101*, 1-12.

Byres, E. J., & Eng, P. (2009). *Cyber security and the pipeline control system*. Lantzville, BC, Canada.

Caselli, M., Zambon, E., Petit, J., & Kargl, F. (2015, March). Modeling message sequences for intrusion detection in industrial control systems. In *International Conference on Critical Infrastructure Protection*, 49-71. Springer, Cham.

Choi, S., Chang, Y., Yun, J. H., & Kim, W. (2015, March). Traffic-locality-based creation of flow whitelists for SCADA networks. In *International Conference on Critical Infrastructure Protection*, 87-102. Springer, Cham.

Contu, R., Middleton, P., Alaybeyi, S., & Pace, B. (2018). *Forecast: IoT Security Worldwide 2018*. Gartner, Technical report.

Corbò, G., Foglietta, C., Palazzo, C., & Panzieri, S. (2018). Smart Behavioral Filter for Industrial Internet of Things. *Mobile Networks and Applications, 23*(4), 809-816.

Cyber attack on a German steel mill. (2016, May 31). *Sentryo*. URL: https://www.sentryo.net/cyberattack-on-a-german-steel-mill/ . Accessed 1 March 2019.

Eigner, M. The Industrial Internet: Engineering processes and IT solutions. In *The Internet of Things: Industrie 4.0 Unleashed*. (ed. U. Sendler). Berlin: Springer, 133-155.

Evans, P. C., & Annunziata, M. (2012). *Industrial Internet: Pushing the boundaries of minds and machines*. General Electric. URL: https://www.ge.com/sites/default/files/Industrial_Internet.pdf. Accessed 28 February 2019.

Filkins, B. & D. Wylie (2018). Endpoints Most Vulnerable Aspect of Industrial IoT. *Software World 49*(4), 21-21.

Forsström, S., Butun, I., Eldefrawy, M., Jennehag, U., & Gidlund, M. (2018, April). Challenges of securing the industrial internet of things value chain. In *2018 Workshop on Metrology for Industry 4.0 and IoT*, 218-223.

Fremantle, P. & Scott, P. (2017). A survey of secure middleware for the Internet of Things. *Peer J Computer Science,* 3, e114.

Fu, J., Liu, Y., Chao, H., Bhargava, B. K., & Zhang, Z. (2018). Secure data storage and searching for Industrial IoT by integrating fog computing and cloud computing. *IEEE Transactions on Industrial Informatics, 14*(10), 4519-4528

Gavin, R. (2018). Cybersecurity for cloud-based SCADA. *Control Engineering, 65*(8), 50-52.

Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. New York: Anchor Books.

Hassanzadeh, A., Modi, S., & Mulchandani, S. (2015, December). Towards effective security control assignment in the Industrial Internet of Things. In *2015 IEEE 2nd World Forum on Internet of Things* (WF-IoT), 795-800.

Hounshell, L. (2018, November 6). Cybersecurity, blockchain, and the Industrial Internet of Things. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/11/06/cybersecurity-blockchain-and-the-industrial-internet-of-things/#556dcefd4eec Accessed 4 March 2019.

How the Dutch foiled Russian 'cyberattack' on OPCW. (2018, 4 October). *BBC*. Retrieved from: https://www.bbc.com/news/world-europe-45747472. Accessed 15 February 2019.

Huberman, B. A. (2016). Ensuring trust and security in the Industrial IoT: The Internet of Things. *Ubiquity Symposium*. Hewlett Packard Labs, 2016(January), 2-9.

Industrial Control Systems Security: Regulations (2017, March 9). Wallix. Retrieved from http://blog.wallix.com/industrial-control-systems-security-ics. Accessed 15 December 2018.

Industrial Internet Reference Architecture v 1.8. (2017). Industrial Internet Consortium (IIC). (2017). https://www.iiconsortium.org/IIRA.htm. Accessed 15 February 2019.

Karlof, C., & Wagner, D. (2003, May). Secure routing in wireless sensor networks: Attacks and countermeasures. In *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, 113-127. IEEE.

Joo, Y. M., & Tan, T. B. (2018). Smart Cities: A New Age of Digital Insecurity. *Survival, 60*(2), 91-106.

Lee, R. M., Assante, M. J., & Conway, T. (2014). German steel mill cyberattack. *Industrial Control Systems, 30*, 22.

Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M., & Kumari, S. (2018). A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things. *IEEE Transactions on Industrial Informatics, 14*(8), 3599-3609.

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy* ***2***(2), 155-184.

Márquez, M. A., Herrera, R. S., Mejías, A., Esquembre, F., & Andújar, J. M. (2018). Controlled and secure access to promote the Industrial Internet of Things. *IEEE Access, 6***,** 48,289 - 48,299.

Mavropoulos, O., Mouratidis, H., Fish, A., & Panaousis, E. (2018. August 23). Apparatus: A Framework for Security Analysis in Internet of Things Systems. *Ad Hoc Networks*.

Mehnen, J., He, H., Tedeschi, S., & Tapoglou, N. (2017). Practical security aspects of the Internet of Things. In *Cybersecurity for Industry 4.0*, 225-242. Springer, Cham.

Mouton, F., Leenen, L., & Venter, H. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security, 59*, 186-209.

Ortiz, E., Reinerman-Jones, L., & Matthews, G. (2016). Developing an insider threat training environment. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity*, July 27-31, 2016, Walt Disney World, Florida. Springer International Publishing, 267-277.

Peng, X., Zhu, P. D., Zhu, Y. F., Hu, P. S., & Cui, Yan, C. Z. (2017). Command disaggregation attack and mitigation in Industrial Internet of Things. *Sensors, 17*(10), 1-24.

Presidential Policy Directive 21. (2013) *Critical infrastructure security and resilience*. Washington, DC: The White House Office of the Press Secretary.

Reed, T. C. (2005). *At the abyss: an insider's history of the Cold War*. Presidio Press.

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. (2018, March 15). United States Computer Emergency Readiness Team (US-CERT) Alert (TA18-074A). Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-074A

Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. Design Automation Conference (DAC), *2015 52nd ACM/EDAC/IEEE*, IEEE, 1-6.

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access 4*, 1375-1384.

Serpanos, D., & Wolf, M. (2018). Security and safety. In *Internet-of-Things (IoT) Systems*, 55-76. Springer, Cham

Shetty, M. M., & Manjaiah, D. H. (2017). Challenges of distributed storage systems in Internet of Things. In *Internet of Things: Novel Advances and Envisioned Applications*, 193-204. Springer, Cham.

Trautman, L. J. & Ormerod, P. C. (2018). Industrial cyber vulnerabilities: Lessons from Stuxnet and the Internet of Things. *University of Miami Law Review, 72*(3), 761-826.

Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015). On the security and privacy of Internet of Things architectures and systems. In *2015 International Workshop on Secure Internet of Things* (SIoT), IEEE, 49-57.

Willner, A. (2018). The Industrial Internet of Things. *Internet of Things A to Z: Technologies and Applications*, 293-318. Springer, Cham.

Yazdinejad, M., Nayyeri, F., & Afshari, N. (2017). Secure distributed group rekeying scheme for cluster based wireless sensor networks using multilevel encryption. In *Internet of Things: Novel Advances and Envisioned Applications,* 127-147. Springer, Cham.