EXOSITE

USA Headquarters
275 Market St, Suite 535
Minneapolis, MN 55405
+1.612.353.2161

Taiwan Office
WenXin Road, Section 4
#955, 15F-5
Taichung, 406 Taiwan
+886.4.2247.1623

Best Practices to Build a Pragmatic Security Strategy for Industrial IoT

WHITE PAPER

Released: April 2017

Authors: Mark Benson & Rob Viren

Revision: A

Table of Contents

> “A modern, pragmatic approach to IoT security must involve strategies that pull from both technology and culture equally to be effective.”

1. Introduction

Technology has always been a step ahead of the culture that develops it. Cars existed long before roads, safety standards, and laws governing driving came into being. Similarly, Internet of Things (IoT) security continues to make technological improvements in leaps and bounds, while the culture critical to successful (and secure) usage lags behind.

At the same time, IoT has spread beyond relatively benign consumer products and into large industrials. The insight, conveniences, and power of the industrial Internet has drawn in thousands of mission-critical assets and systems. With the increased power comes the increased risk associated with Internet-connecting multi-million dollar equipment capable of causing harm to personnel and other systems. IoT companies now have to consider security as synonymous with safety when dealing with industrial equipment where device-state changes can have devastating impacts to systems and people.

As industrial applications continue to see high rates of IoT adoption, the human element will play an increasingly important role in security alongside technology. The management of users, permissions, relationships, data breaches, and insider adversaries present a special and unique risk to systems even when they implement the most secure device-level communication. In reality, any system can and will be compromised. As bleak as this may sound, this understanding can help organizations develop an approach to IoT security that seeks to protect against, deter, detect, contain, and minimize the impact of hacking attempts.

A modern, pragmatic approach to IoT security must involve strategies that pull from both technology and culture equally to be effective. This white paper discusses how a comprehensive security strategy first begins with an in-depth understanding of the technology concepts that are key to IoT security. Next, it provides examples of how proven technology approaches can be used together to provide defense in depth. Finally, this white paper identifies the core cultural values that must be in place to support technology components to develop a well-rounded, effective approach to IoT security.

2. The Core Technology Concepts of IoT Security

One of the first steps in developing a comprehensive security strategy is understanding the core technology concepts in the realm of IoT security—data, control, and hardware. Developing an understanding of these concepts can help organizations learn how to better prevent attacks, mitigate impacts, and recover from attacks on IoT systems. This section will explain these concepts in more depth and provide insight to consider when contemplating security for each.

2.1 Data

Data is the currency of IoT solutions—it is the thing we collect, process, analyze, and use to identify and control users, behaviors, and environments. To secure data, it is useful to think about it in three contexts: data at rest, data in motion, and data in use.

2.1.1 Data at Rest

Data at rest is data that is stored on a hard drive, in a database, in flash memory, or in RAM. Data that is customer-private should always be encrypted so that if attackers gain access to a database, they cannot understand the information. Other data, like analog sensor data, may or may not be important to encrypt depending on the application. Of particular importance is the embedded system that may or may not have encrypted flash. Some microcontrollers also allow a fuse to be blown at manufacturing time to disable another user from reading the contents of flash or re-programming it with their own software. These are all mechanisms to protect data at rest.

2.1.2 Data in Motion

Data in motion is data sent from a sensing device over a wired or wireless network, like Wi-Fi, public Internet, or cellular. For this context, it is important to make sure an attacker is not able to listen in on communications and understand what data is being sent. This is especially important for private customer data, but it is also important for machine data in many use cases. Each delivery mode should be carefully analyzed for any IoT solution.

2.1.3 Data in Use

Data in use is data accessed by a user, machine, or web service with particular permissions that others do not have. For instance, a facilities engineer responsible for keeping an HVAC system up and running may have access to see data for their facility, but may not have permission to see another facility. Even more importantly, non-authorized personnel must not have access.

2.2 Control

Control refers to a special piece of data designed to change the state of a device. Control plays an important role in IoT security, as it bridges the gap between the abstract Internet and reality, where a connected device can have physical impact on the world around it. However, simply connecting a device to the Internet does not make it vulnerable. Devices have firmware that hard-codes the intended functions and cannot be easily changed by hackers. Similarly, the Internet cannot interfere with physical readouts of gauges on IoT-enabled industrial components.

However, an industrial component that can be controlled through the Internet must be treated as special and unique. All aspects of data, network, and hardware along the path of control to an industrial device must be scrutinized constantly. A healthy questioning attitude regarding any work done on systems connected to industrial components is important, and maintaining configuration control within a system must take higher priority than making device-state changes easy. As such, a properly designed system will limit user permissions for control of a component only to critical users.

2.3 Hardware

End-user hardware, customer hardware, network hardware, and third-party hardware all play a role in the IoT game, and each have similar impact when considering IoT security. As a result, no cloud company truly exists free of hardware. The employees who code, provide support, and work for the company, the users that connect to the platform, and the servers that host their content all exist in real, physical ways. No matter what kind of computer system an IoT company uses, people will always interact with it in some physical way. The technology to secure hardware continues to mature, to prevent more attacks, and to provide more secure connections between systems; however, the people connected to these advanced machines continue to present the biggest vulnerabilities.

A healthy security culture—a concept that is addressed in greater depth in Section 4—encourages individuals to both understand the capacity they have to make components of a system vulnerable to attack and the sense of responsibility they should have in ensuring the security of that system.

3. Defense in Depth

Another consideration when developing a pragmatic IoT security strategy is to layer proven security technologies to create a depth that yields better results and deters more hackers. The concept of defense in depth comes into play when considering how hackers typically begin—not by suddenly gaining access to critical data and control, but instead through incremental steps in which they throw the widest net possible to find the most vulnerable systems. For example, the Verizon 2016 Data Breach

Investigations Report found that the average attack took days, not minutes.[1]

In response to this known behavior, a series of strategies can be used to respond to attackers at each step of their process to minimize the impact of hacking events: engaging in proactive activities to facilitate prevention, architecting systems for risk mitigation, leveraging the best technology to secure identities, and establishing processes to protect data and control in its many forms. The sections below discuss these strategies that are designed to address some of the most common vectors of attack.

3.1 Proactive Response

Innovative, proactive strategies have been devised to deal with the inevitability of successful intrusion. Some methods use social engineering against hackers that attempt to access sensitive data and control devices. One method involves creating a sandboxed, controlled environment that mirrors a real one. A fake employee is created that clicks on all phishing links, appears to have maximum authorization in the system, and has fake sensitive information. Hackers will take the bait of a completely valid-looking and vulnerable account, but will only be able to access the sandboxed, controlled environment. As a result, an organization can monitor and develop a better understanding of hacking behavior, methods, and motives.

Another method leverages the fact that hackers often look for API vulnerabilities and rely on successful malware to gain access to servers. Technology has been developed to create fake, insecure endpoints that lead hackers again into a controlled environment where malware can be run with no risk to the actual servers. Showing vulnerability and hosting malware can lower the chance a hacker will end up on a real system.

The most proactive response to an attack relies on early detection. When malware is detected quickly, it can be isolated or deleted to prevent attackers from scanning networks for other credentials, spreading malware to other computers, or finding sensitive information. If a hacker gets by the traps, a network must be in place that is configured to monitor unusual network activity and frequently scan hardware for malware. Accurate logging of information within an IoT application can also make it easier to track

[1] Verizon 2016 DBIR

strange behavior—without logging, it becomes impossible to know what happens within a system and makes early detection more difficult.

A strong questioning attitude is also a key part of a proactive response—workers and users should feel empowered to ask questions and report odd behavior from applications and hardware. New applications suddenly installed, strange emails from unknown persons, and login records at incorrect times all hint at activity that is outside the norm that should be reported and investigated.

3.2 Security by Design

When considering IoT security, there are several methods that can be used in the design of a system to prevent and deter hacking events. A surefire method to prevent an intruder from controlling critical assets is to structure an architecture that does not allow for control functionality. A one-way street allows an organization to benefit from the data collected without the risk of loss of control. A flexible IoT platform should allow device configurations that support both control and data-production-only capabilities. This type of flexibility allows an organization to tune the level of security to their IoT application, minimizing risk and maximizing the benefit.

User and permission management forms another critical pillar in securing IoT applications. It should be assumed that one or more user accounts will be hacked. Distributing and isolating permissions as much as possible lowers the risk profile of an attacker gaining access to critical assets. Some organizations have gone as far as to have no single user with root access to control over accounts. Of course, this makes it more difficult to give permissions, change them, and manage them, so the drawbacks have to be weighed against the level of risk associated with an attacker gaining access.

Virtualization of an application can also be used to make it significantly more difficult to cripple a network. Hosting applications in virtual environments distributes the risk of a platform to many instances of a single program. This means that even if hackers can cripple or gain access to a single virtual machine (VM), the functionality of the system at large is not compromised. Similarly, VMs can be destroyed without significant ramifications. The destruction of a VM that does not persist data can essentially reset the system to a known configuration. Virtualization and distributions of functionality complicate the options available to attackers and assists in deterrence.

3.3 Securing Identities

Taking steps to secure the identities of system users is a critical step in IoT security. Implementing a properly managed two-factor authentication system requiring a U2F key, or other technology, can create a solid technical barrier in front of would-be hackers looking to control a device or gain access to data through phishing and other social engineering scams. Passwords and authentication can seem abstract to those unfamiliar with technology, but the concept of a U2F key compares closely to the idea of house and car keys in protecting your most important assets.

It is important to keep in mind, however, that good security does not always equate to a good user experience. Although requiring two-factor authentication for every application would be more secure, it can be cumbersome for users. Again, this balance must be considered based on the level of risk associated with the device connected to the platform. Flexible options for a two-factor authentication application can enable users to succeed without being too prescriptive in risk evaluation. The authentication can be cached and recognized on a single device or there could be a timeout for the authentication. Of course, these options increase the opportunity for a hacker to gain access, but the risk of having an unusable application could outweigh the risk of the connected device.

Two-factor authentication also does not solve all issues, as the manner of implementation can have a significant impact on the level of security this method provides. The demands of a good user experience can require that a security token is valid for as long as 12 hours, which gives attackers a rather long window of opportunity if they gain access to user credentials and a temporary key. And, answers to question verifications like “What was the name of your first pet?” or “Where was your first job?” can often be looked up by a motivated attacker. Depending on the level of risk associated with a solution, it may be useful to consider other options like text verifications and phone-based authentication apps that provide significantly better protection than security questions.

3.4 Governance, Risk Management, and Compliance

Governance, risk management, and compliance (GRC) represent the components of process control within an organization that can play an important role in IoT security. Process should dictate the activities of workers within an organization, and workers should have governance to ensure compliance with company and regulatory processes. Processes specific to IoT security must be developed and applied within an organization according to the level of risk associated with the connected product and the process itself. For example, issuing permissions for the control of important assets should have higher governance than issuing permissions for access to view data. A well-defined process, that undergoes constant improvement and users are trained adequately on, gives people the best opportunity to perform tasks successfully and securely with the intended outcome.

Organizations implementing IoT should focus on process for all security-critical functionality within the organization. The quality assurance process, the reviewing of security, and the hiring process should all be subject to constant scrutiny. The review of and improvement of processes leads to better outcomes overall. As such, process control and improvement should be a central focus.

4. Core Cultural Concepts of IoT Security

The previous sections covered some of the core technology principles of an IoT-security-focused organization. This section will focus on an equally important, yet often overlooked, aspect of a comprehensive IoT security strategy—the company culture and values that must be in place to support the technology components of IoT security.

4.1 Principles for a Strong IoT Security Culture

This section outlines the principles of a strong IoT security culture, which owe their inspiration to an industry that has successfully put safety and configuration management at the center of its focus for more than 40 years—nuclear power. The Institute of Nuclear Power Operations (INPO) nuclear safety culture principles, which have been field tested in real-world conditions, provide a close parallel to the importance of control in industrial IoT applications and helped guide the creation of the seven principles that follow.

1. **Everyone is personally responsible for IoT security:** Workers, users, and coders feel personally responsible for the safety and security of devices connected to a network. Every stakeholder takes the time to evaluate their impact on the security of the system and, those who can, design in safeguards when possible to protect against and minimize the potential impact of attackers.
2. **Leaders demonstrate commitment to IoT security:** Leaders within organizations frequently mention security, sometimes as a stand-alone topic. They make time to train users and workers about the importance of security and the potential impacts of being an organization that is connected to an IoT platform. Leaders show, both verbally and by action, that security is a top priority.

3. **Decision-making reflects IoT security first:** Security should be central to the delivery of an IoT product. All decisions made in regard to the IoT platform should prioritize security over the delivery of feature requests. When necessary, security should take priority over usability based on the level of risk associated with a data or control breach of the IoT application.

4. **IoT is recognized as special and unique:** Companies that work with IoT should understand the seriousness of the devices and systems attached to the network. Identities, permissions, and user management should be treated with the utmost care and scrutiny. State changes of a device attached to an IoT application should be treated with the highest level of security possible.

5. **A questioning attitude is cultivated:** Workers should feel empowered to ask questions of any aspect of a system they work with. They should feel encouraged to report any instance of abnormality and get a timely response to concerns. A questioning attitude cultivates a culture in which people are more cognizant of daily activities and, as a result, are more aware of irregularities that may give early indications of a breach.

6. **Organizational learning is embraced:** All individuals connected to an IoT platform should understand their potential impact and have a thorough understanding of the components of an IoT system. Organizations should take time to educate and train their workers to better understand the common vectors of attack used by hackers, the role they play in prevention, and the appropriate processes in the event of a breach.

7. **IoT security undergoes constant examination:** Improving security technology, spreading secure cultural ideals, and testing security should be a constant effort. A healthy security program consistently seeks opportunities to improve, test systems, and patch often. Workers should be encouraged to provide feedback for improvement and to take proactive security measures to keep ahead of attackers at every opportunity.

5 Conclusion

As IoT continues to mature as an industry, the technology and culture surrounding it must constantly adapt to address the realities of hacker behavior, mistake-prone humans, and the seriousness of the equipment in play. By understanding the core technology concepts of IoT security, creating layers of technology-based security methods, and fostering a culture committed to security, organizations can implement IoT in a way that deters attackers, keeps assets and people safe, and minimizes risk.

We can help you build a pragmatic security strategy for your industrial IoT project.

Connect with our team
of IoT experts to learn more.

exosite.com | +1.612.353.2161