HOW TO INCREASE THE SAFETY OF INDUSTRIAL IOT

A guide to IIoT Security
CONTENT

CYBER SECURITY IN INDUSTRIAL LANDSCAPE

EXECUTIVE SUMMARY

Introduction and Context
The need for IoT Security

Parts of a Complete IoT Security Journey
Device Level
Communication Level
Cloud Level

APPENDIX

19

Completing the IIoT Security Journey
Certifications
Certified Testing Programs

19
The Internet of things has become the buzz word over the past few years and many giants such as Amazon, Google, and others are rushing to become “The IoT hub” offering a wizard of services to cater to this requirement. There have been predictions of millions of linked devices existing by 2020 with objects as mundane as water in your refrigerator and tires in your vehicles becoming a part of this intermeshed world. Manufacturers from a wide array of industries are attempting to leverage the potential of IoT to address multiple needs of business consumers.
Some examples:

1. Cut the cost of delivery or maintenance for certain items. General Electric has introduced a system using which it performs predictive maintenance in jet engines to predict faults and ensure that they do not grow into big issues. Tracked flight data is also used to reduce fuel consumption and increase engine’s efficiency.

2. Create new revenues from value added services or Platform as a service. For example, Rolls Royce’s Power by the hour approach allowed operators to pay a fixed sum per flying hour instead of paying for the engine upfront.

3. Perpetual connectivity with client which ultimates customer satisfaction and retention: E.g. Caterpillar has used sensors in vehicles that it rents to end customers to continually run diagnostics which are then conveyed to the company. This diagnostic can then help the company prevent downtime for vehicles. Once downtime is predicted, the company could send a service personnel or easily replaceable parts to the end customer and train them through the use of AR to perform the fix themselves. A 2016 survey by PriceWaterHouseCoopers (PWC) revealed that 72% of data manufacturers predict that their data analytics will improve customer relationships and customer intelligence along the product lifecycle.

According to Frost and Sullivan, only 25 to 30% of manufacturing companies around the globe have adopted IIoT in 2016. This number is expected to increase to 80% by 2021.

Whether it is to reduce cost, create new revenues or improve customer relationship, a new advancement in science will get adopted across users only in presence of trust between the user and the supplier. Despite the industry’s widespread acknowledgement of IoT’s significance, cyber security has remained an elusive topic for many of the companies.

According to Gartner, 1 in 5 vehicles on the road will have some form of wireless network connection by 2020 amounting to more than 250 million vehicles worldwide. With this progressively increasing connectivity among industrial and consumer devices, IoT security gains paramount importance. For example, consider a case wherein a casino was hacked via a thermometer placed in an aquarium in the lobby. The hacker was able to get a foothold in the network, connect to the roller database
and then pull the data across the thermostat to the cloud. Similarly, there have been cases of banks being hacked through CCTV cameras since these cameras are purchased purely on the basis of cost.

Similarly, B2C companies are expected to grow to $25 billion in 2020 up from $5 billion in 2015. Imagine a scenario, wherein hackers have complete access to your location, calls, messages, etc. through your wearables. Such a scenario could lead to potential risks which would lead to user dissatisfaction and might become a cause for companies to be sued.

This ebook’s purpose is to elaborate on the way that Industrial Technology and Operational Technology should meet and to touch on the various aspects in which a company can and should approach strengthening of cyber security.
INTRODUCTION AND CONTEXT

In 2009, the Stuxnet virus paralyzed Iran’s nuclear program by hacking into the interconnected Control Systems (ICS) of fifteen radioactive enrichment plants. At the time, this was the biggest and most complicated cyber attack that was introduced into a system using a single machine and USB port. The attack consisted of two subtasks. The foremost task was to record and transmit details regarding normal plant operations. By doing this, it aimed to destroy around thousand centrifuges by making them spin out of control. The attack also impeded the program by reducing its efficiency by 30%.

All such attacks call Industry experts to action and shows the extent of effort that needs to be put in by Operational Technology (OT) departments to protect every device, system, etc. With the current advanced technology, hackers now have the ability to creep into any system and negatively impact operations through a single network target.

By 2020, 100% of large enterprises will be asked to report to their boards of directors on cybersecurity and technology risk at least annually, which is up from today’s 40%. - Gartner
THE NEED FOR IOT SECURITY

As most of the IIoT applications in various verticals like manufacturing, transportations, utilities are coming into effect, security needs to be woven into this edge-heavy ecosystems. The security layer needs to be distributed, redundant, flexible, and adaptive in order to keep up with the systems that they protect. The recent attacks at Target, Sony pictures, Equifax, exhibit the high amount of data and privacy loss that could be faced by customers. Any security attack on Industry 4.0 enabled platform could potentially lead to a disaster that could not only exceed the loss during the aforementioned attacks but could even exceed the disastrous effects of Fukushima Daichi or Union Carbide in Bhopal.

Most of the current cybersecurity methods across the industry are outdated and focus around maintenance of firewalls and other such outdated methods. These cybersecurity methods, though not useless, definitely are not equipped to handle the security loopholes today. These need to be revamped to ensure that current systems can also be managed. Recently in July 2017, the Rise of Thingbots reported that the IoT attacks increased to 30.6 million IoT brute force attacks which was a 280% increase from December 1, 2016.

In face of such heterogeneous applications and increasing number of IoT devices, the existing cybersecurity measures will struggle to defend the vast, distributed infrastructure. The number of IoT devices connected to internet is supposed to increased to 50 billion by 2020. With addition of each new device, hackers will obtain a new target to attack. There lies an urgent need to have zero trust security model to establish a safe and foolproof IoT platform.
In the past, there have been incidents of someone’s vehicle being controlled remotely by hackers and being accelerated or decelerated without any control of the driver within it. Specifically, a few years ago, Chrysler performed a recall of around 1.4 million vehicles after a few hackers showed that they could hack into the Jeep’s internal systems over the internet. They also later proved that they could send messages on vehicle’s internal network known as CAN bus and perform sudden application of breaks or accelerator, turning the vehicle’s steering wheel at any speed.

Additionally, a recent meta study titled “The Internet of Hackable Things” compiled from industry and academic reports found that the smart device healthcare and smart homes & buildings posed daunting risks.

1. 90% of devices collected at least some form of information through the device.
2. 80% of devices, their mobile and web counterparts included, did not require a strong password.
3. 70% of devices allowed an attacker to identify valid user accounts through enumeration.
4. 70% of devices used unencrypted network services.
5. 6 out of 10 devices that provided user interfaces had weak credentials.

Many of these security risks are not limited to consumed IoT devices but also extend and cover Industrial IoT.
To realize its complete potential, Industry 4.0 requires security that is autonomous, real time and adaptive. Instead of interacting with centralized devices, equipments and applications need to interact with each other to protect themselves. A thing to note here is that IoT Security is not an end goal but a journey on which the development partners and consumers need to move hand in hand.

IoT security breaches can be grouped into three levels based on where they occur namely:
1. Device Level breaches
2. Communication Level breaches
3. Cloud or application level breaches

Hence a wholesome security solution should look at preventing breaches from all these directions. Some of the most important solutions are listed below:
A system needs to be incorporated to ensure the authenticity of each device that links to the IoT platform. This confirmation of authenticity of data can also be done using implementation of Blockchain.

Ensure authenticity of device data
One of the common problems of IoT device breaches is IoT device spoofing wherein an attacker creates a device that mimics hardware on an IoT platform feeding wrong data into the network, adversely affecting any machine learning that occurs on the platform. Hence, a system needs to be incorporated to ensure the authenticity of each device that links to the IoT platform. This confirmation of authenticity of data can also be done using implementation of Blockchain. Implementation of IoT wallets that use asymmetric cryptology...
can be used to confirm that data being sent to the network comes from an authenticated device.

**Keeping track of all updates and basic changes**

As IoT becomes a bigger reality, the device manufacturers/OEMs keep on launching security updates to protect devices. However, many corporations or users tend to ignore these updates, sometimes for fear of new bugs in the device and sometimes just due to ignorance or failure to keep track of these updates.

Additionally, quite often individual users as well as industries forget to change passwords of these devices leaving major loopholes in the security system. For example, quite often wireless access points and printers come with well known administrator IDs and passwords which are sometimes not changed at all. On top of this, sometimes these devices come with built in web servers to which anyone can login using default usernames and passwords. This sort of access can give huge power into an attacker’s hands. Even when the passwords are changed, they more often than not, lack sufficient security.

Malware trojans like Mirai and Bashlight effectively utilize this inefficiency. For example, Mirai uses common usernames and passwords to pinpoint and infect vulnerable IoT devices. Once infected, these devices continue to function as normal. Through the infection and control of multiple devices, Mirai launches Distributed Denial of Service (DDoS) attacks. In
October 2016, through a complex network of such infected devices, Mirai launched a DDoS attack on Dyn, resulting in downtime of multiple famous websites such as Netflix, Twitter, Reddit, etc.

In 2013, an IoT botnet was discovered by a researcher at Proofpoint wherein 25% of the botnet was made of devices as inconspicuous as baby monitors, smart TVs and other household devices. In order to avoid such scenarios, it is important to keep the passwords and devices updated.

A thing to note when applying updates is that software updates should be accepted only from authenticated sources. An authenticated update should be digitally signed by the software vendor.

The patching process also needs to be performed in such a way that it minimizes the risk of losing data or interfering with operations. For example, before starting the update process for a device, all devices need to be informed that a specific device will be going offline. After performing the update of device, the device needs to be verified before returning it to normal operating mode.

**Power Cycle the device:**
Some malwares such as the Krebs malware can be stored in the memory of the device and has the option of being erased only with a power cycle. Hence, it is important to manually power cycle the devices every once in a while.

**Disable Universal Power Plug n Play support:**
Many devices have uPnP which opens the virtual port allowing attackers to poke a hole in the router’s shield, making the device discoverable online and prone to malware infection. Hence, it is important to close such uPnP connections.

**Anti Tampering of devices:**
Once someone has access to one of the devices on the network, he/she can alter the device as required. Hence, an application should be in place that can determine tampered, counterfeit, or unauthorized emissions from altered devices by establishing a baseline power and utilizing machine learning models to detect anomalies in consumption of power. The models can be used to detect anomalies for a certain set of hardware which can be personalized for the application. In this way, it would ensure that interfered devices are detected early before they cause any damage.

**Device Authentication and Secure Boot:**
Unique keys can be embedded into the System on chip (SoC) which can then be used to confirm the identity of the device when it connects to the gateway. Additionally, the boot process can be linked to the installation of an operating system which will be signed and the certificate will be burnt into SoC memory. A ROM based bootloader can be implemented that has a
secure boot protocol and that verifies OS on flash memory before booting.

Restrictions on WYOD (Wear your own device)
Companies need to adjust their Enterprise Mobility Management (EMM) policy to disable bluetooth wearable devices and IT managed smartphones and tablets altogether or in high risk areas. EMM can also be restricted to disable wearable specific apps on managed smartphones.

In cases wherein wearables lack enterprise grade authentications, IT can use WLAN to block or allow enterprise network access to business wearables.

Network Based Controls:
Most internet controlled devices can be managed efficiently via dynamic Host Configuration Protocol (DHCP), a network used for automating IP parameters. DHCP logs and lease files provide a good way to manage inventories. Restricting DHCP to known devices and segregating new devices onto subnets provides a good inventory control policy. DHCP server configurations should always tie back to an IP address management and inventory control system.

Some malwares such as the Krebs malware can be stored in the memory of the device and has the option of being erased only with a power cycle. Hence, it is important to manually power cycle the devices every once in a while.
Intrusion Prevention System (IPS) can be placed inside the network and all traffic has to pass through IPS before reaching the server.

Firewall/IPS/ID

Intrusion detection system (IDS) can be placed behind firewall which will take into account traffic flow and complete network design. IDS can be used to detect intrusion in one of the following ways:

1. Signature: The patterns of known attacks can be saved as signatures in an IDS system. A new packet will be verified and alerts generated in case of matches against the signature in database.
2. Anomalies: A baseline can be generated for certain use cases for a customer. For
e.g., if 10 users open connections at a time with more than 5 connections per user i.e. more than 50 connections, then an alert will be generated.

3. **Protocol Anomalies:** If the effective protocol is HTTPS but requests are being sent in HTTP or if unknown commands are detected in network, then an alert can be generated.

Intrusion Prevention System (IPS) can be placed inside the network and all traffic has to pass through IPS before reaching the server. Hence, malware will not be allowed to reach the server and alarms will be raised in case of malware.

**Securing radio channels**

All the devices interacting with each other use common radio frequencies and protocols which communicate among each other, a central hub and then the internet.

Sensors can be deployed within a location to detect all radio frequencies between a certain range such as 100kHz and 6 GHz. These sensors can then monitor the positions and emissions from all devices within the detection range. When a new device tries to connect to the network, the sensors will recognize the device as a threat to security. The system should also be able to detect when an existing device sends signals that may indicate a breach in their security or when they may be performing attacks on other devices within the area.

**Encryption to secure communications**

Hackers, more often that not, constantly monitor network traffic with the sole intention to identify loopholes which might allow them to install malware or carry out attacks. Hence, in order to keep the data secure, one needs to consider encryption during initial configuration. Usage of encryption tools that guarantee end to end security makes it difficult for hackers to access the data transmitted through internet. This will ensure that the data in the database is secure and not compromised. File MD5 hashes can be used to ensure completeness and success of file transfers as well as that files are not tampered with.

IPsec and SSL are the two most common options for encryption. IPsec is considered better than SSL since these convert non IP data into IP. They can be the first IP connectivity point in the network. Since most low end sensors do not allow for encryption, it is a good idea for the first hop router to be the first encryption

**Usage of encryption tools that guarantee end to end security makes it difficult for hackers to access the data transmitted through internet.**
point in the network. This option also provides benefit for both remote access and site to site connections.

All data transfers between the edge device and the server can also be done over a 128 bit encryption of the application. When using the encryption keys as well, the encryption keys should be independently calculated on both sides of the connection ensuring that the keys never get transferred over internet.

IoT network security
This can intend to include protection and security of network from IoT devices to back-end system on the internet. This could include the traditional methods such as antivirus and antimalware. This could also include other methods such as firewalls, intrusion prevention and detection systems.

Support for Transport Layer Security
All communication should occur in an encrypted form using HTTPS. All communication from the edge microserver component to the server should occur over standard Websockets Protocol which is based on secure and encrypted TLS protocol.

Multi Level Authentication:
Once a websocket is established, the connecting device should provide credentials in order be allowed to communicate with any other part of the solution or system.

Auditing:
All file transfers and application tunneling such as Remote desktop should be audited at both the server end as well as on the edge devices.

When using the encryption keys, the encryption keys should be independently calculated on both sides of the connection ensuring that the keys never get transferred over internet.
A pluggable authentication model that allows businesses to integrate their specific authentication model would provide independence to the businesses.

Authentication and Authorization:
In order to ensure that only permitted users access the system, an extremely granular security model that allows data isolation and service execution at required levels would be required. The application should support HTTP authentication which would require a user to establish a web session using a username and password. If required, authentication can also be delegated to LDAP system, allowing the LDAP system to manage password policies such as password expiration, account lockout, password strength and history, as well as password dictionary use.
A pluggable authentication model that allows businesses to integrate their specific authentication model would provide independence to the businesses.

**Application Level Security**
Applications can also be secured using third party applications such as VMWare, KAA or Mainflux which provide end to end solutions for edge computing, thus reducing the development effort and ensuring security.

**Ensure that devices are patchable**
Malware attacks are constantly evolving. Hence, IoT mandates that you keep up with the changing trends. It is necessary to ensure that you use devices which do not come with pre-prepared passwords as such devices make it difficult to change passwords or to apply patches. In short, devices should be easily patchable. For example, if a printer requires firmware to be upgraded, IT department is less likely to upgrade it when compared to a server or desktop system. Custom firmware often require additional effort and time to be upgraded.

A cloud application should allow users to update and apply patches to their hardware remotely. This system should also ensure that updates are tested before installation.

A stringent commissioning system needs to be put in place that logs into any device using initial configuration settings as well as some well known settings often used by hackers. It should scan all connected devices for any security vulnerability, validate and close it before the device is moved to production environment. Such a process would in turn reduce the security issues in this area.

**Security logging sub system:**
System should have a set of logging services for the security, configuration changes and the application layer. Any change and login made into any of these systems, successful or not, should be logged and monitored.

**Risk assessment and Activity Monitoring**
In order to learn from previous attacks and continuously improve the system, it is necessary to install a system that would monitor and perform anomaly detection. Depending on detection of any anomaly in data from a particular device, shutdowns can be triggered if there is any indication of tampering or network based attack. Additionally, automated alerts and actions can be created in case of any attacks, leading to automated shut down of a system and engagement of an incident which will be handled by support engineers to verify the risk and fix any error. This system can also provide protection from replay attacks.

**Encrypted storage of all sensitive data**
To prevent misuse of data, it is better to ensure that all data is encrypted. Passwords should be encrypted at all components within the IoT solution with the inclusion of passwords stored at the platform for users and passwords at edge devices. Storage of encrypted data for persistence also increases security.
Blockchain could be possibly used in the area of IoT security due to a few advantages it could provide in this domain. It can serve as a secure network that would act as a platform for devices to connect securely without the potential risks of device spoofing.

Machine to machine (M2M) authentication is a core need of a secure IoT platform which can be easily implemented through the use of blockchain eliminating the need of a central regulator. Every device in the node would need to be instantiated on the blockchain and would use its uniquely identifiable blockchain identifier to demarcate itself in the network. For a device to connect and interact with another device in the network, it would use its wallet to raise an identity request. The wallet would create a request bearing a digital signature which when sent to the target device can be verified using the public key of the sender.

In case of those devices that are constrained by storage issues, the wallet could be stored on a proxy. This would involve some level of aggregation but can be expected to be of minimal impact. In this manner, each device could be identified and infected devices and applications can be isolated.

However, the decision to use blockchain as a measure of security is also hindered by the fact that strong encryption methods could induce a period of impasse. Hence, it would be recommended to evaluate this on a case by case basis.
COMPLETING THE IIOT SECURITY JOURNEY

Just as a strong house needs a strong foundation, similarly a strong IoT platform would need to meet Security concerns early on from its inception. In line with this, IoT platform developers and industries need to understand how to identify and mitigate risks. As a baseline, some of the courses and certifications that could equip its participants to learn a little about IoT Security are mentioned below:
There are many certification programs available in the field of IoT security.

**IoT Security Foundation (IoTSF)** provide a basic quick certification course that runs over 2 days that teaches attendees on methods to research and assess IoT threats and risks as they arise and enables them to implement a security reporting scheme in their organization.

**Global Science and Technology Forum (GSTF) Certified Internet of Things (CIoTS)** is a comprehensive five day training and certification program which explores the infrastructure, communication, sensor technologies, data storage, analytics and security facets of IoT. This can be attended by roles such as IT/IS Executives, Managers, Business Analysts, IT Architects, Risk management employees, IT technical service specialist, etc.

**IoT Security Certified Analyst (ISCA) certification** by Axelta is a 4 day IoT security training program that takes the attendee through a detailed journey of various vulnerabilities in IoT and methods to evaluate security at hardware, software and communication level followed by experiments on MIPS attacks and embedded OS level vulnerabilities.

**Cisco Industrial Networking Specialist** certification program tests the hands on skills through simulations and tests conceptual knowledge. Candidates new to this course can also take other basic courses such as Control systems fundamentals for Industrial Networking (ICINS) and Networking Fundamentals for Industrial Control Systems (INICS).

**Certificate in Internet of Things by University of Washington** is an eight month online course which take the participant through a detailed process of development using Internet of Things. The participants are taught about usage of raspberry pi platform, usage of concepts involved in machine to machine communication, application of techniques for connecting and reading sensor data, distributed computing and cloud storage, etc. Though it does not deal with security specifically but it covers security in terms of communication, etc.
Certified Testing Programs

There are multiple certified testing programs available in the market. Some of the more well-accepted ones are listed below:

Underwriter’s Laboratory Cybersecurity Assurance Platform (CAP) provides a standardized, testable criteria for assessing software vulnerabilities and weaknesses. It allows identification of zero-day vulnerabilities over all interfaces, identification of known vulnerabilities, analysis of static source code for weaknesses identified by Common Weakness Enumerations, and suggestion of security measures to mitigate risks associated with access control and authentication, remote communications to products, decommissioning and software updates of products.

ICSA Laboratory IoT certification Testing program has an identified list of vulnerabilities and tests a set of six components found in most IoT devices including physical security, alert/logging, and communications. ICSA charges a flat fee or annual contract for its certification testing program and can run from a few thousands to above $100,000.
APPENDIX

¹2017 Roundup Of Internet Of Things Forecasts
³Industry 4.0: Buidling the Digital Enterprise
Dr. Reinhard Geissbauer, Jesper Vedso, Stefan Schrauf-
https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf
Why should Enterprises work with Ideas2IT? We might not be able to match the staffing power of large scale IT organizations, but what we offer is the ability to take enterprises into the next decade.

We help forward-thinking enterprises usher in new tech, and innovation.

We take a deep interest in cutting-edge technology, and we’re always learning, understanding and implementing the latest tech. We have a habit of picking the right technologies and betting on them. From Machine Learning to Blockchain, we’ve consistently identified winners and doubled down on them before the general public (and our competitors) caught on and adopted. Several of our top-level execs have built and scaled startups of their own. Our CEO has co-founded three companies to date, one of them funded. We’ve taken several products to market, and we know what it takes to build products successfully. This makes us extremely good at solutioning, with very little data. We’ve worked on projects for billion-dollar organizations, and know what it takes to work with enterprises. Besides, we leverage all of our learnings from working with Valley startups, to help enterprises with innovation.

USA (Onshore)
1400 Coleman Ave,
Santa Clara, CA,95050 USA.
Tel: +1-408-755-9621

EUROPE (Sales Office)
Schlossbachstrasse 38,
Rorschacherberg,Switzerland ,
CH-9404 EUROPE.

INDIA (Offshore Development)
RR Towers-5, 8th floor,
T.V.K Industrial Estate,Guindy,
Chennai, 600032, INDIA.