Security in the Industrial Internet of Things

Josiah Anderson
University of California, Riverside

Keith Zmudzinski
University of California, Riverside

Abstract

The Industrial Internet of Things is a unique type of distributed system that must contend with integrated systems, constrained scalability, and maximizing dependability, which includes security. Because the IIoT fuses the cyber and physical worlds as an integral part of its architecture, it must contend with a wide range of possible attacks, both physical and virtual. SCADA systems also suffer from a set of attacks unique to them, and as such much take specific precautions against them. Indirect attacks on large scale services are possible through the use of low-powered devices, such as controlling power demand in electrical grids through hijacking in-home appliances. Producers of IoT platforms must ensure they have taken sufficient security safeguards, not doing so gives rise to the possibility of large scale IoT attacks, such as with the Mirai Botnet. As the IIoT becomes more mainstream, its security flaws and their possible remedies must be studied and addressed in order the platform stable and the general public safe.

1 Introduction

The Industrial Internet of Things is an emerging area of distributed computing and industrial control systems that is certain to impact the daily lives of citizens of advanced industrialized nations. Unique challenges are presented by this new area, and we aim to discuss these challenges with a specific focus on security perspectives. We discuss first why Industrial IoT are distributed systems, and the unique challenges that come along with them. We discuss a survey of attacks and possible countermeasures, as well as empirically-driven risk modeling for SCADA systems heavily employed in Industrial IoT systems. We discuss theoretical attacks on power grids using high-wattage appliance IoT botnets, and tie this into discussion of recent DDoS attacks by large scale IoT botnets.

2 Industrial IoT as Distributed Systems

Industrial IoT (IIoT) represents a specialized kind of distributed system. Iwanicki [1] identifies three crucial issues affecting the adoption of Industrial IoT as *interoperability*, *scalability* and *dependability*. Industrial IoT systems are collections of interconnected devices monitoring or controlling physical resources in a way that appears as a single system, which fits the classic definitions of distributed systems [1].

IIoT can be defined in three layers: data storage, application logic, and *sensing and actuation*. The third layer represents the embedded devices which interact with physical objects and are of limited resources, may also be exposed to elements, may be highly heterogeneous, and have great variety of physical placement. These properties make them unique from traditional distributed platforms.

Interoperability. Industrial IoT systems are often integrated into already existing infrastructure systems and components, some of which may be legacy systems. *Standardization* is one approach, but has seen only partial success, with standards only partially implemented. *Middleware* for IIoT is limited by different industries having sometimes vastly different requirements and needs.

Scalability. *Size scalability* in IIoT is difficult with device placement often being fixed and tight constraints on device resources. Solutions to geographic scalability such as replication, asynchronous communications, local caching and eventual consistency are rarely feasible in the sensing and actuation layer, in part due to low-powered wireless devices. *Administrative scalability* solutions, such as virtualization and cloud computing, are improbable where entities share physical space, sensors and actuators, and communication bands or channels.

Dependability. Maximizing *reliability* of components is difficult due to resource constraints, preventing virtualization, sandboxing, or advanced monitoring. Redundancy is hampered by limited communication, realtime requirements, and precisely defined device points. *Safety* in IIoT must ensure failures do not have catastrophic results that put people or infrastructure at risk. *Availability* may be highly limited, from inability to have physical redundancy of hardware/software systems. *Maintainability* is challenging for essential services that require continuous uptime. *Security* is challenged by the limited nature of devices, such as lack of secure communication protocols.

Industrial IoT systems pose a number of unique challenges from a distributed systems perspective. They have to inter-

operate with existing infrastructure and heterogeneous platforms, scale orders of magnitude, be managed by different entities, while being dependable, safe, available, maintainable and secure.

3 Industrial IoT Attacks and Countermeasures

The Industrial Internet of Things comes from a fusion of Operation and Information technology. As such, it assumes the risks and vulnerabilities of both. This results in a technology platform that inherently assumes a high level of risk. In an attempt to ameliorate the dangers posed to IIoT devices, Panchal, Khadse, and Mahalle [2] delineate the layers of IIoT architecture and associated vulnerabilities, discuss possible attacks and countermeasures, and produce an attack taxonomy to assist in the prevention and diagnosis of IIoT attacks.

IIoT attacks pose varying levels of threat depending on at which level in the IIoT architecture an attack is introduced. Accordingly, we need to discuss the different security concerns for each level in the IIoT architecture. There are five basic levels to consider, in increasing levels of abstraction.

1. The low level devices that interact with physical components, such as actuators and motors.
2. Distributed Control Systems, Programmable Logic Controls, and Gateways; the devices that interact with those devices in level 1.
3. SCADA and Human Machine Interfaces.
4. Intranet and Web services, as well as other applications used for on site business.
5. Enterprise level applications, Cloud computing, and Data analytics.

We now briefly list five different IIoT attacks and countermeasures, each of which are effective at different levels of the IIoT architecture, as listed above.

1. Brute Force: Attackers attempt to sign-in using combinations of common login information. Setting up non-default passcodes can help stop such attacks.
2. Man-in-the-Middle: Attackers intercept and modify communication between devices. Using mutual authentication can help prevent this.
3. IP-Spoofing: An attacker forges an IP address to impersonate another device. Not using the IP Industrial protocol, which identifies devices by IP, can help.
4. Remote Code Execution: When an attacker introduces malware to control the system remotely. Common malware prevention techniques may prevent such attacks.
5. DoS: Network bandwidth is targeted to bring a service down. Using DoS prevention systems that utilize Intrusion Detection Systems may help prevent such outages.

Due to the wide range of possible attacks against IIoT devices, it is useful to have a classification strategy to manage the varying characteristics of these attacks. Panchal, Khadse, and Mahalle created such a taxonomy, based on four features: Attack Vector, Attack Target, Attack Impact, and Attack Consequence. Under each category, it is further broken down into either Cyber, or Physical.

We see that the number of potential attacks on IIoT devices is overwhelming, as it not only must contend with traditional cyber attacks, but physical ones as well. We believe this incentivizes collaboration between security experts from Information and Operational technology, to better safeguard against IIoT attacks. While this enumeration of possible attacks and the created taxonomy certainly doesn't cover all possible attacks, it does provide a beneficial framework for those that are either planning for the prevention of attacks, or are in the midst of recovering from one.

4 Security Risk Modeling for IIoT SCADA Systems

Cyberattacks can disrupt and disable Industrial IoT devices comprising critical infrastructure. In 2015 an attack was launched on Ukraine's power grid, disabling power and causing rolling blackouts for 225,000 Ukrainians [3]. Falco, Caldera, and Shrobe [3] provide a risk analysis of vulnerabilities and exploits in SCADA systems using statistical methods. There is a trend of connecting SCADA-based IIoT systems to IT networks. Regulatory bodies in the US have mandated reliability standards, but up to 75% of companies have been able to opt-out with others preferring to pay fines [3].

The MITRE Corporation maintains a database of CVEs to track known software vulnerabilities, and each CVE has a CVSS score. MITRE also maintains a database of CWEs, which classify CVEs by type. Many of these risk scoring systems fail to consider empirical evidence. The authors note a lack of SCADA specific concrete recommendations.

The authors contend that CVSS metrics are strongly correlated with SCADA exploit risk. Collating the DHS' ICS-CERT databases with MITRE's CVE systems allowed for SCADA CWE density to be calculated, along with web-scraping actual exploits. These were used to calculate exploit density per CWE, CVE density per CWE, average impact score, and average exploitability score. A SCADA prioritization schema includes the top CWEs by vulnerability density, exploit density, exploitability score, and impact score.

Results from exploit density reveals buffer overflows as having the greatest risk, followed by path traversal, improper input validation, access controls and code injection. Multiple regression models showed a strong relationship between the presence of an exploit and the number of vulnerabilities, average impact score and exploitability score. The results indicate that SCADA CWE frequency and exploitability and impact scores' relationship with exploit density is unique. This could indicate that complex CVSS scores are a flawed indicator of risk.

Manufacturers of SCADA IIoT systems should "design out" the top vulnerabilities where possible. Buffer overflows can be remedied by modern memory safe languages such as Rust. Input validation should be designed into the system. Information exposure may be the most difficult to "design out", relying on human elements.

Falco, et al., [3] has found that SCADA IIoT systems as a subclass have exploits targeting distinct vulnerabilities from non-SCADA systems. They also identify highly correlated relationships between some vulnerability metrics and density of SCADA exploits. Security researchers, SCADA IIoT designers, and SCADA operators should focus on core sets of vulnerabilities specific to SCADA, based on this paper's empirical, data-driven findings

5 High Wattage IoT Botnets Can Disrupt Industrial Control Systems

Power grid security standards are based on the assumption that the power demand can be predicted reliably on an hourly and daily basis, based on past and current conditions. With the ubiquity of IoT devices and their poor security measures, Soltan, Mittal, and Poor show this is no longer a safe assumption [4].

Electric power is produced by generators and transmitted via high-voltage transmission networks, or power grid, to industrial and residential consumers. Stable operation of the power grid relies on the balance of supply and demand. The speed of power generators corresponds to the frequency of output. When demand exceeds supply, the turbine rotation decelerates dropping frequency, and vice versa. Changes in frequency cannot be tolerated for long, as low frequencies damage generators. Frequency values beyond certain thresholds trigger relays which disconnect the generators. Power lines have a certain capacity of power that can be carried safely, and unpredicted loads can cause breakage or relays to be tripped. Voltage collapse occurs when supply becomes inadequate, causing outages in the grid. Failures in even a few lines or increased demands may result in large scale outages.

Assuming an adversary with an IoT botnet of high wattage appliances in a region, arbitrary changes in grid demand are possible. Even a fraction of smart thermostats, air conditioners or water heaters could generate very significant demand. These attacks are referred to as Manipulation of the Demand via IoT (MadIoT).

Possible variations of these attacks are as follows. **Significant frequency drop / rise** occurs when switching on all compromised devices, and the resulting increase tripping relays resulting in blackouts. Suddenly decrease may also have the same effect. A **stealthier variation** could be launched by redistributing loads in the system through increasing demand in some locations and decreasing demand in others, keeping total load constant so as not to attract attention from grid operators. Tie-lines connect two independent grids to one another often as part of exchange programs. Failure in one of these lines may result in a huge power deficit and most likely a blackout. **Tie-line attacks** can target near-capacity tie-lines through monitoring grid operator websites. Adversaries can launch attacks aimed at increasing the operating cost by increasing demand, where ancillary services must be purchased at higher prices.

MadIoT attacks are very hard to detect and disconnect by grid operators. This occurs because the breaches are on IoT devices and not on the power grid, with operators seeing only aggregation of distributed changes in demand. *MadIoT attacks are easy to repeat*, allowing for persistent blackouts. *The attacks are black-box*, requiring no knowledge of the topology or detailed properties of the grid. Finally, *power grids are not prepared to defend against them*.

Preliminary suggestions made by the authors on the *power grid* side include ensuring systems have spinning reserve and extra line capacity, accurate estimates of total high-wattage IoT devices, and securing available online data revealing critical information. Security suggestions on the *IoT side* recommend coherent security measures for IoT devices.

The authors note that their study has only used publicly available data which may not account for all factors. Another complication is that it may be more difficult to establish botnets in geographically restricted locations, which is required for such an attack.

6 Real World Example: The Mirai Botnet

In 2016 the Mirai botnet performed widespread IoT based attacks on several high profile targets, including Krebs on Security, Dyn, and Lonestar Cell. Mirai was not a particularly sophisticated attack, it simply took advantage of the lack of security fundamentals pervasive throughout the IoT community. Mirai performed a basic dictionary based attack on low level devices. It chose 10 random login credentials from a hard-coded list of 62, then after gaining entry, began searching for more devices to infect, and so spread exponentially. While the researchers of this paper[5] provide an

incredibly detailed analysis of the factors that contributed to the spread of Mirai, we focus on those most related to distributed systems: the geographic scale of infected devices, and the inability to push updates to many of the infected devices.

The Mirai botnet infected devices mostly concentrated in South America and Southeast Asia, but in total reaching a global scale across many borders and jurisdictions. This led to a plethora of difficulties when trying to coordinate defenses and fixes for the attack. Geographic scaling is generally a desirable quality in distributed systems, however, we see here that it can also be a considerable hurdle to defending against distributed attacks. Another significant stumbling block to slowing the spread of Mirai was the inability of developers to push fixes to many already deployed IoT devices. Due to the nature of these low-powered, single function devices, many simply didn't have the capacity to receive software updates for protection against Mirai, and so even if a fix was produced, there was no way to distribute it.

The Mirai botnet is a perfect example of the dangers IoT and IIoT systems are capable of introducing to the world. Distributed attacks are difficult to defend against, in part because of their large geographic distribution that can make coordination between teams and across jurisdictions difficult, as well as the limited capacity of IoT devices, that can hinder the deployment of security patches.

It may be beneficial to devise a standardized security classification system for these IoT devices, so as to allow the consumer to make a better informed decision about the kinds of security risks they may be taking. For large scale IoT platforms, we could consider mandating the security level used for their IoT devices, since if these devices are compromised, it doesn't hurt solely that platform, but instead can impact the general public. The rampant lack of security mixed with the increased attack possibilities to IoT devices must force us to look more closely at how we as a community can mitigate future attacks.

7 Conclusion

The rise and expansion of the Industrial Internet of Things has created a myriad of complicated issues that must be dealt with carefully and thoughtfully. Due to the limited nature of its devices, as well as the architecture of Industrial IoT itself, the security challenges presented are both varied and unique. The fact that these devices and architectures are often employed in critical infrastructure and services raise the stakes further. As we can observe from past attacks, attacks against IIoT have the potential to cause increasingly major disruptions in essential services, as more companies and utilities come to integrate their platform with Industrial IoT. The need for robust security design and implementation will only increase in the future.

References

[1] K. Iwanicki."A Distributed Systems Perspective on Industrial IoT," 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2018, doi: 10.1109/ICDCS.2018.00116

[2] A. C. Panchal, V. M. Khadse and P. N. Mahalle, "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 2018, pp. 124-130, doi: 10.1109/GCWCN.2018.8668630.

[3] G. Falco, C. Caldera, and H. Shrobe, "IIoT Cybersecurity Risk Modeling for SCADA Systems," 2018 IEEE Internet of Things Journal, Vol. 5, No. 6, December 2018.

[4] S. Soltan, P. Mittal, and H.V. Poor, "BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid," In 27th USENIX Security Symposium, 2018.

[5] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas and Yi Zhou. "Understanding the Mirai Botnet". In 26th USENIX Security Symposium, 2017.