INTERNET OF THINGS FUNDAMENTALS

Version 1.0

16 July 2018

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.

Contributors: Ted Harrington, Independent Security Evaluators; Florian Gallini, Interel; Florian Kriechbaumer, Interel; Cody Morash, Telus; John Harvey, LEGIC; Steve Garnjobst, Datatrend Technologies; Parminder Batra, TraknProtect; Matthew Fitzgerald, Ubiquiti.

Table of Contents

1 Document Information

The Internet of Things (IoT) is a topic that is often discussed, but not yet well understood. And for hoteliers who do understand what IoT is, there is still a lack of understanding as to how they can best make use of the myriad connected device options available on the market to improve guest experience and internal operations. This white paper will provide strategies to get started with IoT, highlight best practices for implementation and provide real-world examples of successful implementations through the use of case studies.

1.1 Document Purpose

The intent of this white paper is to help the hospitality industry pave a path for successful adoption of connected devices. To achieve successful adoption of connected devices, three things must happen:

1. Issues must be understood by those working at the property level
2. Issues must be understood by those working at the brand level
3. Security must be robustly integrated into system design and implementation

Benefits to both business and guest are the driving forces toward adoption of connected devices; at the same time, security compromises are the biggest threat to adoption and delivery of the associated benefits. This document will provide the necessary insight, documentation and guidance to accomplish the three points above, while additionally addressing security concerns and best practices.

1.2 Scope

The purpose of this document is to outline best practices for designing, implementing and maintaining IoT solutions in a secure manner. The goal is to empower industry members to make informed decisions about IoT and help them navigate on a path toward successful adoption of IoT, within the context of their objectives. This white paper is designed to outline *ways of thinking* of how to approach this technology rather than *prescriptive steps* for how to approach this technology - it is not intended to be published as an industry standard or compliance framework.

1.3 Audience

This document has been created for HTNG members, notably the technical and executive leadership at hotel brands, interested to deeper understand how and why to deploy systems in a secure manner.

This white paper is built upon the assumption that the readers are familiar with IoT and why they might benefit from it. For readers who do not already have this baseline understanding, please consult the IoT workgroup's "*How Hospitality can win with IoT*" resource.

1.4 Definition

There is no universal definition of IoT, but for the purposes of this white paper, IoT has been defined by:

IoT consists of devices that have been made intelligent through an ability to ***communicate*** *and* ***interact*** *with the* ***physical world.***

Hospitality IoT includes examples like:

Guest Room Devices	Back of House Devices	User-Owned Devices
• Air sensor • Alarm clock • Blinds • Lighting • Lock system • Minibar • Motion sensor • Service button • Shower • Smart TV • Telephone • Thermostat • Voice assistant • Water management	• Access control system • Boiler • CCTV • Chiller • Fire alarm • Pump	• Casing device • Gaming system • Laptop • Smartphone • Smartwatch • Tablet

2 How to Get Started with IoT

When reviewing the considerations that have to be taken into account, it may seem that the upfront investment – human, knowledge and financial capital – required to deploy an IoT solution is significant. However, good practices exist for a simplified IoT adoption roadmap in a four-step process.

Source: INTEREL

2.1 Identify

Identify a use case that promises a high value-add from IoT technology. While it may be tempting to identify a technology and then look for an application, chances for stakeholder buy-in and success are higher when the expected benefit can be clearly articulated and measured. The ideation phase should be concerned with discovering possible business processes that can benefit from an IoT application. For example, try analyzing known pain points in the organization and assessing their fit for an IoT project.

2.2 Develop

Develop your prototype or proof-of-concept. Here, the goal is maximum impact with minimum investment. There may be an existing solution that addresses the majority of the requirements out of the box. This will help you to prevent high upfront investment of a custom solution and allow you to evaluate whether the problem in Step 1 can be resolved with an IoT deployment. A proof of concept could be deployment in a corporate lab, a single room in a hotel, or an entire hotel, subject to the type of application.

2.3 Strategize

Once the concept has proven itself successful, a strategy for a full rollout needs to be established. During this phase, non-functional questions such as scalability, process automation, security assessments, financial modelling, business system integration, resource planning and the fit into the overall enterprise architecture and infrastructure all need to be answered. Building on upgradeable, future-proof technology is key given the long IT upgrade cycles in today's hospitality environment.

2.4 Monitor

Once you've completed the first deployment, you will need to begin monitoring and managing user feedback, device lifecycle and performance. A robust IoT management platform with applications for data collection and analysis is critical for ongoing success.

There are several vendors that offer out-of-the-box IoT devices, infrastructures and applications who are willing to invest in the methodology above and adopt the right consultative approach to ensure joint success.

Sharing results of both prototype and scaling stages in projects with vendors is critical to enable them to steer their product development initiatives in line with market requirements.

3 Best Practices

No matter how much time is spent researching individual device options and applications, no implementation will realize its full potential without a focus on the big picture implications IoT has on the business. The best practices captured below highlight integration, infrastructure, management platforms, big data, people and processes, security and privacy perspectives to help guide a company to get the best return for its IoT investment.

3.1 Integration

In order to effectively support diverse applications in an IoT installation, it is necessary to choose an underlying architecture which is independent of the applications it will support. Application-specific logic and data should be separate from the underlying architecture, with the architecture being flexible enough to support a wide variety of applications.

For example, a smartphone app used by a guest should easily support not only “Mobile Key” functionality for opening their guest room door, but also allow entry to the hotel parking garage, the locked wardrobe in the room and additionally support folio charges from on-site vending machines. The app provides the single front end for security and authentication to support multiple feature sets.

The same approach applies with device-to-device communications in the guest room. For example, a room door lock communicating with a room controller to send a “guest has opened the door” notification to trigger a Welcome Scene, can at the same time communicate this event to a central server for security purposes.

So, how can this be achieved?

For smartphone-to-device IoT applications, the guest-facing mobile app should incorporate a software development kit (SDK) or library which can manage multiple distinct application files. Addressing the files by a device should allow for a unique and mutually authenticated selection of the correct device-specific application file. Applications should be digitally signed to ensure the provenance of the application, using application-specific encryption keysets kept in a secure storage component. Only a device which is authenticated to access, decrypt and read the device-specific application file will be able to communicate with it (i.e. a door lock reading a file containing a mobile key).

It is recommended that the size of the files should be flexible to allow each application/device provider to determine the amount of data required for their application. A transparent channel to allow a device to securely communicate to the mobile app GUI and to the mobile app’s management server via the SDK is advisable. In this manner, additional user input such as a PIN code for entering a fitness room locker or room safe can be requested by the lock device without the SDK having to control this application-specific conversation.

Similarly, device-to-device communication can allow diverse devices to mutually authenticate through a secure Bluetooth mesh connection, allowing the exchange of application-specific data between related devices.

3.2 Infrastructure

While this document is not intended to address a prescriptive IoT reference architecture, the following concepts are important to keep in mind when designing your own architecture:

- Communication between devices and the path to the cloud

- Suitability and security of chosen protocols for an environment where physical validation and access cannot be controlled
- Cross-compatibility between devices from multiple vendors
- Upgradability and control of software running on the devices
- Data processing, storage and analytics
- Integration with existing business and legacy systems

It's essential to consider these factors during the prototype stage to avoid fundamental flaws that will be costly and difficult to address in later stages.

Figure 3.2.1 represents a non-exhaustive list of topics planners must take into account when designing their approach to the IoT infrastructure. The majority of the unknowns in today's hospitality IT domain lie within the local and fog layers, IoT device and infrastructure management components and the ability for the entity's big data business insights infrastructure to cope with the data generation expected by IoT.

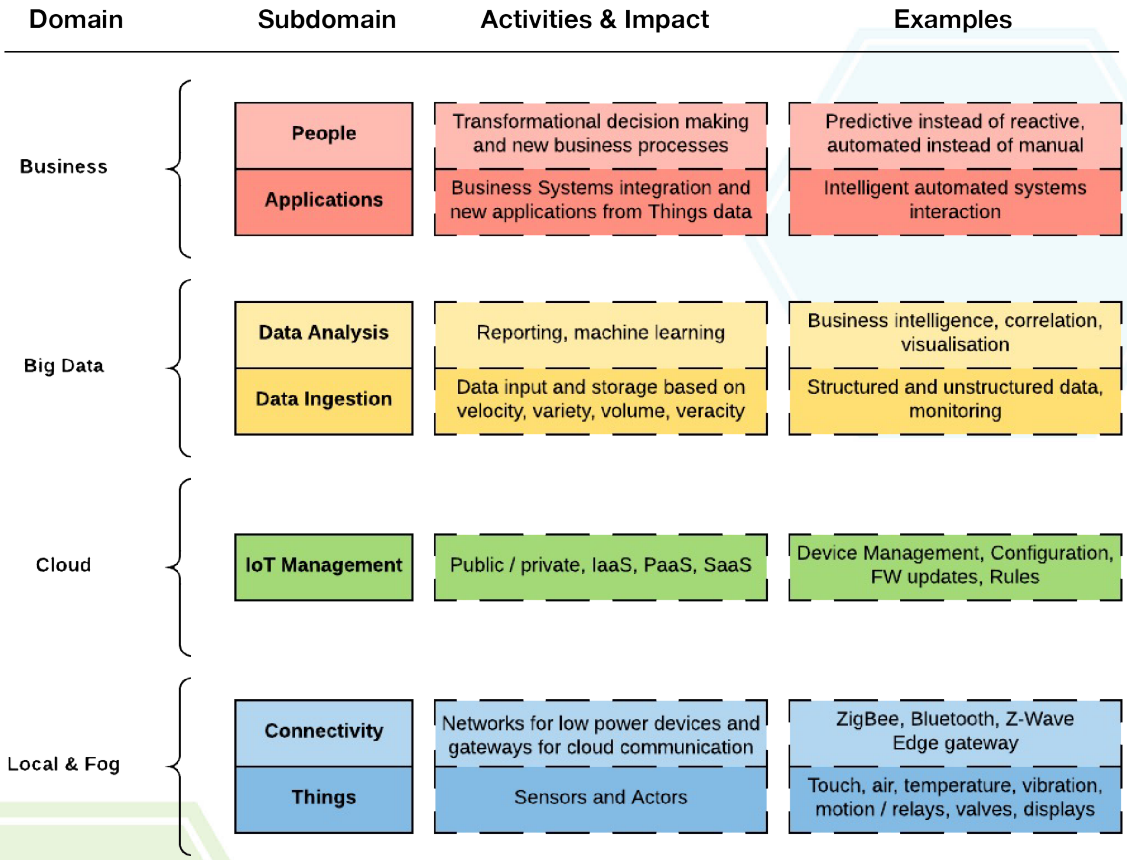


Figure 3.2.1

3.2.1 The Local & Fog Domains: Things & Connectivity

IoT requires a major shift from the traditional network infrastructure as IoT devices follow non-traditional communication paths. Existing digital communication in the hotel is largely managed using TCP/IP-based

networks but connected objects typically do not have the ability to utilize the existing Wi-Fi or Ethernet infrastructure due to size and power constraints.

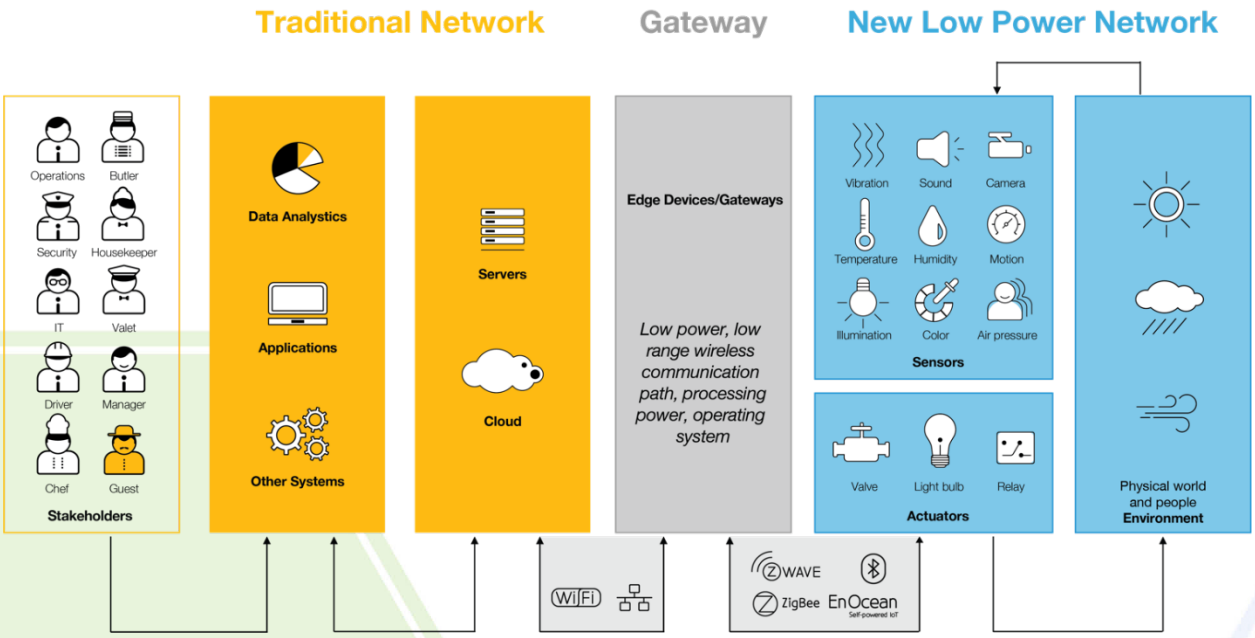
This limitation spurred the development of several low power wireless technologies with varying characteristics around energy consumption, application definition, standardization and certification requirements, bandwidth and range. The most common low power wireless technologies are compared in the table below.

IOT WIRELESS TECHNOLOGIES

Technologies	Standards & Organizations	Network Type	Frequency (US)	Max Range	Max Data Rate	Max Power	Encryption
WiFi	IEEE 802.11 (a,b,g,n,ac,ad, and etc)	WLAN	2.4,3.6,5,60 GHz	100 m	"6-780 Mb/s 6.75 Gb/s @ 60 GHz"	1 W	WEP, WPA, WPA2
Z-Wave	Z-Wave	Mesh	908.42 MHz	30 m	100 kb/s	1 mW	Triple DES
Bluetooth	Bluetooth (formerly IEEE 802.15.1)	WPAN	2400-2483.5 MHz	100 m	1-3 Mb/s	1 W	56/128-bit
Bluetooth Smart (BLE)	IoT Interconnect	WPAN	2400-2483.5 MHz	35 m	1 Mb/s	10 mW	128-bit AES
Zigbee	IEEE 802.15.4	Mesh	2400-2483.5 MHz	160 m	250 kb/s	100 mW	128-bit AES
THREAD	IEEE 802.15.4 + 6LoWPAN	Mesh	2400-2483.5 MHz	160 m	250 kb/s	100 mW	128-bit AES
RFID	Many	P2P	13.56 MHz, etc.	1 m	423 kb/s	~1 mW	possible
NFC	ISO/IEC 13157 & etc	P2P	13.56 MHz	0.1 m	424 kb/s	1-2 mW	possible
GPRS (2G)	3GPP	GERAN	GSM 850/1900 MHz	25 km / 10 km	171 kb/s	2 W / 1 W	GEA2/GEA3/GEA4
EDGE (2G)	3GPP	GERAN	GSM 850/1900 MHz	26 km / 10 km	384 kb/s	3 W / 1 W	A5/4, A5/3
UMTS (3G) HSDPA/HSUPA	3GPP	UTRAN	850/1700/1900 MHz	27 km / 10 km	0.73-56 Mb/s	4 W / 1 W	USIM
LTE (4G)	3GPP	GERAN/UTRAN	700-2600 MHz	28 km / 10 km	0.1-1 Gb/s	5 W / 1 W	SNOW 3G Stream Cipher
ANT+	ANT+ Alliance	WSN	2.4 GHz	100 m	1 Mb/s	1 mW	AES-128
Cognitive Radio	IEEE 802.22 WG	WRAN	54-862 MHz	100 km	24 Mb/s	1 W	AES-GCM
Weightless-N/W	Weightless SIG	LPWAN	700/900 MHz	5 km	0.001-10 Mb/s	40 mW / 4 W	128-bit

Source: http://www.mwrf.com/systems/4-major-m2m-and-iot-challenges-you-need-know

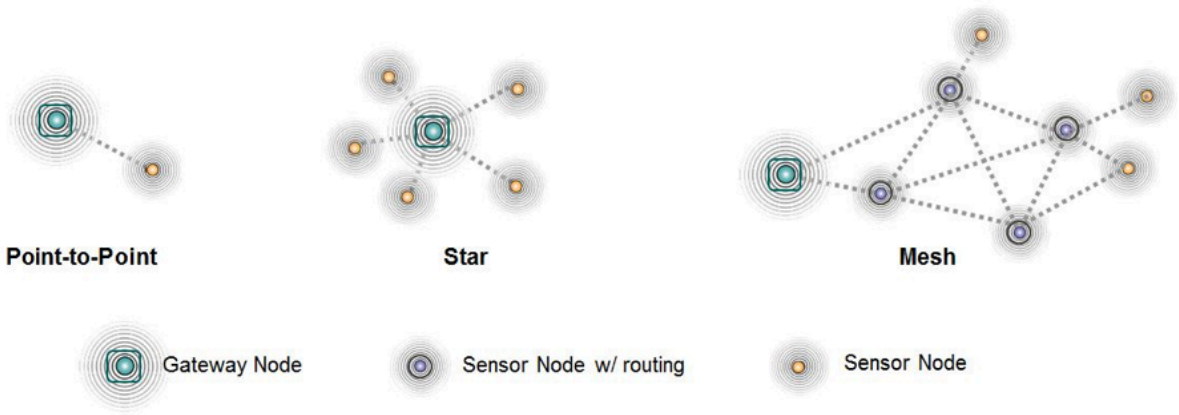
As a consequence, hoteliers need to be in control of new types of networks to orchestrate the communication of IoT devices amongst themselves, into existing on-premise networks and into the cloud. This is often facilitated by gateway, or "Fog," devices located at the edge of the local and cloud networks, as shown in the figure below.



Source: INTEREL

Within the new low-power network, three options exist for communication patterns:

1. Point-to-Point: Direct point-to-point communication between objects that need to exchange data
2. Star Architecture: End nodes are all connected to a central gateway that has the intelligence and processing power to take actions and process data
3. Mesh: Non-hierarchical and decentralized network across various objects in order to deliver data to and from a specific end node



Source: ***http://radar.oreilly.com/2014/04/3-topologies-driving-iot-networking-standards.html***

Understanding which option is adequate for which use case depends largely on the specific implementation factors, such as the:

- Number of devices to be connected
- Complexity and amount of data to be transmitted
- Requirements for latency and resiliency
- Communication protocols in use
- Communication range required
- Battery life constraints

Regardless of the communication pattern you choose, it is important to consider the security, commissioning, maintenance, standardization and upgradability implications of your deployment.

3.3 IoT Management Platforms

Fundamental capabilities of IoT Management Platforms include:

- **Provisioning and Authentication**: to enroll devices and ensure network access is restricted to devices with the proper credentials
- **Configuration and Control**: to remotely configure, reset and update devices
- **Monitoring and Diagnostics**: to minimize device downtime and receive alerts in case of issues
- **Software Updates and Maintenance**: to remotely install software updates
- **Data Export**: to share device data with other applications, i.e. analytics software
- **Integration**: to link device management with business applications

The marketplace for IoT management platforms is still developing, with no clear industry leader(s). When evaluating IoT management platforms, the following broad characteristics may be helpful:

- **Range of Features**: Platforms offering the broadest range of feature sets are best suited to manage service providers, or organizations with skilled technical staff, due to the complexity of integration and management. When selecting an IoT management platform, consider the tradeoff between features and ease of use. Organizations with limited in-house technical capabilities and complex requirements may decide to outsource IoT management.
- **Commercially Licensed vs. Open Source**: As with other software platforms, organizations must weigh the benefits of lower up-front costs and vendor lock-in avoidance against the limited support and less-defined roadmap typical of open source platforms.
- **Vendor-specific vs. Multi-platform**: Vendor-specific platforms typically offer streamlined deployment, more robust support and greater simplicity while multi-platform options offer greater flexibility. Vendor-specific solutions are typically best suited to business-critical systems where seamless integration and simplified support are paramount.
- **PaaS vs. DIY**: While do it yourself (DIY) IoT management platforms are available, cloud-based platform as a service (PaaS) is the predominant model for IoT management. A PaaS solution offers ubiquitous geographic coverage and fast deployment for widely dispersed organizations.
- **IoT Development Toolkits**: For organizations with significant software development resources, IoT toolkits provide the means to deploy custom IoT management platforms with tight integration into existing business applications. However, IoT toolkits typically don't provide ready-to-use management tools. Deploying off-the-shelf IoT management applications for initial project phases, followed by a planned migration into a custom platform can speed up time to a full deployment.
- **Cellular Network Support**: Management platforms provide varying degrees of support for cellular networks, which is typically required for global and/or remote location deployments. Cellular network use can also offer faster deployment with minimal to no impact to existing data networks.

3.4 Big Data – Data Ingestion and Analysis

While the new networks represent a major infrastructure shift, connected objects are also going to serve as a significant driver for a second prominent technology trend – big data. The ability for IoT devices, or "Things," to generate and exchange information will serve as an additional data generator for hotel systems in large volume, variety, velocity and veracity – commonly known as the 4 V's of big data.

Table 3.1 shows some examples:

Attribute	Item	Example
Volume	Thermostat	Frequent regular data transmission, such as sending current room temperature every few minutes
Variety	Location Tracker	Large amounts of unstructured location parameters that have to be interpreted into meaningful mapping data
Velocity	Panic Button	Realtime information has to be sent with minimum latency
Veracity	Lock	Accuracy of data and quality of service is paramount for security-critical information

While it is not the focus of this white paper, it is advisable for hotel IT infrastructure planners to consider these factors when designing their data warehouse and analytics systems.

3.5 People, Processes & Application

The greatest business benefits of an IoT deployment can be found with the decision making that IoT-generated data can enable. This includes the representation and interpretation of data collected by things, stakeholder interaction with things and integration and interaction of IoT with other business systems.

As described in the workgroup's resource, "How Hospitality can win with IoT," there are numerous benefits IoT can offer to hospitality stakeholders in the form of easy-to-understand reports, simple-to-use applications and tightly connected systems that optimize operational workflows to deliver maximum ROI. The infrastructure should deliver easy and ubiquitous access to these tools. To do so, start by identifying the various user personas and their goals for interacting with the capabilities of IoT devices. Table 3.2 shows a basic starting point for a persona needs assessment.

Stakeholder	Focus Areas
General Manager	Operational efficiency, guest experience
Engineering	Energy & water savings, equipment maintenance, remote monitoring
IT	New network deployment, devices, security, enablement
Housekeeping	Staff efficiency, guest service optimization
Guest Services	New guest interaction
Marketing	Personalization, analytics, advertising
F&B	Inventory, quality control
Security	People safety, access control, incident management
Owner / Franchise	ROI, privacy
Brand	Loyalty, central control, privacy, ROI
Guest	Personalization, new experiences

3.5.1 Dashboard Monitoring and Analytics Reporting

Every hospitality technology platform requires the ability to capture actionable insights regarding the health of the system, and IoT enables this capture. Knowing the real-time status of devices in a guest room, and throughout the hotel, is critical for maintaining high guest satisfaction ratings. Additionally, IoT analytics can play a key role in providing actionable insights on operational processes, policies and standards to support the guest experience. Through the measurement of resources, staff, systems and devices, the hotelier can determine if KPIs are being achieved, whether resources are being utilized effectively, monitor trends and forecast resource requirements.

Types of analytics:

- Device monitoring, dashboard reporting and cross-system alerting for a single site or across multiple properties
- Guest location (e.g. geo-fencing airport to detect arrival)
- Operational effectiveness

Executive staff	• Executive KPI reporting
Front desk	• Front desk KPI reporting

	• Resource and asset tracking
Housekeeping	• Guest room status including occupancy detection • KPI reporting for housekeeper time/motion and location • Asset tracking
Engineering	• Maintenance issues (duration based and real-time) • Energy management
Food and beverage	• Deliveries • Food safety • Minibar replenishment • Tray removal from hallways
Marketing	• Location-based offers • Preference-based offers
Security	• Bad guy detection and identification • Emergency response • Staff safety

3.6 Security Challenges that Are Unique to IoT

IoT introduces a handful of security challenges that are unique to this type of technology. These challenges impact defense paradigms and must be accounted for in threat models and trust models that vendors and hoteliers alike deploy. These challenges include:

- ***Limited resources***. Many connected devices are physically small and are packed with components. These conditions put a natural limit on computing power. Connected devices in some cases are battery operated, while in others are hardwired for power. In either case, energy consumption may be limited as compared to larger devices with higher levels of computational power. Taken together, all of these factors make it difficult to implement cryptography and other security best practices.
- ***Limited ability for user interaction***. Many connected devices lack visual displays, user-oriented buttons, or other methods of user interaction. This limits the capabilities for vendors to implement security measures such as out-of-band setup, key verification, multi-factor authentication, etc. Even with the use of companion smartphone applications, the authentication measures available for connected devices is often more limited than more traditional computational systems, and these limits force the deployment of less secure alternatives, or alternatives that are more likely to include deployment errors.
- ***Limited willingness to invest in secure development***. Rabid demand for connected devices has created market conditions that incentivize first-mover and early-mover advantage, which are often erroneously seen as at odds with cost and timeline investments required to properly secure devices. Short-cutting the secure development process almost always results in deployment of devices that have easily exploitable vulnerabilities. While reduced investment in security is also a general issue in all systems and not just connected devices, it is an issue that research has proven to be notoriously prevalent in the IoT sector.
- ***Physical access undermines most security models***. Almost all security models assume that physical access to a device guarantees that compromise is possible. Connected devices typically require direct physical access by the user to the device. In a consumer home environment, this is not a significant issue in the threat model, as consumers are unlikely to benefit from exploiting themselves. However, in a hospitality context there is a high volume and constant turnover of guests with physical access to the same devices, and there could be extreme benefit for an attacker to exploit all future guests. This inherently and severely impacts the threat model in a hospitality IoT context.

3.7 Security Challenges that Afflict IoT that Are Not Unique to IoT

In addition to the aforementioned security challenges that are unique to IoT, connected devices are also impacted by many security challenges that more broadly impact most or all systems. These challenges include:

- ***User preference for convenience over security***. Any security features that add even minor friction to the user experience are often abandoned or rejected, regardless of their value to the security posture. This issue is magnified in hospitality, which places significant emphasis on optimizing the guest experience wherever possible.
- ***Security is an evolving target***. What is considered secure at one moment is often proven to be vulnerable at a later moment. Adversaries constantly advance their techniques. There is a constant cycle of software, libraries, and operating systems being found exploitable and then patched. Taken together, all of these require constant evolution of the security posture through patching and system updates. This issue is magnified in IoT, where connected devices in many cases do not have the ability to install updates, or if the ability exists, it is very difficult for the average user to perform.
- ***Building is different from breaking***. Developers are focused on system performance, and often are not trained in secure system design. An overwhelming majority of computer science degree programs have either only very limited curricula on security, if there is any at all. Even those developers who do spend considerable energy on secure system design do not spend even a fraction of their hours focused on security as compared to the entirety of time that adversaries spend focused on figuring out how to break systems.

3.8 What To Do About These Security Challenges

The most effective security model around any given device or architecture will be dependent on use-case so prescriptive steps aren't the best approach for most organizations. The following methods will help a company approach security in the manner most appropriate to your deployment.

3.8.1 Think strategically

Effective security organizations understand that effectiveness requires strategy, which then informs the tactical execution. To best pursue this mindset, effective organizations should consider these 11 concepts that support the ability to think strategically about security:

1. Adopt a security mission
2. Be your security champion
3. Define risk
4. Allocate appropriate resources
5. Plan for the future
6. Adopt an adversarial perspective
7. Understand your Threat Model
8. Understand your Trust Model
9. Understand how modern adversaries operate
10. Perform security assessments best aligned with your goals
11. Understand the role of compliance

3.8.1.1 Adopt a security mission

Effective security starts with making it a priority. While this sounds simple in concept, it is often very difficult in practice. Historically, the most successful security organizations are defined by executive buy-in to a well-articulated, well-defined and well-communicated security mission. Effective security organizations define the purpose behind *why* security matters to them, *what* they do to pursue those objectives and *how* they pursue the mission.

Contrary to conventional wisdom, effective security is not achieved solely via a collection of products, or through satisfying the basics of some sort of compliance framework. Rather, security is a combination of

people, process and products, all strategically resourced and deployed in the context of a security mission.

Organizations should:

- Define why security matters to the unique needs and conditions of the organization
- Obtain executive buy-in about the security mission
- Develop and execute a communication plan to ensure all levels of the organization have a common understanding of the security mission

3.8.1.2 Be your security champion

Effective security is essentially an exercise in advocacy. Security is often hard to see, touch or feel, and it is most often felt as a void. A breach may result from a lack of effective security, so organizations should define at least one person – and in the best examples, many people – to serve as the champion for security in the organization. This individual or team advocates for the security mission, ensuring that it gets integrated into all aspects of decision making across the organization.

Organizations should:

- Empower a person or group to advocate for the security mission
- Grant the champion the necessary support, executive visibility and influence to drive meaningful impact
- Remove conflicting priorities to allow the champion to focus on security

3.8.1.3 Define risk

Risk is a combination of likelihood and impact, while likelihood is comprised of attacker motivation and chance of success. Risk should be defined, measured and mitigated, with an acceptance that it will never be eliminated. Once organizations can accurately understand their risk, they can then make business decisions about how to allocate resources to reduce it.

Organizations should define:

- Attacker motivation
- Chance of attack success
- Business impact in the event of a successful attack
- Mitigation strategy to acknowledge acceptable risk and reduce unacceptable risk
- Measurement of security processes and reevaluate the above continually over time

3.8.1.4 Allocate appropriate resources

Like marketing, accounting and legal, security is a core business discipline. Appropriate cost-benefit tradeoffs should be considered when allocating resources toward the pursuit of organizational effectiveness in this domain. Ineffective security organizations see security as a cost to be minimized and attempt to survive by doing just the bare minimum, while effective security organizations recognize that security requires the investment of manpower and financial resources to be effective. It should be noted, however, that there is a condition of diminishing returns, after which point additional investments in security won't deliver correspondingly higher returns on effectiveness. *Appropriate* resource allocation should be the goal.

Organizations should:

- Define what success looks like
- Quantify the manpower and financial investments required to deliver on that vision
- Make informed, data-backed decisions on where to invest in pursuit of the desired outcomes

3.8.1.5 Plan for the future

Technology evolves, market conditions change and attackers innovate. As such, effective organizations consider security in a future context, by thinking about how to adapt the security policies over time. IoT introduces particularly notable future-state conditions, as many IoT solutions are designed to be buyer, rather than vendor, supported. In either model (vendor-supported or buyer-supported), effective security organizations understand that bugs will be discovered, security vulnerabilities will be published, and attackers will evolve. Effective security organizations make it easy to ingest bug or vulnerability disclosures and have a plan and mechanism for updates.

Organizations should:

- Plan for how to remedy security issues that are currently unknown
- Implement an easy-to-use updated mechanism across all deployed systems
- Empower users and security researchers with a communication channel to disclose security flaws to the vendor for remediation

3.8.1.6 Adopt an adversarial perspective

To defend against an attacker, you must think like the attacker. Effective security organizations recognize this and attempt to apply it in a handful of ways.

3.8.1.7 Understand your Threat Model

No system can be impenetrable against every attacker and every attack. One should focus on the adversaries that an organization is most concerned with in the context of the assets the organization wishes to protect. The attack will surface when an adversary launches malicious campaigns and organizations can then design and deploy security programs that are effective against the most concerning type of threats. Threat Modeling is an exercise undertaken to define assets, adversaries and attack surfaces in the pursuit of optimizing the defense paradigm.

Organizations should:

- Define the assets to protect
- Define the adversaries to defend against
- Define the attack surfaces and determine which abuse, and misuse cases can be deployed
- Communicate the threat model across all internal and external stakeholders
- Update the threat model frequently

3.8.1.8 Understand your Trust Model

An inverse to the Threat Model, a Trust Model is an exercise through which an organization defines *who* it trusts, *why* it trusts that person, and *how* trust is provisioned and validated. All organizations must be able to trust certain internal and external parties in order to execute on the business and functional needs; the

Trust Model empowers the organization to do so while adequately understanding and mitigating the risk associated with allocating such trust.

Organizations should:

- Define who they trust
- Define why they trust that person
- Outline a process for provisioning trust, including how to ascertain authentication, authorization, and access control
- Outline a process for revoking trust

3.8.1.9 Understand how modern adversaries operate

Most organizations adopt security models defined by the premise of keeping attackers on the outside of rigid perimeter defenses. However, the concept of a defined perimeter is outdated, and modern adversaries typically do not attack perimeter defenses directly. Rather, attackers typically attempt to exploit trust and gain access through the supply chain with stepping stone attacks. This is a notoriously effective attack model in an IoT context, which typically tends to be overly permissive with trust. Effective security organizations understand this attack model and implement defense mechanisms accordingly.

Organizations should:

- Consider stepping stone attack methodologies
- Review integrations for potential harm in the event of successful exploitation of third party trust and/or access
- Perform an effective security assessment

3.8.1.10 Perform security assessments best aligned with your goals

Organizations should pursue security assessments to investigate for security flaws, which can then be remediated. This concept also implies that organizations must best understand *what* they want to accomplish with a security assessment and *why* that is important. For some organizations, a commodity level, low intensity, automated penetration test will be sufficient to satisfy their security needs. For others, more thorough approaches, such as manual white box security assessments, will be more appropriate. Effective security organizations understand this distinction and apply methodologies accordingly.

Organizations should:

- Define objectives for security assessment, in accordance with their defined Threat Model and Trust Model
- Understand which methodologies are best suited for different objectives, and their corresponding outcomes
- Vet partners for security pedigree, including contributions to security research, talks and technical capabilities
- Invest appropriate financial and manpower resources

3.8.1.11 Understand the role of compliance

Most organizations will be required to adhere to a compliance framework, either to address their own organizational needs or the needs of their customers. Depending on the framework, compliance typically does an adequate job of establishing the baseline requirements for the foundation of a security program.

However, compliance should not be expected to provide the entirety of the security program. Effective security organizations recognize the role of compliance in satisfying stakeholder needs but go beyond the outlined minimum where delivering a robust security program is important.

Organizations should:

- Identify which compliance frameworks are important to the organization and why
- Define what a successful outcome of the security model looks like
- Define the delta between compliance and the desired outcome and mobilize accordingly

3.9 Privacy

In addition to security, guest privacy needs to be considered. Many IoT systems work in real-time tracking if the guest is in the room or what the guest is watching on TV. Typically, there is no readily available means to separate this information from the person staying in the room. This information requires real-time protection. The other concern is that some hotels may want to track a guest's room settings to better accommodate the guest on return to the room or on future visits. When associated with the individual guest this information falls under the protection of rules like GDPR. It is important to notify the guest about the IoT information that is collected, how it will be used, and how the guest can, prevent its retention, and request to have the information removed.

Privacy has traditionally been defined as "freedom from intrusion," yet in a modern context the application of the term has come to mean "an individual choice about who has access to their data," which is a concept that regulators and activists are rallying for. To best protect both end users and the companies who accumulate their data, privacy should be considered from the outset to best integrate well-reasoned decisions about privacy into all subsequent business decisions.

Consider the following three strategies when thinking about privacy in an IoT hospitality context:

1. Consider privacy a leadership issue
2. Consider data collection
3. Consider data usage

3.9.1 CONSIDER PRIVACY A LEADERSHIP ISSUE

As with any domain across the business, what the executive leadership prioritizes is what flourishes. From the standpoint of the marketplace, the industry and regulators, a well-designed approach to privacy is an expectation. Well-defined privacy policies lead to strategic decision making to protect customers and avoid limits risk.

Organizations should:

- Obtain executive buy-in to develop a privacy plan
- Develop a plan to design and implement privacy
- Establish success measures
- Educate and train your employees on an ongoing basis

3.9.2 CONSIDER DATA COLLECTION

Organizations benefit from various types of data that can be collected from their customers and users, including discovering emerging trends, better serving the customer and uncovering new revenue streams. However, with such collection of data comes some risk of regulatory issues, and/or brand damaging issues. Organizations should think carefully about the kinds of data they want to collect, why they want to collect that data, and then weigh the value of collecting the data against the potential reputational and financial impacts of privacy violations that can occur.

Organizations should:

- Inform the individuals about the purpose for which data will be collected, used or disclosed, and obtain their consent in writing
- Provide choice; the recommended model is to require individuals to opt-in to be granted access to their data and offer them the ability to opt-out of data collection at a minimum
- Ensure any third party you partner with has obtained consent from the individuals to disclose their data to your organization
- Identify what kind of and how much personal information your organization handles

3.9.3 CONSIDER DATA USAGE

Once an organization possesses data, the organization must consider how it will use and safeguard that data. To understand how data will be used, organizations should have a well-defined approach to data usage that considers how best to obtain and use data while limiting the potential risks that such data usage introduce. To ensure an organization will safeguard their data, refer to Section 3.6: Security Best Practices.

Organizations should:

- Ensure that the purposes for which the organization obtained consent to collect personal data are the only ones for which that data is used
- Ensure that any changes in the disclosure and the use of the personal data collected receive a new and separate written consent
- Understand there are legal, regulatory and industry obligations and risks that pertain to the use of collected data.
- Ensure there is a formal procedure in place to handle requests for access to personal data, including, but not limited to, their purpose, evaluation of data security measures, storage locations, access rights (individuals and other companies) and disposal mechanisms

4 Case Studies

In order to highlight practical use cases for IoT, this section explores case studies that showcase how IoT has been implemented and had a positive impact on operations.

4.1 Smarter Workplaces (Tyréns)

Multi-disciplinary consultancy Tyréns wanted to gain a deeper understandng of the relationships between people and the buildings they work in – based on hard data, rather than intuition.

Tyréns will revolutionize building management and boosting efficiency by deploying Internet-connected sensors at its headquarters and linking them to its building information models and asset management systems.

4.1.1 Description:

Tyréns is one of Sweden's leading multi-disciplinary consultancies, specializing in solutions that promote sustainable development. The company operates from 30 offices across Sweden, and also has offices in Copenhagen, London and Tartu, employing more than 1,300 people.

Through its work as a leading multi-disciplinary consultancy, Tyréns strives to create better, safer and more sustainable communities. To help achieve this objective, the company wanted to gain a deeper understanding of how people experience and interact with the buildings they live and work in. Tyréns also wanted to find a simple way to share this insight with clients such as architects, building managers and owners.

Tyréns' Building Information Modeling and IoT Strategist, Per Bjälnes, elaborates: "As a test case, we decided to use building information modeling (BIM) techniques to map out a building, and then integrate live data from strategically placed sensors, connected via the Internet of Things. This would allow us to create on-screen visualizations of how each meeting room, each restroom – even each desk – were being used. We realized that this would be an incredibly powerful source of insight."

Tyréns chose its Stockholm headquarters as its first smarter building project. Working closely with IBM, Tyréns used Autodesk Revit to create a building information model, containing a detailed 3D representation not only of every room in the building, but also its furniture, lighting and heating systems. The company then loaded this asset hierarchy into the company's IBM® Maximo® Asset Management System in just four minutes – a task that would typically take several months if all the assets had to be registered manually.

Next, Tyréns worked with IBM Business Partners Intel, Yanzi and SVSi to install 1,000 Internet-connected sensors throughout the building in just four hours and registered their locations in the BIM and Maximo systems. IBM MessageSight allows these sensors to send real-time information about everything from temperature and humidity to light, power usage and movement.

4.1.2 Conclusion

By plotting the sensor data in the BIM, Tyréns can easily visualize exactly what is going on in every part of its building, in real time, 24 hours a day.

Bjälnes adds, "Equipped with this information, we can directly analyze why – for example – it is too hot in a certain room. Depending on the reason – too many people, too much sunlight, the blinds weren't down, inefficient air-conditioning and so on – the building manager can make data-driven decisions to keep temperatures stable. This saves energy and money and will help us to create a better working environment."

Bjälnes continues, “The BIM user interface is very easy to use and requires no technical expertise. This means that every member of staff, from cleaners and receptionists to accountants, can easily access and understand the model, and make data-driven decisions. To take an example, we have installed movement sensors under the tables at each chair in our meeting rooms, which allow us to see how many people are sitting in each room throughout the day. This allows us to assess if the room is being utilized properly, and whether or not it is the most efficient use of space.”

Bjälnes concludes, “Equipped with Internet of Things technology from IBM, Intel, Yanzi and SVSi, we have the potential to revolutionize the way our clients manage buildings, while the insights we gain from the BIM solution will help us to build better, cheaper, safer environments for people to live and work in.”

4.2 Panic Button (TraknProtect)

Panic buttons in different forms have been around for decades. Banks and retailers have long employed hard-wired panic buttons and silent alarms to alert authorities of robberies or other dangerous situations. Home security systems and medical alert systems, such as those designed to protect seniors in home health emergencies, have provided portable panic buttons to consumers and businesses. These systems had often previously relied on phone lines and dispatchers to respond to alerts.

The new generation of panic buttons are quickly becoming the safety standard in an expanding number of work settings such as hotels. In these environments, a panic button is intended to mitigate damage and deescalate a distress situation. These buttons act as a wireless alarm that sends a notification alert to other staff or authorities with the location of the distress call so others can respond quickly. Panic buttons not only empower employees to feel secure but can prevent potentially dangerous situations that can cause harm to both employees and others and in turn, damage a company’s reputation.

4.2.1 Description

Hotel workers face an especially high level of sexual harassment and abuse, mainly from guests. 58% of hotel workers and 77% of casino workers surveyed have been sexually harassed by a guest[1]. In 2011, French politician Dominique Strauss-Kahn made international headlines for allegedly sexually assaulting a housekeeper at a hotel in NYC (a charge that was later dismissed). Public outcry and media attention publicized the potential dangers faced by hospitality workers, and increased pressure on lawmakers and hotels to take action.

In 2012, hotels in New York City were among the first to respond to this issue and distribute personal panic buttons to housekeeping staff. In 2016, Seattle followed suit and approved Initiative Measure 124 introduced by UNITE HERE Local 8 union. A few Washington D.C. hotels introduced panic buttons after the 2011 media attention, and over 30 more hotels joined them in 2017 as part of a deal with their local union, UNITE HERE Local 25. Then, in October of the same year, Chicago hospitality workers made an appeal to a City Council committee for mandatory safety initiatives and the committee unanimously passed the Hotel Workers Sexual Harassment Ordinance, which requires hotels to equip employees with panic buttons by July 1, 2018.

As the national conversation about sexual assault and harassment grows louder with the #metoo movement, more cities are expected to take action and consider similar safety measures. However, there are some issues with dated technologies deployed to provide panic buttons to hotels. For example, most panic buttons’ requirements stipulate that workers need to be able to summon immediate help when they make a distress call, however, many systems fall short. Sound-only panic buttons or alarms are not considered to be in compliance according to some industry experts. These types of buttons are limited to who can hear them, may be a deterrent that can make the perpetrator more aggressive, rely on nearby

guests and employees to be first responders and lastly, in case of a false alarm, these buttons "publicize" the emergency to other guests instead of allowing a hotel to manage the situation differently. While many panic button systems provide an *approximate* location of an employee during a distress call, either based on stand-alone GPS or with the help of another software system, these systems do not provide the real-time location of an employee if the employee moves or is moved; and such panic buttons have been found to have inherent security risks as a result of their "pairing" to a hand-held device, making them ineffective in case of an emergency.

The TraknProtect panic button is a portable device that uses Bluetooth and Wi-Fi to send location alerts when a distress call is made through its IoT platform. The button is about the size of ordinary key fob, can be worn on keys or as a pendant, and has a discrete design. A 2-second push of the button activates a distress call and sends a location alert almost instantly to any device (i.e. via iOS, Android, desktop or voice-call messaging). The desktop notification will make a loud sound to capture the security or front-desk employee's attention to ensure assistance can be deployed immediately.

The TraknProtect platform provides the exact, real-time location of the employee upon alert, even if they move. TraknProtect is able to do this through its IoT Gateway infrastructure that can retrofit in existing hotel rooms and areas. Once the panic button is triggered by an employee, the button communicates through BLE to the nearest Gateway and over Wi-Fi, pushes the location to appropriate parties immediately. This allows hotel security or management to provide prompt assistance to the location of the distress call. Distress calls can also trigger a 24/7 monitoring service which can dispatch the police and ambulance, if necessary.

The TraknProtect platform is serviced by an app and a web portal. After a distress call is made, staff can take notes on the incident through the app or web portal. These platforms produce analytics through the IoT hardware such as safety call reports and the number of incidents that can help hotels understand safety statistics. It will also track false alarms and safety calls to provide reports on the work environment in order to optimize security.

Once installed, the TraknProtect platform can be leveraged beyond panic buttons. The IoT Gateway infrastructure can be leveraged for hotel operations such as inventory tracking, vendor tracking and room service tray tracking.

4.2.2 Integrations – Going Beyond

A panic button solution can be part of an IoT strategy by having it be part of an integrated solution allows with seamless coverage without additional hardware.

Leveraging simplified integration strategies available through IoT architectures, TraknProtect integrates with Interel, which provides control-panels to manage thermostats, lights and temperatures in a hotel room for energy savings. TraknProtect also uses Access Points with BLE modules such as Ruckus H510's, other network hardware manufacturers such as Cisco and integrators such as BluIP. Hotels that have Interel panels in their guest rooms or Ruckus Access Points, do not require TraknProtect gateways, saving the hotel significant cost of setting up TraknProtect gateways.

TraknProtect also integrates with VM Presence, a digital camera and facial recognition system used at events such as the Grammy's, so that when the panic button is pressed, it enhances the camera feed of that location for the security staff to quickly assess the situation prior to responding. Also, the digital feed from nearby cameras is automatically recorded and saved under the same incident file as the panic button call to allow for a complete record of the call, the response time to the call and actions taken.

4.2.3 Conclusion

Panic buttons have been on the rise in the hospitality industry and hotels need a system that is cost effective and forward looking. Leveraging an IoT-enabled system, such as this use case, gives hotels the ability to meet requirements set forth by industry standards and maximize their investment. As the hotel landscape continues to evolve, hoteliers need to ensure that their investments fulfill requirements and yet are versatile to withstand the rapidly changing technology landscape.

4.3 The taming of the "things": Bringing IT controls for door lock connectivity (Ruckus Networks)

Several major concerns for IoT radios and sensors is management, monitoring, security and being part of an information technology group's standard operations. The potential proliferation of devices could be an IT nightmare with questions such as: Where did we place the Zigbee Hub? What is its password? IP Address? The question is why not have these devices connect to the network like any managed device? For example; Wi-Fi has moved to central management with flexible deployment solutions that cane be on property and in the cloud; these management platforms provide an abundance of information about the Wi-Fi environment and clients, plus now they are managing switches, LTE radios and more. Examples of additional radios in a Wi-Fi system are available from Ruckus Networks, Aruba and Cisco, this is clearly an important trend. The rest of this use case will involve a Ruckus Networks and Assa Abloy specific solution.

4.3.1 Description

Ruckus Networks is part of the "in-room AP/switch" product change in hospitality. The wall plate AP, such as H510, is the perfect platform for addition radio services. Adding a small radio module to the two-way communication USB port on the H510 allows for the unit to get power and backhaul communications. The port is disabled by default and is controlled by the SZ Controller Platform where enabling the USB port power, IoT service and secure on-boarding of radios is centrally managed. No additional switch ports or lost radio Hubs are required. Once the equipment is installed, the learning of the Assa Abloy locks is a relatively simple task. The Ruckus IoT Radio is put into pairing mode with adjustable time to allow IT to get to the floor and initiate the Assa Abloy Lock learning/pairing function (this is often done with a special key card or another method). Once complete, the IT personnel review the SZ Controller for a list of Assa Abloy devices and *accepts* each one or in bulk. There is no communication of a device found in the pairing allowed until the device is accepted by IT. The low cost of IoT onboarding, management and monitoring is critical to allow new services such as Assa Abloy Smart Locks.

4.3.2 Conclusion

Ruckus Networks created a modular solution for adding new service radios to Wi-Fi Access Points. This allows the addition of OpenG/LTE, Zigbee, BLE and other protocol radios while allowing them to share the network backhaul of the AP and the management/monitoring and security of the mature SmartZone Controller Platform. Working with Assa Abloy's Smart Door Lock systems, Ruckus is able to provide Zigbee connectivity between the lock and Assa Abloy's Visionline software.

5 Summary

There is little doubt that the introduction of connected objects has had significant impact on virtually all aspects of the hospitality business. This impact is multi-dimensional, covering guest experience, operational aspects across all departments and environmental sustainability.

It is critical to ensure that perceived complexity and challenges of any disruptive technology during the early adopter phase will not stand in the way of realizing its full potential, and stakeholders have to bridge the gap between available technology, vendor products, theoretical models, and practical requirements while maximizing overall ROI.

This white paper was developed with the intention to provide relevant parties a baseline of the dynamics of IoT implementation. The purpose of this white paper is to help hoteliers make more informed decisions when being confronted with the realities of an IoT project and identify which aspects should not be left unaddressed during its implementation.

6 Appendix

6.1 Glossary of Terms

For the purpose of this document the following terms have been defined as follows:

Term	Definition
Bluetooth Mesh Connection	Bluetooth mesh networking, conceived in 2015 and adopted on July 13, 2017, is a protocol based upon Bluetooth Low Energy that allows for many-to-many communication over Bluetooth radio.
Big Data	Extremely large data sets that may be analyzed computationally to reveal patterns, trends and associations, especially relating to human behavior and interactions.
Fog Domain	Domain including gateway devices which are located at the edge of the local and cloud networks.
IaaS	Cloud infrastructure services are self-service models for accessing, monitoring and managing remote datacenter infrastructures, such as compute (virtualized or bare metal), storage, networking and networking services (e.g. firewalls). Instead of having to purchase hardware outright, users can purchase IaaS based on consumption, similar to electricity or other utility billings.
Mesh Architecture	Non-hierarchical and decentralized network across various objects in order to deliver data to and from a specific end node.
PaaS	Cloud platform services are used for applications and other development, while providing cloud components to software. What developers gain with PaaS is a framework they can build upon to develop or customize applications. PaaS makes the development, testing and deployment of applications quick, simple and cost-effective. With this technology, enterprise operations, or a third-party provider, can manage OSes, virtualization, servers, storage, networking and the PaaS software itself. Developers, however, manage the applications.
Point-to-Point Architecture	Direct point-to-point communication between objects that need to exchange data.
SaaS	Cloud application services represent the largest cloud market and are still growing quickly. SaaS uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a web browser without any downloads or installations required, although some require plugins.
Software Development Kit (SDK)	A software development kit (SDK or devkit) is typically a set of software development tools that allows the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system or similar development platform.

Star Architecture	End nodes are all connected to a central gateway that has the intelligence and processing power to take actions and process data.
Stepping Stone attack	Stepping stones are compromised hosts in a network which can be used by hackers and other malicious attackers to hide the origin of connections.
Threat Model	Threat Modeling is an exercise undertaken to define assets, adversaries and attack surfaces in the pursuit of optimizing the defense paradigm.
Trust Model	An inverse to the Threat Model, a Trust Model is an exercise through which an organization defines who it trusts, why it trusts that person and how trust is provisioned and validated.
White Box Security Assessment	White-box testing (also known as clear box testing, glass box testing, transparent box testing and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing).