htng

MOVING
HOSPITALITY
FORWARD

INTERNET OF THINGS (IOT) SECURITY WHITE PAPER

8 December 2020

Version 1

About HTNG

Hospitality Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitate the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

Manufacturers and software providers shall not claim compliance with portions of the requirements of any HTNG specification or standard, and shall not use the HTNG name or the name of the specification or standard in any statements about their respective product(s) unless the product(s) is (are) certified as compliant to the specification or standard.

Permission is granted for implementers to use the names, labels, etc. contained within the specification. The intent of publication of the specification is to encourage implementations of the specification.

This specification has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed. Visit http://htng.org/ip-claims to view third-party claims that have been disclosed to HTNG. HTNG offers no opinion as to whether claims listed on this site may apply to portions of this specification.

The names Hospitality Technology Next Generation and HTNG, and logos depicting these names, are trademarks of Hospitality Technology Next Generation. Permission is granted for implementers to use the aforementioned names in technical documentation for the purpose of acknowledging the copyright and including the notice required above. All other use of the aforementioned names and logos requires the permission of Hospitality Technology Next Generation, either in written form or as explicitly permitted for the organization’s members through the current terms and conditions of membership.

TABLE OF CONTENTS

1 This Document at a Glance

The Internet of Things (IoT) is the collection of electronic components and devices that can be connected through Internet protocols. These devices typically provide a combination of computing, sensing, and controlling capabilities, including smart light bulbs, thermostats, printers, TV's, phones, door locks and cameras.

IoT is a relatively new technology that has been adopted very quickly. As often is the case with new technologies, the security of IoT deployment has been an afterthought. This paper looks at IoT security in the contexts that are often seen in the hotel industry. This is important because we don't want unauthorized people to:

- Unlock our doors
- See if someone is in the room
- Change the room temperature
- Use our infrastructure in web attacks
- And more

Security is a large, complex topic so we will only touch on the edges in this document. Consider the following:

"Information security risk of installing a non-networked light bulb is basically zero, but the minute you connect it, there are so many things you have to think about…" ***- Paddy Srinivasan – LogMeIn***

This paper is targeted toward those that have a role in decision making regarding IoT purchases and implementation but may not be technology or implementation experts, and for technology generalists that want to gain insight into the security concerns with IoT technologies.

Our goal is to provide a broad understanding of the inherent risks in using IoT and provide an introduction to the strategies and best practices that can be used to protect your organizations from these risks, allowing the value that IoT brings to be recognized.

2 Risks and Risk Assessment

Any discussion of security must reflect what needs protection and at what cost. Risk is how we define this; risk is defined as:

“A security risk is any event that could result in the compromise of organizational assets i.e. the unauthorized use, loss, damage, disclosure or modification of organizational assets for the profit, personal interest or political interests of individuals, groups or other entities, constitutes a compromise of the asset, and includes the risk of harm to people. Compromise of organizational assets may adversely affect the enterprise, its business units and their clients.”

- *Julian Talbot and Miles Jakeman Security Risk Management Body of Knowledge, John Wiley & Sons, 2009*

In the security world, risk is calculated by a deceptively simple formula:

Risk = Probability of Loss X Amount of Loss

For the amount of loss, we look at assets and the consequences or impact of the loss. The consequences of loss can include legal costs, fines and reputational damage due to a security incident in addition to direct costs.

For the probability of loss, we look at vulnerabilities, threats, attack vectors and the number of attempts or occurrences versus successes over a period of time.

The value for risk is expressed in dollars (or a comparable currency) and is used to justify the expense required to secure the system. While the formula is simple, determining the numbers to plug into the formula can be a challenge.

In the sections that follow, we will look at the things that need to be protected, threats and vulnerabilities in the context of hotel based IoT.

3 Risk: What Needs to be Protected

Assets are the things the company has and wants to protect. The types of assets most commonly lost in IoT attacks include:

- Information loss:
    - Loss of company information – sensitive information about the company and its business
    - Loss of customer information – sensitive information about the customer
    - Loss of employee information – sensitive information about those that work for the company
- Loss of network infrastructure access and control
    - Leveraging network access and control
    - Leveraging IoT devices to perform attacks on other networks
- Loss of money through theft and ransoms
    - Using access gained through IoT devices for theft of money or other resources
    - Use access to IoT devices to infect systems on the network with ransomware
- Loss of brand reputation and goodwill

The following are less common today but are still a concern that hotels need to protect:

- Loss or damage to facilities and facility infrastructure
    - This includes electrical outages, alarms and environmental controls
- Loss damage or destruction to guest property
    - Damage to guest computers, phone, tablets and other electronics
    - Damage to guest vehicles
    - Damage to luggage and contents by flood or fire
- Loss of safety and health of guests and workers
    - This includes losses due to failures of door locks, emergency lighting and signage, smoke and fire alarms, and elevator controls

3.1 Information Assets

Hotels typically have more customer data than other businesses, especially as hotels move to hyper personalization models wherein more and more aspects of the IoT experience affect a guest’s stay. Be aware that IoT systems like network access points, set top boxes and printers in business centers may be collecting guest information.

Examples of types of information that need to be protected for both guests and employees include:

- Personally Identifiable Information (PII) which is any information that can be used to identify an individual. This includes email address, computer MAC addresses, photos, driver licenses, passport numbers and membership numbers.
- Financial information including payment card information and bank or other financial account numbers.
- Personal information which may include travel plans, room number, room occupancy, medical information, disabilities, religious preferences, sexual preferences, TV viewing and dietary preferences.
- Biometric information including face photos and fingerprints.

Information assets for the business include those assets that might reflect poorly on the company, damage the company's reputation or give others a business advantage if the information was known outside the company. These examples include:

- Contracts
- Strategic plans
- Tactical plans
- Financial account information
- Procurement information
- Internal contact information
- Occupancy and occupancy rates

3.2 Network Infrastructure

A good line of thinking is that any network is only as secure as the weakest device that is accessible on that network. IoT devices are often that weakest link. IoT devices represent a risk to the network infrastructure of the organization and typically if the network goes down, business operation is hindered as well.

Insecure IoT devices are not only a risk but also a threat to the network. An insecure IoT device can give an attacker access to other systems on the network which exposes even more risk. Compromised IoT devices can also be used to attack your own network from inside to prevent the network from being usable, or to attack other networks in Distributed Denial of Service (DDoS) attacks. Many IoT devices also collect and may share information about device users. Sharing information with third parties may even occur without the knowledge of the business.

3.3 Brand Reputation and Goodwill

Brand reputation and goodwill can be hurt by almost any type of information attack. A primary risk to reputation with IoT is guest experience. If IoT environmental controls are shutdown during the hottest week of the year in Florida, your guests are not going to have a good experience.

3.4 Facilities, Safety, Health and Guest Property

Facilities, safety, health and guest property are all somewhat related, because while the specific losses are different, the causes of the losses are often related. For example, if the environmental controls are hacked and the hotel is left in the humid air of Florida in the summer, by the time the air-conditioning has been recovered there may be significant amounts of mold and mildew in the air handling systems. This may have a health impact on workers and guests in the facility which would cause a loss of revenue while the mold and mildew is mitigated. A similar event occurred in the University of Maryland dorm system in 2018-2019 school year. A successful attack on IoT door locks can lead to items being stolen from guest rooms or even worse, attacks directly on guests in their rooms.

4 Risk: Threats

Threats are the things that can cause harm or loss to your systems. Understanding the threats against an organization helps in determining risk. Threat agents are the people or organizations that may cause harm to your systems. Not all of these are nefarious, as some damage can be caused by innocent accidents, but the primary concern here is those who exploit vulnerabilities in a system with the intent to cause harm.

4.1 Threat Agents Or Actors

Threat agents are typically people, but a threat could also be weather, earthquakes, or other “acts of God.” Understanding threat agents and their motivations helps to determine the probability that harm or loss to the organization will occur. The following list classifies the type of active threat agents typically encountered.

- Internal Employees Unintentional – Causes unintended, typically accidental harm
- Internal Employees Hostile – Uses system access to cause intentional harm typically to address a perceived wrong but may also be acting in the role of thief
- Contractor Unintentional - Causes unintended, typically accidental harm
- Contractor Hostile – Uses system access to cause intentional harm typically to address a perceived wrong, but may be using access to act on other roles
- Customer – Typically causes unintentional or accidental harm
- Cyber Attacker – An attacker with intent to directly or indirectly harm the organization. Initial attacks may be exploratory.
- Competitor – An attacker within the industry that attacks to gain a business benefit over the organization. These attacks typically deny access to the competitor’s systems or extract competitive information.
- Government – A government attacks typically to gain information both about the organization and its customers. In some cases, governments may attack to impact actions of an organization.
- Thief – Thieves are typically looking at stealing or leveraging resources and may actively steal funds, extract money through ransoms or use resources for digital currency mining, sending SPAM, or conducting denial of service attacks on other organizations.
- Activist – An activist attacks to promote a political agenda that is often related to organization behavior that is disagreeable to the activist.
- Cyber Explorer – Typically a cyber explorer is simply trying to learn about the systems being explored and does not intend to cause any harm. However, accidental harm is always a possibility and what they learn can make systems more vulnerable, leading to expose the vulnerabilities to others.

The table below shows the threat agents in the rows and the assets that are typically under attack in the columns. Certain assets are more likely to be threatened by particular agents than others.

Table 1: Threat Agents Versus Type of Risk

	Source	Reputation	Theft	Facility Damage	Loss of Business	Loss of Advantage	Remuneration	Loss of revenue	Safety & Health
Employee Hostile	Internal	X							X
Employee Unintentional	Internal	X		X	X	X			
Contractor Hostile	Internal	X	X	X					X
Contractor Unintentional	Internal	X		X	X	X			
Customer	Both	X	X	X			X		
Cyber Attacker	External	X	X	X	X		X	X	X
Competitor	External	X		X		X		X	X
State or Quasi-State	External				X	X			
Thief	External		X		X			X	
Activist	External	X		X	X	X		X	X
Explorer	External	X		X					

The above chart varies based on type of business, clients and location. In particular, the hotel industry is more likely to have threats against facilities since the building typically represents a physical embodiment of the business and against health and safety of the guests because it attracts news stories having a larger impact on reputation and loss of business.

4.2 Threat Vectors

Threat vectors are how attacks can be carried out and represent the various ways a system can be attacked or compromised. Think of a burglar trying to enter your home, threat vectors might: pick the lock on a door, kick a door down or break through a window. The following is a basic list of IoT threat vectors:

- Attacks against network and Wi-Fi connections
- Attacks against insecure communication protocols
- Attacks on poor authentication and authorization practices including poor credential management
- Attacks against firmware and firmware vulnerabilities
- Attacks against IoT software and the ecosystem for IoT devices
- Physical attacks against IoT hardware
- Attacks leveraging poor configuration management practices
- Attacks against secrets stored insecurely within the devices
- Attacks leveraging insecure services

The next section covers vulnerabilities; weaknesses that can potentially be exploited.

5 Vulnerabilities

Vulnerabilities are weaknesses that can be exploited by a threat agent. Think about the burglar example in Section 4.2. The burglar may have looked at several houses in the neighborhood, but selects those with the locks that are easiest to pick. The threat vector is how he gets in (through picking the lock on the door), and the vulnerability is the weak lock.

Many IoT vulnerabilities are directly related to limitations in the devices themselves. IoT devices often have limited capabilities due to limitations in the processor, storage, memory, communications and security mechanisms. IoT devices often have no capability for secure processing, secure memory and have limited support for tools to harden against common attacks and vulnerabilities.

IoT devices range from the very complex, built on robust computing platforms with full operating systems, to systems built using System on a Chip (SoC) designs with very limited resources. These limitations typically include:

- Limited storage and secure storage
- Limited support for encryption
- Limited tamper resistance
- Limited device performance
- Limited network support
- Limited or missing integrated firewall capabilities

IoT devices represent a range of these limitations. For example, a typical modern printer may have ample storage capabilities and support for secure communications, but may have no support for tamper resistance or secure storage.

A typical set of IoT vulnerabilities includes:

- Weak access control
- Insecure network services
- Insecure operating ecosystem
- Lack of update support
- Use of outdated and insecure software
- Insecure default settings
- Lack of cryptographic support
- Lack of secure storage

Devices with multiple vulnerabilities are more likely to be exploited and hence contribute to the risk of an organization.

5.1 Access Control, Credential and Identity Management

Like all network-accessible systems, IoT devices should require credentials to authenticate and authorize users of the services the device exposes. This typically means the provision of user IDs and passwords, or a token that is securely sent each time the device is accessed. Ideally, each user is limited to only the services they need to access. This implies support for roles within the IoT device. The device should also allow the creation, update and deletion of these credentials. Many IoT devices do not have user interface elements that allow for straightforward access control credential changes.

Many devices ship with default or vendor-supplied hard coded credentials. A secure device should force these credentials to be changed when first accessed. Failure to update default access control credentials is an avoidable user error that is all too common. If credentials are stored on the device, the device must be able to store them securely.

OWASP is the Open Web Application Security Project, one of the premier organizations identifying security issues on the Internet and providing mitigation tools to prevent the issues. The number one IoT vulnerability identified by OWASP is weak, guessable and hard-coded passwords.

5.1.1 Mitigation Strategies for Access Control Vulnerabilities

The most common mitigation strategy to protect against access control vulnerabilities is to change default passwords when devices are installed. The passwords should be replaced with secure passwords that consist of: 15 or more characters, a mix of upper and lower case characters, numbers and special characters. These credentials should be changed regularly and multiple failed attempts to login should be logged and alarmed.

If available, consider using secure authentication tokens and solutions based on Public Key Infrastructure (PKI) instead of password authentication if supported by the device.

5.2 Credential Sharing

IoT devices often have limited support for the number of credentials that can be used to access the device and the roles that authorize the accessible features. It is common to have one administration credential and a single user credential. Many organizations tend to use the same credentials on every device of a certain device type; For example, every printer might be configured with the same admin password. This means if the credential is compromised on one device it is compromised on all of them.

5.2.1 Mitigation for Credential Sharing

Prefer devices that integrate with the network user directory for authentication and authorization credentials or an alternative; devices that use secure authentication tokens like SAML, JWT or OAuth are created using a trusted identity system. Another alternative is to use a credential proxy system that requires the user to authenticate to the proxy with their credentials and the proxy intercepts the message replacing the user credentials with the correct device credentials.

IoT device credentials should be unique to each device and updated frequently.

5.3 Insecure Network Services and Protocols

Many IoT devices enable insecure network services such as Telnet and FTP by default. These services implement older protocols which pass credentials and data over connections that are not encrypted or secure. The following are examples of commonly exposed insecure services that should be disabled or replaced by secure services:

Telnet

Telnet is an old terminal service which should have been retired decades ago. Use a recent version of SSH (Secure Shell) instead.

FTP

File Transfer Protocol should be replaced with the SSH utility SFTP or with FTPS the secure version of the FTP protocol.

POP3

Post Office Protocol is an old email client protocol, use POP3S instead.

IMAP

Internet Message Access Protocol is another email client protocol, use IMAPS instead.

SMB

Server Message Block is a protocol used for file and printer sharing with Windows systems. Older versions are very vulnerable to attack and different implementations (Samba for example) have different vulnerabilities. If this service is not needed, make certain it is disabled. If it is required, make certain it has all of the latest patches applied.

HTTP

Hypertext Transfer Protocol is the protocol used for serving web pages. Many IoT devices have embedded HTTP servers. The secure HTTPS protocol should be used instead. Using HTTPS also implies that certificates can be managed on the device and that HTTPS handshake protocols can be updated and retired as needed.

SNMP

All versions of the Simple Network Management Protocol prior to version 3 are considered insecure. Any devices with SNMP versions prior to version 3 should either upgrade the service or disable it on the device.

Of course, this list is just a sample of some of the more common Network Services vulnerabilities and is in no measure complete.

5.3.1 Mitigation Strategies for Insecure Network Services

Most devices provide the ability to disable protocols that will not be used. When configuring the device, make certain obsolete protocols like Telnet and the other protocols from the previous list are disabled. If you need to use one of these protocols and the secure alternative isn't available, make certain that the device is isolated from the rest of your networks. This can be done by creating a separate physical network or by creating a Virtual Local Area Network (VLAN) using network routers and firewalls (Section 6.1). These isolated devices should have access limited by a gateway or firewall and restricted to only those systems that need to communicate with the IoT devices.

IoT devices on the network that have unsecure services exposed can be easily discovered by periodic network scanning and reporting of any unexpected exposed services.

5.4 Software and Firmware Vulnerabilities

Software vulnerabilities are weaknesses caused by flaws in the software running on the IoT device or its ecosystem that can be exploited. IoT devices often act as servers on a network by accepting connections and providing services to clients. IoT devices may also act as clients connecting to servers, sending messages and receiving responses. This leads to the same types of vulnerabilities that are common with many Internet systems; for example, buffer overflow and code injection attacks may allow malicious code to enter the systems.

5.4.1 Software Stack Vulnerabilities

Stacks are collections of software components that build upon one another to provide a capability to the computer or operating system. Stacks often provide basic services such as network protocol support. Developers of IoT devices often use these pre-developed stacks shared from component manufacturers, developed as open source or developed internally. Many of these developers may have little experience writing secure software. Once the firmware or software for the device has been developed, it is often not updated by the manufacturer, even if the underlying software has been updated. Even when vulnerabilities are pointed out, the manufacturer typically limits updates to only the most recently manufactured devices which the vendor considers to be still under support. This period of time can be as short as 90 days for home devices.

5.4.2 Inability to Securely Update Firmware

Security issues can be discovered at any time after a device is deployed. When security issues are discovered it should be possible to securely update the effected software/firmware. Some IoT devices are not capable of being updated in the field. This leads to hoteliers needing to choose between leaving vulnerable devices on the network or removing the devices and their functionality from the hotel network.

Devices that are field updatable often do not have mechanisms to authenticate the source and verify the integrity of new software/firmware. Without these authentication and verification checks, unauthorized firmware can be installed on the IoT devices.

5.4.3 Web Page Vulnerabilities

Web servers are built into many devices to provide user interfaces for configuration and to expose web services. Web pages hosted on these devices have the same vulnerabilities as web pages hosted on the web. This is especially true if the pages are Internet accessible. Web vulnerabilities include for example, cross site scripting and injection attacks. Making matters worse, the server may try to reach out to the web for images style-sheets and JavaScript code bringing new vulnerabilities in with these external resources.

5.4.4 Mitigation Strategies: Network Isolation

Isolation separates the IoT devices from the rest of the networks by creating either a separate physical network or by creating a Virtual Local Area Network (VLAN) using network routers and firewalls. These isolated devices should have access limited by a gateway or firewall and restricted to only those systems that need to communicate with the IoT devices. The Network Isolation strategy is discussed in more detail in Section 6.1.

5.4.5 Mitigation Strategies: Update Firmware

The primary means to reduce vulnerabilities due to firmware is to make certain it is possible to update the firmware on the device. This way if vulnerabilities are discovered and fixed, the firmware can be updated to address the weaknesses.

> If the firmware can't be updated, then the removal and replacement of the devices must be a strategy to consider.

It is best if the update capability is secure. Secure update typically involves the ability to download the firmware over secure network connections, Public Key Encrypted files, using digital signatures to sign the files and published public checksums of the files. Consider that if you can't update a vulnerable device it will likely need a costly replacement.

A checksum is a term used for a mathematical algorithm applied to a stream of data and used to verify the integrity of the data. See also “Message Integrity Pattern” in Section 7: IoT Security Patterns.

Of course, updates don't matter if the device provider never issues any updates. It is important to understand providers update policies, which vary between manufacturers. Policies may also be split with feature updates offered for a shorter time period than security updates.

It is common in the IoT world for alternative firmware/software to be offered for a device. These alternatives are frequently made by the open source community for specific devices. Examples include Android alternatives such as Lineage OS and Cyanogen Mod, Router firmware like DD-WRT, Tomato, Gargoyle and Open WRT, and Tasmota firmware for certain IoT switches and sensors. These firmware alternatives are an option to extend the lifetime of a device since these projects tend to be maintained longer than the manufacturers support periods.

5.4.6 Mitigation Strategies: Embedded Web Servers

A web-server embedded within an IoT device is subject to the same vulnerabilities as any web-server. Unfortunately, the owner/operators of the device have limited impact on the forms and content the server provides. The web-server content (HTML, CSS, images and JavaScript) for these devices should be examined for vulnerabilities and weaknesses. The best situation is that all HTML, CSS, images and JavaScript come from the device itself and not from the web. The isolation strategy can also help by limiting the Internet servers a device can access and ensuring secure access.

5.5 IoT Ecosystem Vulnerabilities

If internal device concerns were not enough, many IoT devices require third party support from web and cloud systems that may also be insecure. This potentially leads to poor protection of sensitive information and potential compromise of the devices utility and the systems connected to the device. The primary vulnerabilities include:

Permanent Ecosystem Shutdown

Shutdown means the permanent closure of the ecosystem that supports the device. This can happen when a company decides to no longer support the device or when a company is acquired, or goes out of business.

Ecosystem Outage

Dependencies between devices and their ecosystems are vulnerable to ecosystem outages. Outages of the ecosystem may also make the device unusable during the outage period.

Ecosystem Compromise

It can often be assumed that if the ecosystem a device depends on is compromised the devices attached to the ecosystem and information shared between them may also be compromised.

Mitigation Strategies

The simplest way to avoid ecosystem vulnerabilities is to not purchase devices that are dependent on proprietary external ecosystems. Instead, prefer devices with standards based open interfaces that either do not require a separate ecosystem or can be supported by multiple ecosystems. If you must purchase a system that requires a proprietary ecosystem, look for manufacturer guarantees of support including software and firmware updates as needed through the expected lifetime of the system and consider the risks that the company may be acquired or go out of business.

5.6 Cryptographic Security Vulnerabilities

Due to limited resources, many IoT devices do not have the capability to securely store cryptographic secrets such as encryption keys. Secret keys are often used to control network access to the device and loss of the keys can allow unauthorized access. Often keys are shared allowing multiple devices to be compromised. Unauthorized replacement of certificates may also allow the replacement of firmware updates with malware.

IoT devices may not be able to use vetted and validated cryptographic libraries and stacks due to resource constraints or availability of vetted libraries for the platform. This can lead to errors in the implementation cryptographic functions. Implementation of these algorithms on a new platform is often complicated due to timing issues and side channel attacks. These vulnerabilities can lead to key leakage and the exposure of confidential data.

5.6.1 Mitigation Strategies: For Crypto Weaknesses

Secure IoT devices are preferred over insecure devices. At a minimum, secure devices must provide several features including:

- A unique identifier for each device; this is often a CPU serial number.
- A real-time clock required to support time-based security elements. Normally a small battery is used to keep the clock working when the system is turned off.
- A Secure Boot capability verifies the integrity of the firmware and software along each step of the boot process.
- A secure storage element which is a place where data is stored and can only be accessed using elevated privileged instructions. This may be stored on chip or in an external device.

Additional features that are readily available on some devices include:

- Cryptographic acceleration: This speeds up cryptographic operations like encryption or decryption using specialized hardware.
- One of the following three hardware security enhancements:

Trusted Execution Environment or TEE

This is a separate section of the SoC (System on Chip) heart of the device that provides a separate capability to execute secure code. Many ARM processors include a TEE hardware capability. ARM is a family of processors designed by the company Advanced Risc Machines and popular in many cell phones and tablets.

Trusted Platform Module or TPM

A TPM is typically an external (to the SoC) chip that provides a number of services such as cryptographic acceleration and secret storage and it is typically permanently fixed to the motherboard. Some TPM systems can be plugged into a motherboard as needed.

Hardware Security Module or HSM

An HSM in the IoT sense is similar to a TPM but is a removable module attached to the motherboard. HSM appliances are network appliances used to provide high volume cryptography acceleration and secret storage. HSM appliances are not typically used for IoT services or devices.

5.7 Hardware Vulnerabilities

When attackers can physically access operating hardware, new classes of vulnerabilities become possible. Physical access to a device in operation may allow access to keys or other sensitive data that may appear on internal communication lines. An attacker can monitor or potentially modify data in the device as it operates. These vulnerabilities include access to external connections such as network and USB ports, as well as access to the internals of the device. Internal device access is a problem because savvy hackers with hardware access can read data from the wires using clips and connectors designed for testing the board as it is being built.

IoT devices are often installed in unprotected locations. Consider set-top boxes for example.

5.7.1 Mitigation Strategies: Tamper Protection

The primary strategy against hardware vulnerabilities is tamper protection. Tamper protection typically renders the device inoperable after tampering (typically by opening the case) to prevent this mode of attack. Tamper protection can provide a range of outcomes upon detection of an event, including logging the event and even erasing data held on the device upon detection. The choice of outcome is risk dependent. Some common mitigation strategies include:

- Placement of devices into difficult-to-access locations
- Limit access to external ports by covering or enclosing them.
- Deploy devices that restrict access to internal physical interfaces (JTAG, UART, GPIO, etc.).
- Use devices with tamper resistance and tamper detection built-in. Devices should implement tamper detection and/or response techniques depending on the risk profile of the device. This can include seals or casings as well as circuits designed to identify attempted physical intrusions.

5.8 Story: Mirai

In 2016 a student at Rutgers University created a virus, now known as Mirai, designed to specifically attack IoT devices. The virus contained a series if IP address ranges to scan and a table of default login credentials for a number of common IoT devices. When infected, each device would scan the IP address space looking for IoT devices with open Telnet ports (typically 23 and 2323). Mirai would then attempt to log-in into the device using the list of default login credentials embedded in the code. Once logged in, the virus would be uploaded to the device and information about the newly discovered device would be sent to a central server. The virus code typically was only stored in volatile RAM memory on the device and if the device was rebooted, the code would be removed. However, the device would become re-infected within a few minutes based on the data stored about the device when it was first infected. The IoT devices successfully infected by Mirai quickly became the largest botnet in Internet history at that time. Later in 2016, the Mirai botnet was responsible for the largest denial of service attack in the history of the Internet when the botnet was used to shut down the website of well-known security researcher and reporter Brian Krebs.

Lessons learned from this story include:

- The need to change device credential before a device is deployed
- Isolate devices from the Internet and prevent direct Internet access
- Disable insecure network services like Telnet

While Mirai was not used this way, remember that each of the infected devices could have been used to scan internal networks to locate vulnerable servers and desktop machines within the company networks.

6 Company Wide Mitigation Strategies

In the previous section we looked at mitigation strategies designed to address specific vulnerabilities. In this section we look at broader enterprise mitigation strategies to reduce the general risk of deploying IoT within the company. Some of these strategies are also good IT practice in general, but are often neglected in IoT deployments.

Mitigation strategies can be based on controls (technical, process) behavioral changes (training, awareness) or detection/response (monitoring, containment). Defense in depth requires a mixture of many interrelated strategies and, more importantly, ongoing assessment of their effectiveness. This allows for a model of continuous improvement that is critical in the prevention of cyber-attacks.

6.1 Network Isolation

Even the latest firmware and software can't address zero-day vulnerabilities before they can be exploited. Zero-day vulnerabilities are those that are not discovered until the device or software is deployed in production. The danger of a zero-day is that it can often be exploited before a fix can be deployed. These vulnerabilities may exist for years until they are discovered.

Network isolation is a strategy to limit the sources of potential attacks reducing the scope and risk of zero-day attacks and vulnerable firmware. This strategy isolates IoT devices to their own physical or virtual network segments. These Virtual Local Area Networks known as VLANs can easily be created using the routers and firewalls that configure and control the networks. Access to the IoT segments is limited to only those systems that need to access the devices within the isolated network segment. Access is typically controlled by firewalls or gateways.

Devices that must accept Internet connections from outside the organization should be in a demilitarized zone (DMZ). A DMZ is a special network segment that has a firewall controlling access between the protected segment and the Internet, and another firewall controlling access between the protected segment and the other networks within the business. These firewalls limit both incoming and outgoing connections restricting access to the devices to a very limited number of systems.

6.2 IoT Logging and Monitoring

Log files are generated line-by-line by systems describing what is occurring in the system when the log entry is created. The entries often fall into three or more classifications with the most common being error, warning, and informational or info. Error entries each describe an error that occurred during processing. Warning entries which warn about a possible problem, and informational entries describe less important events. The types of log entries generated and the amount of log output is a common configuration setting on many systems.

IoT devices may generate a lot of log data but may not have enough storage to collect this data internally. Yet these logs typically need to be collected, aggregated, processed, filtered, summarized and monitored so appropriate alarms can be raised to inform the system operators that actions must be taken. This log data collection and analysis may be part of an IoT solution or third-party logging tool used to collect, process and analyze the data generated from IoT devices.

Data generated from IoT devices can indicate everything from the operational state of the device to the conditions of the situations the device is designed to measure. Log message structures can contain information such as date, time, device ID, status, values, etc. IoT devices may have single functions or multiple sensors on them that generate a higher amount of data. More complicated devices may report on many different conditions across a variety of areas. Event logging locations can exist locally on a server, an appliance or in the cloud for aggregated event logging.

Different IoT devices may use different strategies for logging and monitoring. Devices that generate a large volume of data often have more advanced solutions for collecting the log data. When passing large amounts of data to the cloud is not feasible, some devices provide more onboard computing capabilities. Newer advanced models are moving toward edge computing where the processing of IoT data is closer to the edge of the network providing insights in a timelier fashion.

In addition to logs generated by the devices themselves, it is also useful to monitor IoT related network traffic to understand where incoming messages are coming from and where outgoing messages are being sent. Monitoring the network for security should help in understanding: if the IoT devices are sending data securely, if the data can be manipulated on route, or if the data integrity is being maintained.

6.2.1 Monitoring and Alarming

"If a tree falls in a forest and no one is around to hear it, does it make a sound?"

This famous thought experiment applies to logging (capturing messages not cutting trees) and monitoring as well. Log and monitoring outputs must be observed. Of course, this would be a tedious job for a human to do. This is why most monitoring systems can be configured to raise alarms when analysis shows something has happened that is out of the ordinary. Each alarm should be investigated by a person and if the alarm isn't relevant then the analysis should be modified to prevent the alarm from being generated. Otherwise, the cause of the alarm should be addressed and corrected.

6.3 Network Monitoring

Monitoring of assets and events occurring within a network is an essential component of any cyber security program. Hoteliers should consider establishing a monitoring capability for all of their IoT systems with the goals of:

- Enabling visibility of out-of-policy configurations
- Identifying unauthorized devices being inserted onto hotel networks
- Recording security-relevant events occurring across a system

Traditional IT assets such as servers and workstations log events as they occur and store those events in files which are then accessed by or transmitted to cyber security monitoring software. IoT systems are often disadvantaged in terms of logging capabilities given that there is no room to install an agent and not all devices write events to logs. The integrity of the log files stored on IoT devices can also come into question if the proper permissions or integrity-protections are not applied to the device file structure. Even so, hoteliers should begin to have conversations with their IoT suppliers to include monitoring requirements in RFPs. For example, at minimum, IoT devices should log the following events to a file as they occur.

- Authorized access to the device
- Attempted unauthorized access to the device
- Changes to critical device configuration such as authenticators/passwords
- Firmware updates

In addition, metadata about the events should be logged. This includes at minimum, the username of the actor that performed the event and a timestamp.

Monitoring the health and status of IoT assets can also provide visibility into potential security-relevant events. For example, monitoring either the rate of battery consumption or the CPU utilization can identify spikes that could indicate abnormal processing requirements such as being part of a botnet, or simply be an indication that a device is not functioning as normal. In certain use cases, monitoring for unexpected geo-location changes can also identify potential misuse.

A robust monitoring program can also aid security administrators in identifying IoT device configurations that are not compliant with organizational policy. This can include connection security configurations, networking configurations, and identity and access management configurations. Monitor devices and alert on out-of-policy configurations to allow quick resolution.

A monitoring program will include procedures for accessing log files, rotating log files off devices and storing log files. Logs should be rotated off devices on a routine basis to ensure that they do not exceed storage capacity and are not subsequently overwritten. Logs may be sent to a gateway or to a cloud service for storage. Logs may also be evaluated in near-real-time by enterprise systems that support alerting.

Network data should be correlated with IoT device logs as well. Network security infrastructure can provide valuable data related to potential misuse of a system. Logs generated by firewalls, intrusion prevention and detection systems, and other network security devices can quickly capture and flag traffic being sent to unexpected endpoints or over unexpected ports. Additional events that can be logged within the supporting network include:

- Repeated connection attempts
- Scanning for topics
- Abnormal termination of connections
- Device no longer reachable

The Radio Frequency (RF) layer can also provide useful information. RF monitoring may be conducted on a periodic basis to identify data leakages associated with the RF communication layer of an IoT implementation. For example, IoT devices may support beacons that signal device location. RF monitoring can also be used to identify devices attempting to connect to RF networks such as ZigBee and ZWave.

Effective monitoring requires time to tune the various system components in order to reduce false positive rates. This requires a good understanding of the baseline behaviors of the devices and other assets that compose the IoT system. Once these baseline behaviors are understood, thresholds for events and standard operating expectations can be defined and then turned into security rules that trigger alerts.

6.4 Cyber Security Insurance

Most companies like to feel that they are doing what is required to secure their technology exposure to cyber-attacks. However, technology solutions are only getting more complicated and companies may also want to have additional plans to help mitigate the risk of cyber incidents to keep the company operating. Each year only brings greater risk through larger and more costly breaches. When it comes to limiting a company's exposure to technology security risks, a company may seek out cyber security insurance to help cover the costs associated with investigation, business losses, dealing with privacy governance and legal activities. This is a new and still developing area of insurance.

Getting into a cyber security insurance agreement may require a discovery assessment to better understand where the company is today in IT and IoT exposure.

Cyber insurance policies vary in the types of incidents and expenses covered as well as the additional benefits provided. For example, policies may cover incidents such as:

- Cyber hacking
- Cybercrime and extortion

- Denial of service attacks (DDOS)
- Data breaches and loss of data
- Disclosure of both internal and external private and confidential information

When analyzing a policy, companies should be aware of the types of expenses that are covered and weigh the expense of the coverage versus the perceived risk. Some of the typical expenses that may be covered depending on the policy include:

- Technical expenses to investigate and stop the attack
- Forensic analysis
- Regulatory fines and penalties
- PCI (Payment Card Industry) assessment
- Post-incident public relations costs
- Defense/legal costs including potential third party lawsuits
- Damages and claims
- Breach response costs such as credit notifications or monitoring services
- Business interruption costs such as loss of income and the cost to restore the business operations
- Financial losses due to theft through misdirected fund transfers
- Damage to hardware, software and data assets
- Data compromise liability

Cyber insurance carriers often provide additional benefits to policy holders which aid in proactively reducing the risk of an incident occurring. Some of these benefits include regular security audits, compliance assistance and pre-incident response planning.

Even after a policy is in place, if the covered company does not meet the minimum duties and responsibilities outlined in the policy, the company is at risk of not being covered at the time of an incident.

7 IoT Security Patterns

Design patterns are repeatable solutions to commonly occurring problems. Security Design Patterns provide an easy-to-understand approach to mitigating vulnerabilities that can often be exposed within a system. Organizations and administrators are able to choose the patterns that best apply to their implementations. These different patterns include:

Gateway-Security Pattern

The gateway-security pattern provides single entry and exit points for messages between IoT devices and the outside world. The gateway acts as a gatekeeper to verify credentials and validate incoming messages to enforce policies for both incoming and outgoing messages.

Isolation or Bulkhead Pattern

Isolate IoT devices to their own network segments that are separate from other segments in the business. This pattern typically uses VLANs or physically separate networks. VLAN access may be controlled by firewalls or gateways designed to control and limit access to resources within the network segment.

Defined Communications Pattern

Limit messages so they can only travel between approved devices. This is typically implemented using a control list of approved message destinations which effectively limits communications to only approved peer devices and services. Note that this may be enforced by a gateway or firewall.

Secure Channel Communication

Provide a secure channel of communication between two or more parties, in this case, between an IoT device and a connecting system. This can be accomplished using Transport Layer Security or point-to-point encryption (P2PE) for example.

Message Confidentiality Pattern

Message confidentiality controls and prevents eavesdropping by encrypting the messages before they are sent and decrypting the messages when they are received. This is also known as point-to-point encryption or P2PE.

Message Integrity Pattern

The integrity of a message is verified to make certain the message was not damaged or changed during transmission. This is typically done by calculating some sort of error code (for example, parity bits, a hamming code or a Luhn check), or by using algorithms such as checksums, Cyclical Redundancy Checks (CRCs), or various hashing algorithms including MD5, SHA-1, or SHA 256. Once the number has been calculated for the received file, it is compared to the number calculated by the sender prior to the file being sent. The integrity of a message should be confirmed prior to any further processing of the message.

Sender Verification Pattern

The sender of a message can be verified typically using digital signature technology. Additionally, it is possible to ensure that the message has not been modified after the signature was applied.

Secure Logging Pattern

The secure logging pattern captures and securely writes a message describing any attempted access to the IoT device. A best practice is to capture both network and direct hardware access attempts including tamper alarms. Direct access might include serial port or JTAG (Joint Test Action Group) access for example.

Secure Pairing Pattern

Configure devices to require secure pairing procedures in order to communicate with device peers. Only allow guests to pair with devices that are explicitly designed for guest interaction.

8 Recommended Policies

Throughout this paper, methods and techniques have been described that will help hoteliers securely onboard and manage their IoT environment. However, those methods must be transcribed into formal policies within organizations so that they are carried out effectively. Formal policies are more than just suggestions; they are a deliberate set of steps and procedures that guide decision making. No one person or department can be wholly responsible for the security of your organization's environment and data. Even the best designed solutions can be undermined by well-intentioned individuals who do not have the necessary guidelines and support to be successful.

The following sections highlight some best practices that organizations may wish to adopt as formal policies. The inclusion of these policies should be considered a part of an organization's entire cybersecurity framework.

8.1 General Policies

- Each device on the network should have a unique identifier
- IoT devices are isolated from business and guest networks. Where access to the IoT devices is needed, the access is controlled via gateways and/or firewalls and is limited to only those systems that need to connect to the IoT device.

8.2 Acquisition and Lifecycle

When purchasing IoT devices, the following must be considered:

- There must be support to securely update the device.
- The device should support a secure means of updating keys, certificates, signatures and other secrets stored on the device.
- A secure means of storing keys, certificates and other secrets on the device must be provided.
- Devices must support a means of secure communications.
- The period of firmware and software support by the manufacturer must be considered as a part of the lifecycle cost evaluation.
- Dependencies on and the life-cycle of additional web- or cloud-based services required to effectively use the device must be considered as a part of the lifecycle cost evaluation.
- Impacts on guest, customer and employee privacy must be analyzed, and a mitigation plan must be in place for each type of IoT device before the devices are deployed. User or customer data must be removed from devices between each different user.
- A plan must be provided detailing how a device is securely retired when it is removed from service at the end of its life. This should include sanitization of the device to remove any remnant customer data.

8.3 Credential Management

- Default credentials are changed before IoT devices are deployed and accessible.
- Establish credential standards for IoT devices include:
    - Password length
    - Mix of upper and lower case letters, numbers and symbols

- Credentials are regularly changed on each device. The frequency of credential change for each device needs to be established based on risk and company policy but should be at least quarterly.
- Device credentials are not shared between users. If needed, a credential proxy or other means are used to support individual identities for each user even if the device supports a limited number of identities.
- Roles are defined for each type of device used to limit users to the services that they need to access. These roles may be pre-defined by the device and built into the device, or may be enhanced using a gateway or proxy. Typically, there should be at a minimum separate administrator and user roles.

8.4 Firmware Updates

- New device vulnerabilities and the availability of firmware updates for each type of IoT device are monitored regularly.
- All IoT devices must have secure update capabilities. At a minimum, update images must be signed and the signature must be verified before the update is installed.
- A plan to address devices that are no longer able receive firmware updates must be in place when a new type of device is deployed.
- Vendor update policies and the expected period of time the device will be supported by updates must be considered as a part of the acquisition process.

8.5 Certificates and Secrets

Certificates and keys may come in public and private forms. Private certificates are a secret that must be protected. Most certificates are backed by a third party known as a Certificate Authority (CA) that verifies the certificate. Most certificates also have a limited time period for which the certificate is valid.

Encryption keys are used to encrypt and decrypt messages and are required for secure communication protocols like HTTPS. Both private keys (used in asymmetric encryption algorithms) and shared keys (used in symmetric algorithms) must be protected.

- Each IoT device must have a secure means of storing private keys and other secrets.
- Each IoT device must have a means of updating private keys and other secrets.
- Expiration dates of certificates are monitored and a plan is in place to replace the certificates on the device before the current certificate expires.
- Shared keys should be rotated (changed) on a periodic basis.

8.6 Secure Communications

- IoT devices must support secure communication protocols like HTTPS and SSH.
- IoT devices are configured to use only secure communication protocols and insecure protocols are disabled.

8.7 Auditing, Monitoring, Tracking and Alarming

Monitoring and Alarming

Each IoT device is monitored to track access and incoming and outgoing messages. Alarms are established to warn of atypical behavior. Alarms are investigated and alarm parameters may be modified to reduce false or insignificant alarms. The health and state of the infrastructure supporting the IoT devices is also monitored.

Establish an Operational Baseline

For each IoT device and system, the expected and observed behavior of the device is captured and documented to establish a baseline. This includes known and approved communication paths (IP addresses), ports and protocols. This baseline is used when analyzing events as they occur to determine if the device is operating within norms.

Track the IoT Inventory

Inventory and asset management procedures are established for all IoT devices. Establish naming conventions and metadata (attributes) that allow for the easy understanding of device type, location, owner and function. Manage both hardware and software, and establish visibility into third party software used within devices.

Incident Response

Incident responses plans are created for each type of IoT device to address both security incidents and outage recovery. Each device is assigned a priority used to evaluate and establish the system in terms of expected incident response timelines. Escalation procedures are established to address systems under attack or to deal with unexpected security incidents.

Auditing

An audit is periodically performed to ensure that IoT devices are in compliance with the IoT device policies and procedures.

9 Other Considerations

As hoteliers consider adding devices initially intended for the consumer space, such as Amazon Alexa, Apple TV, Google Home, etc. to their properties, hoteliers should review the data collection policies and the terms and conditions associated with each device. Many of the devices, particularly the voice assistant devices and entertainment devices, collect what may be considered personal information. In the consumer space, the consumer agrees to the terms and conditions associated with the data collection.

In a lodging environment, the guest does not have a clear way to agree or decline the data collection. As hoteliers consider deploying these devices in the rooms on their properties, they should ensure that they are not exposing themselves to legal and/or regulatory liability (e.g. GDPR, CCPA) through the use of any of these devices. It is recommended that hoteliers consult their legal or privacy counsel to help address this.

10 Conclusion: Best Practices for IoT Security

The goal of this document has been to help the reader to understand the added risk that IoT adds to hotel organizations. This paper has tried to provide an understanding of the reasons behind the added risk and limitations of many IoT devices. Mitigation strategies for specific vulnerabilities and techniques and best practices that can be put into place to manage the risks have also been discussed. In conclusion, the risk of deploying IoT devices in a hotel environment is manageable.

Management begins before the acquisition process! Before purchasing devices, make certain the impact on guest and employees has been evaluated and is understood. When selecting a device to purchase for deployment make sure they address the following capabilities:

- Ability to securely update the devices' firmware
- Ability to change passwords
- Ability to communicate securely by supporting current HTTPs and other related transport
- Ability to disable legacy protocols such as Telnet if they are implemented on the device
- Ability to securely manage secrets such as encryption keys and on-device passwords

As the devices are deployed:

- Update firmware to its most recent release
- Change default passwords to new secure passwords
- Deploy IoT devices to isolated network segments so if a device is compromised it has no access to other systems
- Disable insecure protocols and unused services, and enable secure protocols and communications
- Install and/or update security certificates

As the devices become a part of the operational routine make certain:

- Passwords are changed on a regular basis with new secure passwords
- IoT devices and networks are monitored and logs and alarms are reviewed
- IoT policies are established and enforced
- Firmware and software updates are monitored and applied

Following the advice provided within this document should significantly reduce the potential risks of operating IoT devices in your environment.

11 Appendices

11.1 Useful Resources

The list below of linked resources provides additional supplemental information and context:

- HTNG IoT Workgroup's "How Hospitality Can Win with IoT" White Paper
- HTNG IoT Workgroup's "Internet of Things Fundamentals" White Paper