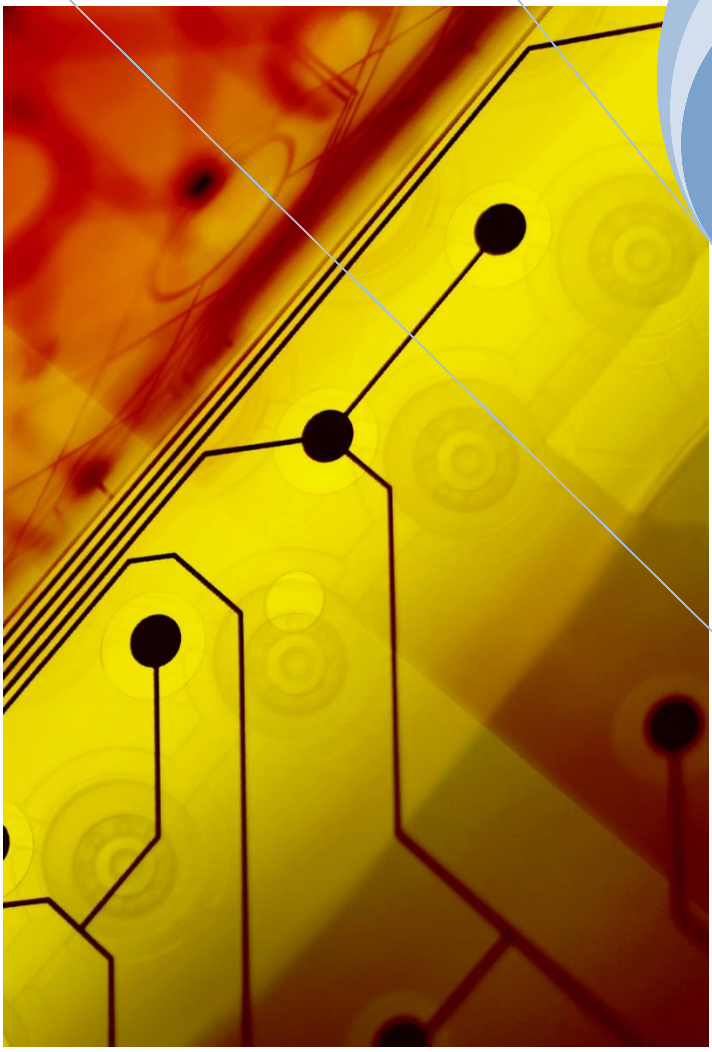

The Risks of IIoT in Industry 4.0

27-Jan-20

Introduction

“Industry 4.0" can take different definitions as things usually do when they are still taking form. However, all of them usually encompass key features such as the utilization of large scale interconnectivity that is defined as Internet of Things (IoT) and Industrial Internet of Things (IIoT), Artificial Intelligence (AI) including machine learning and large data processing and/or data mining [1][2][3]. This can be characterized by a business that can track all its manufacturing statistics (e.g. unit production rate, defects, maintenance problems and delays), supply chain information and variables and even marketing and sales data all at the same time and dynamically change operation parameters of the business such as supply or price adjustment and ordering of parts or raw materials. This is usually supported by a cloud computing infrastructure and machine learning to predict trends from analysis of this data in real-time to leverage a business and/or product in the market [1][4][3]. They have been proven to reduce production costs and revenue by increasing equipment life up-time and availability all while improving product quality and factory safety [5] . The large-scale interconnectivity of IoT and IIoT is integral for Industry 4.0 but it also introduces cyber security risks. Simply put : the more interconnected a system is , the more vulnerable it is to cyber attacks [6]. A cyber attack is when a party maliciously gains access to or alters a network/system either by direct access to it or through the internet and can be either targeted (e.g. there’s an intended target network or system) or untargeted (e.g. attacks systems and/or networks indiscriminately)[7].

The Risks of IIoT

The interconnection of IIoT is made possible by large networks of sensors/actuators, data storage and processing and user interfacing[8]. All of this creates a dynamic system called a Cyber-Physical System (CSP) which is described as the core of Industry 4.0 [9]. All the attacker has to do is gain access to one device in a subsystem to affect it and if the subsystem is not secured enough this can spread to other sub-systems until they control crucial parts in the system.

IoT is inherently vulnerable to this because its philosophy dictates high interconnectivity. The most common types of cyber attacks are [10]:

- Botnets:
  This is when an attacker takes control of a device through malicious code and can use it as a part of other cyber attacks such as large scale attacks or simply as an access point to a system by running code on it and using its access privileges.
- Denial of Service (DoS):
  This is when an attacker uses a large number of controlled devices to send large numbers of requests to a server or service point overwhelming its buffers, effectively hampering it’s ability to serve legitimate users.
- Man-In-The-Middle:

This is when an attacker gains access to the communication channel between 2 or more devices. This allows the attacker to do anything from stealing information to changing the data sent masquerading as one of the devices being communicated with.

- Advanced Persistent Attacks (APTs):
  The attacker gains access to the network or sub-system undetected and steals crucial data or alters the system for extended periods of time. It is one of the hardest threats to prevent or resolve because the system might not even be recognized as compromised.
- Ransomware:
  The attacker takes control of a sensor or actuator and affects its behavior whilst blocking control over it from the operator and demanding, effectively holding the business for ransom. For example affecting a smart thermostat and raising the temperature. A more common type is to encrypt crucial data and hold the business ransom for the decryption key.

All these can be used to alter manufacturing machines affect production management systems by compromising a single sensor or actuator or device[11][10].

IoT devices in particular suffer from lax security standards. They do not go under the same certification scrutiny as routers , servers or even personal computers, with little to no software updates and often without a way to restrict connections to it (a firewall), so exploits are too common[12] and the attacker often needs only one working exploit to compromise a device. This provides a difficult threat to deal with , since a lot of these devices are embedded systems and cannot be secured with a simple update if such an update even exists often being proprietary systems [12]. The threat is further compounded by the fact that most of these small devices do not have the processing power to implement advanced encryption methods , making their communication traffic extremely vulnerable , especially to Man-In-The-Middle attacks[13][14].

The threat of these attacks is neither young nor small. One of the first successful attacks on an IIoT system was on American nuclear power plants where the “Slammer” worm infected two critical monitoring systems in 2003 [13]. Another infamous incident in America is when a virus was used to infect signal and dispatching control systems of a major transportation services system leading to a major halt of operations of freight trains as well as many other incidents reported in literature [13].

Solutions

Ultimately, the benefit of Industry 4.0 is too attractive for businesses to forgo, so the risks must be dealt with or the economic threats can be detrimental. Estimated losses are in the range of 30 billion and 1 trillion USD with the damage to private data being hard to quantify [15]. The obvious answer to the largest chunk of the threat is to simply put better security standards for IoT devices, especially ones used in crucial roles. A variety of secure platforms have been proposed that already exist such as Intel Software Guard Extensions which introduces security related instructions such as encrypting data even in internal chip data transfers and Trusted Platform Module which is a chip that is added to a device that performs those same functions in a more isolated fashion (being a separate chip) [16][17]. These platforms and more along with multifactor authentication [18] can fulfill security roles without adding processing load and violating real-time processing constraints [13]. For a simpler solutions there is already attempts to provide encryption algorithms with low processing loads for small IoT devices that may not support such platforms using simple XOR-ing [14]. There is also large research efforts being conducted such as the 12.5 million USD security project NZD and the newer project STRATUS aimed at creating security tools to protect cloud and IoT devices [19]. It seems that the industry's trend towards heavy use of IoT is inevitable and so are its impending risks. However, security technologies are bound to adapt along with the industry.

Works Cited

[1] "What is Industry 4.0 | Epicor UK." [Online]. Available: https://www.epicor.com/en-uk/resource-center/articles/what-is-industry-4-0/. [Accessed: 25-Jan-2020].

[2] "What is the Internet of Things? WIRED explains | WIRED UK." [Online]. Available: https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot. [Accessed: 27-Jan-2020].

[3] "Industry 4.0, IoT in Digital Manufacturing, creating smart factories | BearingPoint United Kingdom." [Online]. Available: https://www.bearingpoint.com/en-gb/hot-topics/industry-4-0-and-iot-hot-topic/. [Accessed: 27-Jan-2020].

[4] "Industry 4.0 and Industrial IoT in Manufacturing: A Sneak Peek - Aberdeen." [Online]. Available: https://www.aberdeen.com/opspro-essentials/industry-4-0-industrial-iot-manufacturing-sneak-peek/. [Accessed: 27-Jan-2020].

[5] "6 Important Industry 4.0 Statistics to Know." [Online]. Available: https://blog.flexis.com/6-important-industry-4.0-statistics-to-know. [Accessed: 25-Jan-2020].

[6] "Technological Interconnectivity Increases Exposure to Cyber Risks | ERM Software." [Online]. Available: https://www.logicmanager.com/erm-software/2016/05/31/technological-interconnectivity-cyber-risks/. [Accessed: 27-Jan-2020].

[7] "How cyber attacks work - NCSC." [Online]. Available: https://www.ncsc.gov.uk/information/how-cyber-attacks-work. [Accessed: 27-Jan-2020].

[8] "IoT Explained - How Does an IoT System Actually Work? | Leverege." [Online]. Available: https://www.leverege.com/blogpost/iot-explained-how-does-an-iot-system-actually-work. [Accessed: 27-Jan-2020].

[9] "Cyber-Physical Systems - a Concept Map." [Online]. Available: https://ptolemy.berkeley.edu/projects/cps/. [Accessed: 27-Jan-2020].

[10] "8 types of security threats to IoT | IoT security threats |," 2019. [Online]. Available: https://www.allerin.com/blog/8-types-of-security-threats-to-iot. [Accessed: 25-Jan-2020].

[11] "4 Risks of IoT in Manufacturing | Travelers Insurance." [Online]. Available: https://www.travelers.com/business-insights/industries/manufacturing/4-risks-of-iot-in-manufacturing. [Accessed: 27-Jan-2020].

[12] "The Internet of Secure Things – What is Really Needed to Secure the Internet of Things? | Icon Labs." [Online]. Available: https://www.iconlabs.com/prod/internet-secure-things-—-what-really-needed-secure-internet-things. [Accessed: 25-Jan-2020].

[13] A. R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proceedings - Design Automation Conference*, 2015, vol. 2015-July.

[14] A. Esfahani *et al.*, "A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019.

[15] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth¨, "Economic Impact of IoT Cyber Risk-Analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance."

[16] “Intel® Software Guard Extensions | Intel® Software.” [Online]. Available: https://software.intel.com/en-us/sgx. [Accessed: 27-Jan-2020].

[17] “What Is a TPM? How This Chip Can Protect Your Data | Laptop Mag.” [Online]. Available: https://www.laptopmag.com/articles/tpm-chip-faq. [Accessed: 27-Jan-2020].

[18] M. W. Condry and C. B. Nelson, “Using Smart Edge IoT Devices for Safer, Rapid Response with Industry IoT Control Operations,” *Proc. IEEE*, vol. 104, no. 5, pp. 938–946, May 2016.

[19] R. Nelson, “Future trends in IM: Industrial strength security,” *IEEE Instrumentation and Measurement Magazine*, vol. 22, no. 6. Institute of Electrical and Electronics Engineers Inc., pp. 33–34, 01-Dec-2019.