Threat Model:
Emerging Locking Systems

Door Lock Security Working Group
Hotel Technology Next Generation (HTNG)

Revision Date: August 31, 2015

Prepared by: Independent Security Evaluators (ISE)
www.securityevaluators.com

Contact: Ted Harrington Ted.Harrington@securityevaluators.com
Executive Partner and Co-Owner, *Independent Security Evaluators*.
Co-Chair, *HTNG Door Lock Security Working Group*.

Authors: Paul Dant
Ted Harrington
Jacob Thompson
Ian Thomas

Table of Contents

Purpose & Introduction

A threat model is a tool commonly used to drive security analysis and testing of a system. Beginning with a system's logical or structural architecture, the threat model is a depiction of the assets within or protected by the system, potential threats targeting those assets, and attack surfaces likely used by adversaries in compromising one or more assets. Without this model, quantifying overall risk to better understand necessary controls and mitigation factors is unlikely to produce meaningful results.

This document presents a framework to achieve the following:

- **Consolidate common objectives**. Hotel brands, owners and vendors share a number of common objectives and concerns. Collaborative analysis of system security ensures a unified understanding and nomenclature.
- **Evaluate business security goals**. To help consolidate common objectives, a clear set of business security goals can be identified and assessed using this model.
- **Identify emerging threats**. New technologies introduce new risk by presenting new opportunities for adversaries and new challenges for hotel brands, hotel owners, and vendors.

HTNG Door Lock Security Working Group

The HTNG Door Lock Security Working Group was formed in 2014 to empower hotel brands, hotel owners, and vendors to better identify and mitigate security risk introduced by new locking system technologies, such as:

- Highly-integrated online lock systems.
- Mobile device-based solutions utilizing near-field communication (NFC) and Bluetooth technologies.
- RFID locking systems.

Such emerging locking systems introduce new communication protocols and communication layers; many are Internet-connected (either directly for functional and support purposes, or indirectly), and may integrate with cloud-based systems. In some cases, guest-provided devices, like mobile phones, can introduce entirely new attack surfaces or cede a portion of the trust model to an adversary. As with many of the currently deployed locking systems, emerging locking systems commonly integrate with other systems such as property management systems (PMS) and point of sale (POS).

The goals of the working group in assembling this document are to:

- **Protect guest safety and privacy.** All stakeholders share the common goal of protecting guest safety. If a guest is not safe and secure, then a hotel brand, a hotel owner, or a vendor could experience significant financial and reputation harm.
- **Empower hotel owners to make informed decisions**. Computer security and electronic lock knowledge are specialized. An open document that brings together experienced brands and hoteliers with premier vendors and organizations possessing specialized knowledge will allow the hotel owners to objectively compare the security capabilities of different lock systems in order to make informed decisions.
- **Collaborate with all stakeholders**. Hotel brands and owners must collaborate with vendors to ensure a lock system meets business objectives and reduces the risk of financial or reputational harm.
- **Help vendors to produce locks that better protect the assets that are important to hoteliers.** With effective feedback, vendors can produce more hardened systems and provide effective risk mitigation strategies to the hotel brand, the hotel owners, and the vendors.
- **Empower involved parties to reduce risk**. Reducing risk of financial and reputation harm is a primary business goal practiced by all the interested parties. It makes good business sense to reduce risk that potentially affects profits and losses.

Hotel Industry Context

With some exceptions, the hospitality industry is primarily a franchise model: individual hotel properties are typically owned by an independent proprietor, who meets certain requirements set by the brand in order to license the brand name. Brands can make suggestions and even requirements of the hotel owner but, ultimately, the hotel owner makes the purchasing decision when it comes to procurement of locking systems.

Owners are usually small operations with very limited or nonexistent security budgets and minimal or no technical security expertise on staff. In this business context, it is not a reasonable expectation that owners will be able to perform effective security assessments on the locking systems they procure, or understand the security and privacy implications introduced by the systems selected. In some cases, operations and management of a property (or set of properties) is outsourced to a third party property management organization. As with property owners, the overall understanding of security and privacy will vary as will the security budget.

This document and the associated working group aim to resolve this business procurement challenge as it relates to ensuring the protection of the assets enumerated herein.

Purpose of Lock Systems

Lock systems play a key role in managing property access control. New functionality in next generation locking systems introduces potential risks that could impact the security of assets. From that perspective, this threat model seeks to assess threats against the following basic security requirements:

- **Authorized individuals have access to a property location.** Only individuals authorized to access a specific area of the property should be able to enter that area. Authorized individuals include the guest and his or her party; staff, such as housekeeping and maintenance; and others such as medical rescue.
- **Unauthorized individuals do not have access to an unauthorized property location.** In addition to providing authorized access, the system must ensure unauthorized individuals, who should not have access, are denied entry into the unauthorized area.
- **All transactions are logged accurately.** All transactions and system events (both successful and failed) must be accurately logged and adequately protected.

Baseline Security Context

In order to establish a meaningful baseline for the evaluation of emerging technology security capabilities, understanding of existing security risks associated with existing lock system technologies are presupposed and assumed out of scope:

- Existing mechanical lock mechanisms (e.g., pin tumbler) may still be vulnerable to traditional attack mechanisms:
    - Lock-picking (e.g. pick guns, bump keys), brute-force entry, or bypass via a secondary entry point (like a window) defeat the physical lock device.
    - Traditional mechanical keys can be trivial to duplicate even without a physical copy; bump keys for specific lock models can be made using 3-D printed models available on the Internet.
    - Given adequate, undetected physical access, specialized tools such as a mule tool may be used to physically trigger a lock's interior handle in a manner that mirrors an authorized party exiting the area (as opposed to an unauthorized party entering the area). This scenario may further impact security with the logging of inaccurate (or no) event data.
- Human elements of a system are always vulnerable to social engineering attacks:
    - Front of house staff may be fooled into granting access to an unauthorized area of the property. Typical mitigations include security awareness training and rigid requirements for the reissue of a guest key.

The scope of the HTNG Door Lock Security Working Group, as well as this threat model deliverable, is focused on the new attack surfaces introduced by new functionality. This threat model is built upon the underlying assumption that the threat model and risk analysis pertaining to the mechanical aspects and other relevant characteristics of traditional locking systems are understood and analyzed elsewhere. For instance, this threat model considers how a

locking system can be attacked through a web application, but does not focus on the mechanical specifications of the deadbolt. Overall, this threat model will have served its purpose effectively if a newer locking system can be validated to be at least no less secure than a traditional locking system.

As lock system technology continues to evolve, this baseline understanding will set the proper expectations around mitigating controls regardless of the introduction of additional features that are certain to come in future product iterations.

System Architecture

In order to accurately model and identify risk, a logical or structural architecture is necessary to enumerate the inputs to the model.

The components typically present in a deployed hotel lock system architecture are presented below; while the lock system itself is a single component of the overall system, operational integration with other systems are considered for the purpose of this threat model. Note that specific implementation and design decisions, along with vendor technology choices, may influence the way components interact, and thus introduce new areas of risk.

Note: This diagram (and corresponding explanation) is indicative of the highly connected ecosystem in which lock systems are typically deployed and integrated. However, the diagram is not representative of all possible design and implementation choices. Every organization must adapt this generalized framework to their customized deployments.

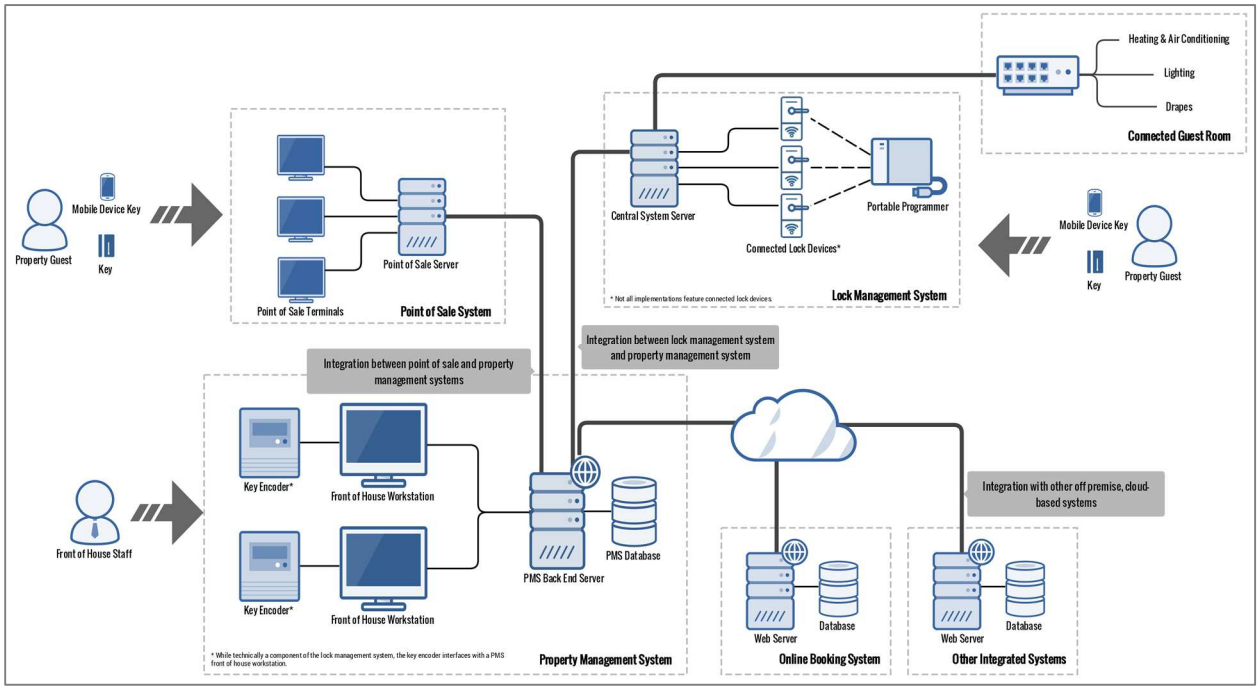


Figure 1 - Logical System Architecture

Lock Management System

The lock management system represents the set of components involved in communication between property locks, keys, and control systems. Integration with a property management system (either on premise or cloud-based) is common.

Central System Server

In a connected lock system, the central system server is a backend component serves as an aggregation point for key and lock data. It maintains connectivity with lock devices via TCP/IP network (wired or wireless).

This component commonly interfaces with property management systems for front of house access control management. The central system server component may also provide backend connectivity to a vendor cloud service for vendor support. The nature and extent of integration is varied; as a result, identifying specific exposures requires deeper analysis of a concrete vendor implementation.

Key Encoder

The key encoder device is capable of manipulating key device data; it is typically attached to a front of house workstation or terminal (TCP/IP, USB, and RS-232 are common interfaces) and intended for use by authorized property staff.

Given the capabilities of this component, proper access control to the device as well as the connected workstation is imperative.

Key

The key is a device or credential provided to staff and guests for access to authorized property locations like guest rooms, guest room safes, and restricted areas. Depending upon the specific lock system implementation, the key may take the form of a RFID or NFC device issued to the guest by the hotel. Next generation technology introduces the ability to use a guest-owned mobile device as a key, requiring additional communication mechanisms like Bluetooth.

In modern implementations, keys issued to staff and guests may provide additional functionality like access (and transaction processing) for guest parking, vending machines, and other POS use cases.

Information encoded to a key typically includes the authorized room number(s), a departure or expiration date, and a randomly generated account ID value. Older or misconfigured lock system implementations may store additional sensitive information. The security of the key data (i.e. cryptographic system) is implementation specific.

Master Keys

Any key that grants access to more than one door or location is considered a master key. The role of a specific master key is an important consideration; attackers seeking elevated access throughout a hotel property will likely apply this knowledge in an effort to launch targeted attacks.

The following diagram represents a master key access hierarchy; the aggregate level of property access granted by the master key decreases from top to bottom.

Figure 2 - Master Key Access Hierarchy

Lock Device

The lock device electronically control access to areas within a given property based upon data provided by a key. Common lock device implementations feature RFID for transmission of data; next generation devices equipped with Bluetooth and NFC communication mechanisms expand compatibility for "keyless" systems featuring a guest's previously enrolled mobile device as the entry mechanism presented to the lock.

In a connected system, each lock device ultimately interfaces with a central server component. In a non-connected system, each lock device individually authorizes based upon information presented on the key and a set of rotating access codes; activity logs are stored locally and accessible with a portable programmer.

Portable Programmer

A portable programmer is a device capable of interfacing with a lock device (physically or wirelessly) to interrogate the lock for configuration, status, and audit log data. The portable programmer may also trigger the lock to open, providing access to a controlled area, and power the lock device externally in the event of batter failure.

While specific capabilities may vary by vendor and implementation, the portable programmer is typically equipped with configurable, on-board access control. Proper configuration of the device for effective authentication is essential as well as physical access control.

Guest Room Environment

In some implementations, the lock system integrates with guest room environment controls for drapes, lights, and temperature.

Property Management System

The property management system (PMS) provides extensive functionality to support the overall operation of a hotel property. As a result, it is commonly deployed with multiple integration points; related systems (both on and off the property) communicate centrally with the PMS. Given this deployment architecture, exposures within the PMS have the potential to compromise the lock system components and, conversely, exposure within the locking system may lead to compromise of the PMS.

PMS Backend Server & Database

Property management systems typically feature a backend component that drives application functionality, data access, and storage. Integration with other property systems typically stems from this component of the PMS.

Many PMS vendors offer cloud or software-as-a-service models that obviate the need for an on premise server; these offerings may introduce additional exposures. In particular, the PMS deployment model influences the type of application and connectivity required at front of house workstations.

PMS Front of House Workstation

The front of house workstation or terminal is used by authorized hotel staff for operation and management of the property to include access control management where an issuing and encoding device is in place. Front of house workstations may communicate with an on premise PMS server or a remote, cloud-based PMS product.

Mobile Device Key

While traditional lock systems utilize key devices encoded and issued to staff and guests, next generation systems present a model in which guest-owned mobile devices, enrolled with a mobile application provided by the hotel brand, can be used to access authorized areas throughout the property.

Because the device is owned and controlled by the guest, the mobile device key component is considered separate to (and integrated with) the lock system.

Other Integrated Systems

Abstractly, other PMS-integrated systems will likely adhere to a basic, common architecture of backend and frontend components. The specific implementation details of such integration may expose the PMS to additional risk and, in turn, potentially the lock system.

Examples of commonly integrated systems include property CCTV, fire & safety, and time & attendance.

Related Backend System Server & Database

The backend server component of a system typically drives application functionality, data access, and data storage. In the cases of PMS integration, the backend component typically exposes an application programming interface (API) to facilitate communication between the systems.

Related Front of House Workstation

The front of house component drives the interaction between authenticated users and the related system.

Users

Identifying the roles under which authorized users interact with a system can reveal the potential impact of attacks targeting or involving those users. In cases like social engineering or eavesdropping, attackers target a user's knowledge of or access to a system; that distinction is important when considering a user as a potential attack surface versus an asset being protected by the system.

The following roles exist within the system:

Property Management

The entity with overall responsibility for management of the property may be independent of the property owner and hotel brand. Ultimately, third party property management organizations assume responsibility for the management and operations of a property (or set of properties) and may be subject to specific owner or brand security expectations.

Front of House Staff

Front of house staff interface directly with hotel guests in a customer service capacity to include checking guests in and out of the property. In many cases, this involves front of house staff issuing and revoking access keys using the PMS. Additionally, front of house staff members may be authorized to move throughout the property, including restricted areas and guest rooms.

Maintenance and Housekeeping Staff

Maintenance and housekeeping staff typically require unrestricted access to most areas of a property. In the case of maintenance, restricted areas with serviceable components like generators, HVAC, etc. must be readily accessible. Housekeeping, on the other hand, will typically have unrestricted access to guest rooms as well as supplies and guest information.

Property Guest

In traditional models, property guests interact with front of house staff to authenticate and subsequently gain authorization to the guest's assigned room. Once in possession of a key, property guests use the key to interact with lock devices throughout the hotel property to reach authorized areas.

In next generation "keyless" systems, property guests may bypass interaction with front of house staff completely by using an enrolled mobile device, owned by the guest, to access authorized areas of the property.

Assets

Before establishing an understanding of business security risk, it is necessary to identify assets and define their value. Assets include tangible elements such as information or equipment and extend to more abstract elements like reputation. The impact of the loss of these assets should be quantified to the best degree possible; this exercise is typically iterative and largely subjective.

The following assets have been deemed by hoteliers and other working group members to be relevant to this threat model:

Guest Personal Safety

The personal safety of a guest takes priority over all others. Loss of personal safety for a guest can result in significant financial and reputational harm to an hotelier or vendor.

Guest Personal Property

A guest who experiences a loss of personal property has the potential to cause financial and reputational harm to hotel brands, hotel owners, and vendors.

Employee Personal Safety

Employees expect a level of personal safety while at work; failure to reasonably protect an employee from personal harm will significantly impact brand reputation and result in financial loss.

Guest Information and Privacy

A guest experiencing a loss in personally identifying information (PII) or general privacy will likely cause reputational damage.

Guest Experience

Guests visiting a property tend to expect convenience balanced with privacy and security; perceivably tedious security systems and protocols may erode the guest experience and lead to reputational damage.

Hotel Facilities and Equipment

Unauthorized access to hotel facilities and equipment may result in significant cost due to damages or theft; facilities with integrated industry control systems (ICS) susceptible to attack may also risk harm to or loss of life.

Brand Reputation

Building and preserving brand reputation is expensive and hard-earned over a long period of time. Compromise of a locking system could instantly harm the brand reputation that took such investment to build. This type of damage is often difficult to quantify but has both direct and indirect impact on the financial performance of a brand.

Proprietary Corporate Information & Business Intelligence

Intellectual property, including custom software, business analysis algorithms, and any derived business intelligence are highly valuable assets and may provide competitive advantage if compromised.

Guest Trust

A compromise of the locking system would likely erode guest trust not just in that particular brand but in the overall hospitality industry, as it pertains to the industry's ability to protect guest assets. This in turn could adversely affect revenues at all hotels if guest stays decline as a result of eroded trust.

Lock System Availability

In order to properly manage access control throughout a property, the lock system must be available at all times. In the event of an attack against the system's availability (i.e. a denial of service attack) or another event impacting availability (e.g., extended loss of primary power, catastrophic loss of system components), the failure state of the locks throughout the property may prevent authorized guest access or inhibit egress in the event of an emergency.

Log File Data Confidentiality

The confidentiality of audit and debug logs needs to be protected as debug logs often contain sensitive information about application users as well as the application's implementation.

Log File Data Integrity

The integrity of audit logs needs to be protected to ensure an audit trail exists of all actions performed by users of the overarching system. The scope of this requirement is not necessarily constrained to the lock system alone.

Supply Chain Integrity

Many devices are built leveraging a range of hardware and software components from a variety of providers, and utilize established communication protocols. Many of these aspects are designed and produced beyond the scope of an individual lock manufacturer. Vulnerabilities introduced through this supply chain are thus adopted by the manufacturer in the build process. Understanding and ensuring the security integrity of this supply chain is a critical asset to safeguard.

.

Threats

Any robust defensive model requires a thorough understanding not only of the assets to be protected, but also of the adversary trying to steal those assets. Too often security practitioners design and review systems as if in a frictionless vacuum; this simplification can lead to solutions that have little relevance to real-world operations. An adversary-focused threat model allows companies to manage risk by directing resources against those threats and vulnerabilities that will have the greatest impact.

To properly introduce threats into the model, a number of threat attributes are defined to provide a qualitative risk profile:

Motivation	The specific reason(s) why an adversary would allocate resources towards an attack.	
Skill	EXTENSIVE	The threat is capable of complex, high-tech, sophisticated attacks or has access to resources with those capabilities.
	MODERATE	The threat may be capable of planning and executing attacks with limited complexity.
	LIMITED	Attacks are likely sloppy, not planned well, and do not require knowledge or skill to carry them out.
Financial Resources	EXTENSIVE	Threats within this category are able to invest large amounts of money into attack planning and execution.
	MODERATE	Funding may be available to obtain equipment and resources for attacks but prolonged operations and complex attacks are likely out of reach.
	LIMITED	Attacks are limited to those involving little to no financial investment.
Time Availability	EXTENSIVE	Planning and execution of attacks are unaffected by time constraints.
	MODERATE	Attackers have a significant amount of time available but not unlimited.
	LIMITED	Limited time for attack planning and execution are a concern for attackers.
Equipment Resources	EXTENSIVE	Equipment with high computational power is readily available.
	MODERATE	Resources necessary to carry out an attack may be available but with limitation or delay.
	LIMITED	Attackers have access only to basic computational power.

Table 1 Threat Attributes

The following threats, described using the attributes outlined in Table 1, are relevant to this threat model:

Nation State Intelligence (Advanced Persistent Threat)

MOTIVATION	**Espionage, Terrorism, Profit, Political**
SKILL	EXTENSIVE
FINANCIAL RESOURCES	EXTENSIVE
TIME AVAILABILITY	EXTENSIVE
EQUIPMENT RESOURCES	EXTENSIVE

Nation states represent the most capable threat actors. Beyond having the largest budgets and access to resources, nation states have unique capabilities in terms of access to supply chains and human access agents.

Organized Crime

MOTIVATION	**Profit**
SKILL	EXTENSIVE
FINANCIAL RESOURCES	EXTENSIVE
TIME AVAILABILITY	EXTENSIVE
EQUIPMENT RESOURCES	EXTENSIVE

This adversary is analogous to the group the "Russian Business Network" (RBN). They are typically a for-profit organized crime syndicate focusing primarily on cyber-crime activities that generate or launder money. These groups can have extensive membership, and due to available monetary resources can afford to hire skilled counterparts, fund exploit research or purchase exploits, and fund attacks in general. As cyber-crime is a business, targets of high-value will be chosen, costs to compromise assets calculated, and a bottom line decision made as to the worthiness of attempting an attack.

Corporate Sponsored Espionage

MOTIVATION	**Profit, Intellectual Property**
SKILL	EXTENSIVE
FINANCIAL RESOURCES	EXTENSIVE
TIME AVAILABILITY	MODERATE
EQUIPMENT RESOURCES	EXTENSIVE

Corporations will, at times, utilize espionage techniques to gain advantage over competitors or save on research and development. Corporations have significant budgets and are able to hire professional teams to conduct computer network exploitation of their competitors' networks. Social engineering is commonly employed by this adversary.

Hacktivists

MOTIVATION	Socio-Political Activities, Notoriety, Pride
SKILL	EXTENSIVE
FINANCIAL RESOURCES	MODERATE
TIME AVAILABILITY	EXTENSIVE
EQUIPMENT RESOURCES	EXTENSIVE

This adversary is a hacker organization analogous to the group "Anonymous." They are motivated by socio-political activities, pride, fun, and notoriety. These groups can have extensive membership, but it is likely that only dozens make up the core of this organization that pose a threat. They choose high profile targets over high value targets, and typically disclose stolen information rather than use it for identity theft or profit. The goal is notoriety, amusement, and the platform upon which to make a political statement, generally at the expense of the victim. Common activities include web-site defacement, “dox’ing” or releasing embarrassing internal communications, and denial of service or other acts of cyber-vandalism.

Individual Hacker

MOTIVATION	Notoriety, Profit, Challenge
SKILL	MODERATE
FINANCIAL RESOURCES	LIMITED
TIME AVAILABILITY	MODERATE
EQUIPMENT RESOURCES	MODERATE

The classic individual hacker is an explorer. They are generally motivated by the challenge of gaining access to restricted systems but may also work for financial gain. If they are financially motivated they will generally target banking and personal information. Their capabilities vary widely from a so-called script kiddy that is only able to apply existing tools, all the way to a highly professional individual who is capable of custom exploit development. Generally these threat actors have limited budgets and time; however, if properly motivated by a perceived slight or challenge, they may be persistent.

Determined Insider (Malicious)

MOTIVATION	Espionage, Terrorism, Profit, Political
SKILL	MODERATE
FINANCIAL RESOURCES	LIMITED
TIME AVAILABILITY	MODERATE
EQUIPMENT RESOURCES	MODERATE

The determined insider is the most dangerous category of internal adversary, because the determined insider is motivated to harm the company. The malicious insider acts as an agent for an external threat, providing otherwise unavailable access and privilege. As with the disgruntled determined insider, the malicious determined insider threat tends to persist where other inside threats are neutralized.

Determined Insider (Disgruntled)

MOTIVATION	Revenge
SKILL	MODERATE
FINANCIAL RESOURCES	LIMITED
TIME AVAILABILITY	MODERATE
EQUIPMENT RESOURCES	MODERATE

The determined insider is the most dangerous category of internal adversary, because the determined insider is motivated to harm the company. The disgruntled insider has become dissatisfied with the company for reasons such as being passed over for a promotion or by becoming disillusioned with the corporate mission. What makes the determined insider especially dangerous is that, because he is motivated by malice, technology and psychology solutions that may work against other internal threats are ineffective. For instance, the disgruntled insider knows what he is doing will harm the company but proceeds anyway, and so training and even awareness will not necessarily stop this threat.

Opportunistic Insider

MOTIVATION	Profit, Notoriety, Lack Of Deterrent
SKILL	LIMITED
FINANCIAL RESOURCES	LIMITED
TIME AVAILABILITY	EXTENSIVE
EQUIPMENT RESOURCES	MODERATE

The primary defining characteristic of the opportunistic insider is that he or she will compromise an asset when there is no repercussion for doing so. The opportunistic insider may not initially set out to harm the company; rather, over the course of performing his job duties he might be granted access to a valuable asset from which he may benefit by compromising, perhaps achieving financial gain by selling it or obtaining notoriety for being the first person to leak it. Without a disincentive in place, this employee may choose to pursue these gains.

Accidental Insider

MOTIVATION	None
SKILL	LIMITED
FINANCIAL RESOURCES	LIMITED
TIME AVAILABILITY	MODERATE
EQUIPMENT RESOURCES	MODERATE

The accidental insider harms the company not with malicious intent, but simply as a result of poor decision making. Fundamentally, people are an organization's weakest link. People create weak passwords and reuse them across different services, people lack discretion when clicking links in emails or inserting random thumb drives; and people are notoriously susceptible to social engineering attacks. All of these conditions lead to otherwise trusted employees unwittingly turning into the accidental insider.

Privacy Encroacher

MOTIVATION	**Profit, revenge, preparation for additional attacks**
SKILL	MODERATE
FINANCIAL RESOURCES	MODERATE
TIME AVAILABILITY	MODERATE
EQUIPMENT RESOURCES	LIMITED

These transgressors include private investigators, paparazzi and others seeking to gain private information. They intend to learn something about a guest or document a target's activity. They may be well versed in technology. Their activities range from documentation of events to embarrassing and compromising photographs. They have the potential to cause significant reputational harm to an hotelier or vendor.

Property Thief

MOTIVATION	**Profit, Revenge**
SKILL	MODERATE
FINANCIAL RESOURCES	LIMITED
TIME AVAILABILITY	LIMITED
EQUIPMENT RESOURCES	LIMITED

Property thieves are offenders who attack guests and employees with an intention to steal property, such as jewelry, money and supplies. They may be well versed in technology. If they attack a guest, they can cause a fair amount financial and reputational harm to hotel brands, hotel owners and vendors.

Violent Criminal

MOTIVATION	**Revenge, Coercion, Mental Defect**
SKILL	LIMITED
FINANCIAL RESOURCES	LIMITED
TIME AVAILABILITY	LIMITED
EQUIPMENT RESOURCES	LIMITED

A violent offender is an individual who seeks out guests and employees with the intent to impact personal safety. Their crimes spread the spectrum, from simple assault to more egregious and damaging. They are not expected to be capable of complex, high-tech attacks.

Attack Surfaces

The sum of attack vectors, or means by which a threat might carry out an attack against an asset, is referred to as a system's attack surface. In analyzing the security of a system, attack surfaces help identify areas or components of elevated risk that should be prioritized during assessment activities.

Potentially impacted system components are enumerated along with example attack vectors making up the attack surface; in the absence of security assessment against a concrete implementation, vulnerabilities are assumed based upon the component's role in the system (e.g., a system that interacts with users via a web application is assumed vulnerable).

Note: This list should be considered extensive, but not exhaustive. As each organization customizes this threat model to their unique set of circumstances, new attack surfaces are likely to be discovered, while some of these attack surfaces may be deemed inapplicable. Furthermore, as adversary techniques and technologies evolve, so too will attack surfaces change over time.

Network Attack Surface

Vectors making up a network attack surface typically involve exposures and vulnerabilities within network protocols and services. Components associated with the network attack surface are:

- Central System Server
- Key Encoder
- Key
- Mobile Device Key
- Lock Device
- Portable Programmer
- PMS Backend Server & Database
- Related Backend System Server & Database

Attack vectors making up this attack surface include:

Host operating system vulnerabilities. Unpatched operating systems leave unmitigated exposures on devices with network connectivity. Compromise of an operating system vulnerability may provide and attacker with full control over the compromised system.

Insecure, default configurations. Device manufacturers may provide default configurations, for ease of installation, that are meant to be further tightened in a production environment. For example, portable programmer devices may have relaxed (or disabled) access control configurations in place for rapid initial roll-out. Improper configuration after deployment increases the risk of compromise using such a device.

Unnecessary & insecure services. Services operating within either the host operating system or an application may present additional exposures; unnecessary services and services with known security concerns (e.g., Telnet, FTP) should be disabled on production components.

Poor or missing access control & authorization. Failure to implement proper access controls, like effective and multi-factor authentication, present exposures that may lead to asset compromise. This attack vector extends to physical layer attacks targeting access ports of lock devices.

Software Attack Surface

A software attack surface involves attack vectors that target a running application's inputs. As attackers continue to easily exploit vulnerable software, especially web applications, accounting for this particular type of attack surface is crucial, especially considering the highly integrated ecosystem in which these components typically interact. Components associated with the software attack surface are:

- Central System Server

- PMS Backend Server & Database
- PMS Front of House Workstation
- Related Backend System Server & Database
- Related Front of House Workstation
- Mobile Device Key

Attack vectors making up this attack surface include:

Software and application vulnerabilities. Common software design and development errors, as described in lists like OWASP Top Ten and CWE/SANS Top 25 Most Dangerous Coding Errors, may present vulnerabilities ranging from sensitive information disclosure (for development of additional attacks) to complete system compromise. Depending upon the compromised component, escalation of privilege and access to other systems is possible. Examples of attack mechanisms include cross-site scripting, SQL injection, and cross-site request forgery.

Insecure, default configurations. Default software installations are not likely hardened against common attacks; default login credentials, encryption keys, and other default configuration artifacts leave a system vulnerable to known attacks with readily available exploit tools.

Lack of security architecture. Without a valid threat model to aid in the alignment of security objectives beginning with system design, product vendors may lack the ability to identify security critical components and, as a result, implement weak or broken security architectures. Examples include insecure storage of authentication credentials, broken cryptographic implementations, and invalid segregation of application components (i.e. trust zones).

Human Attack Surface

Actors that interface with a system are typically considered an additional attack surface. Example vectors such as social engineering target the knowledge or access of a user. Components associated with the human surface area are:

- Property Management

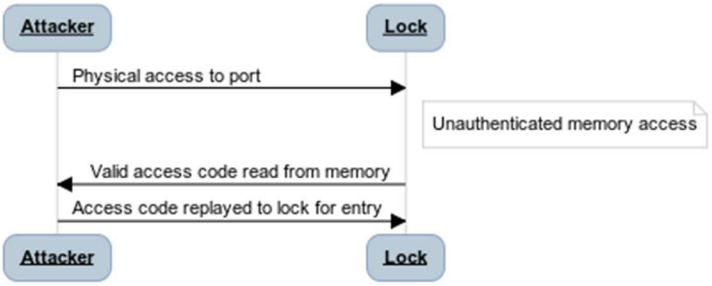
Social engineering and related attack types against human elements of a system are considered out of scope in this threat model.

Misuse & Abuse Cases

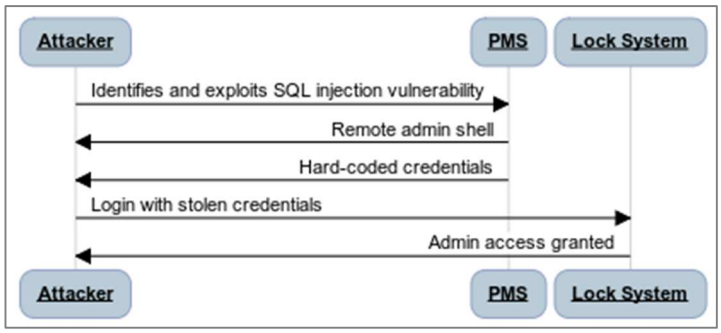
Ultimately, a threat model should define specific attack scenarios, referred to as misuse & abuse cases, in the context of the assets, threats, and potentially vulnerable system components (or attack surfaces) identified in the exercise. By assessing the overall risk, which can be simplified as a quantification of the impact and likelihood of a successful attack occurring against an asset, mitigating strategies can be prioritized to address areas of most concern.

The following list should be considered representative but not exhaustive; these cases will be applicable to most or all emerging lock systems. However, as all systems are unique, additional cases likely apply to individual products, and those cases should be considered in each evaluating concrete product implementations.

An Adversary Gains Access to a Lock Device Port

ATTACK SURFACE	Network
AFFECTED ASSETS	Guest Personal Safety Guest Personal Property Employee Personal Safety Proprietary Corporate Information & Business Intelligence Guest Information & Privacy Brand Reputation Guest Trust
THREATS	Hacktivists Individual Hacker Privacy Encroacher Property Thief Violent Criminal Opportunistic Insider
IMPACTED COMPONENTS	Lock Device Portable Programmer
ATTACK VECTORS	Tampering, Reverse Engineering
ATTACK DETAILS	

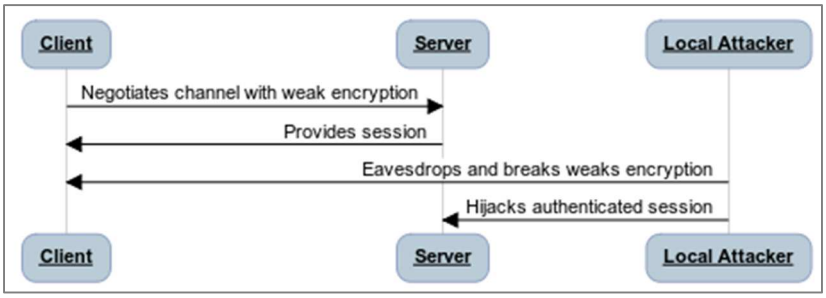
An Adversary Gains Unauthorized Access to the Lock Management System by Compromising a Connected System

ATTACK SURFACE	Network Software
AFFECTED ASSETS	Guest Personal Safety Guest Personal Property Employee Personal Safety Proprietary Corporate Information & Business Intelligence Guest Information & Privacy Brand Reputation Guest Trust Log File Data Confidentiality Log File Data Integrity
THREATS	Organized Crime Corporate Sponsored Espionage Hacktivists Individual Hacker
IMPACTED COMPONENTS	Central System Server PMS Backend Server & Database Related Backend System Server & Database Mobile Device Key
ATTACK VECTORS	Command Injection (cross-site scripting, SQL injection)
ATTACK DETAILS	

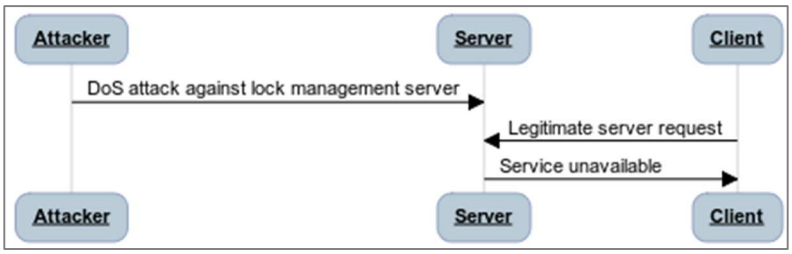
An Adversary Extracts Key Card Data by Exploiting Weak Protocols

ATTACK SURFACE	Network
AFFECTED ASSETS	Guest Personal Safety Guest Personal Property Employee Personal Safety Proprietary Corporate Information & Business Intelligence Guest Information & Privacy Brand Reputation Guest Trust
THREATS	Nation State Intelligence (Advanced Persistent Threat) Organized Crime Corporate Sponsored Espionage Hacktivists Individual Hacker Privacy Encroacher Property Thief
IMPACTED COMPONENTS	Key Lock Device Mobile Device Key
ATTACK VECTORS	Reverse Engineering, Cryptanalysis, Tampering
ATTACK DETAILS	Existing RFID lock mechanisms present identifiable risk varying by implementation. RFID key devices may feature backward compatible technology (like magnetic stripe) that potentially diminishes the security of the data (e.g., requires plaintext storage). RFID lock devices may implement weak, outdated protocols for data transmission. Recent research[iii] has demonstrated susceptibility to eavesdropping in the Wiegand protocol; with the introduction of a device into the RFID lock's physical layer, access codes stored on and transmitted by the key are intercepted and broadcast via a Bluetooth Low Energy (BLE) transmitter. Once intercepted, replay of access codes back to the lock system allow remote control of the lock device until the intercepted codes are invalidated.

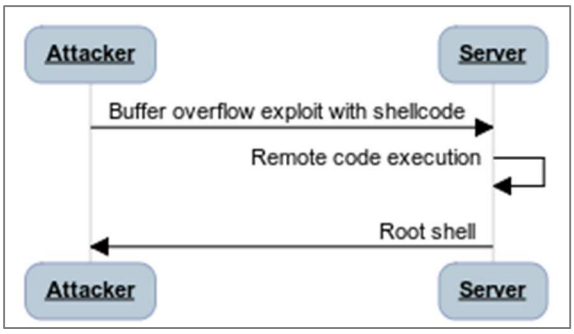
An Adversary Captures a Protocol Exchange and Gains Access to Critical Security Parameters

ATTACK SURFACE	Network
AFFECTED ASSETS	Guest Personal Safety Guest Personal Property Employee Personal Safety Proprietary Corporate Information & Business Intelligence Guest Information & Privacy Brand Reputation Guest Trust
THREATS	Nation State Intelligence (Advanced Persistent Threat) Organized Crime Corporate Sponsored Espionage Hacktivists Individual Hacker
IMPACTED COMPONENTS	Central System Server Key Lock Device PMS Backend Server & Database
ATTACK VECTORS	Eavesdropping, Cryptanalysis, Reverse Engineering
ATTACK DETAILS	

An Adversary Uses the Wireless Network to Launch a Denial-of-Service Attack on the System

ATTACK SURFACE	Network
AFFECTED ASSETS	Lock System Availability Guest Personal Safety Guest Personal Property Employee Personal Safety Brand Reputation Guest Trust
THREATS	Nation State Intelligence (Advanced Persistent Threat) Organized Crime Corporate Sponsored Espionage Hacktivists Individual Hacker
IMPACTED COMPONENTS	Central System Server Lock Device PMS Backend Server & Database Related Backend System Server & Database
ATTACK VECTORS	Denial of Service
ATTACK DETAILS	

An Adversary Injects Malicious Code via the Lock Device Update Channel

ATTACK SURFACE	Network
AFFECTED ASSETS	Guest Personal Safety Guest Personal Property Employee Personal Safety Brand Reputation Guest Trust Log File Data Confidentiality Log File Data Integrity
THREATS	Nation State Intelligence (Advanced Persistent Threat) Organized Crime Corporate Sponsored Espionage Hacktivists Individual Hacker
IMPACTED COMPONENTS	Central System Server Lock Device PMS Backend Server & Database
ATTACK VECTORS	Buffer Overflow
ATTACK DETAILS	

Validation

The threat model presented in this document is a framework that must be customized for the specific implementation and security requirements of a particular organization. After the hotel customizes the threat model, it is critical that the hotel validate its security posture with the threat model in mind. Validation occurs through the performance of security assessments.

When a hotel engages an outside party to perform the security assessment, the following should be well-understood in order to maximize the effectiveness of the assessment and best calculate risk:

- What type of assessment is being performed?
- What is the scope of the assessment?
- What is the methodology being used for the assessment?
- What are the periods of reassessment?
- Will mitigation be articulated?
- What are the types of deliverables the assessment will produce?

Establishing a programmatic approach to security, using the threat model and validation frameworks presented in this document, provides for effective risk management.

Conclusion & Recommendations

This threat model demonstrates the highly connected environments in which lock systems operate. The lock system itself exists as a set of controls to mitigate risk to assets like guest safety and privacy; however, the lock system is also a subset of a much larger ecosystem of integrated services, data sources, and users. Within that ecosystem, integration of components can easily lead to additional exposures that may introduce new security risk to assets both within the locking system in particular and in the related systems more broadly.

Independent Security Evaluators recommends the following actions:

- Use this document as a framework to further define security risks related directly to lock systems as well as related connected systems.
- Consider additional aspects of the threat model that may be unique to your system.
- Conduct a thorough, manual security assessment of the components and systems described within your unique threat model. Only assessment against concrete system implementation will identify vulnerabilities and their potential for exploitation.
- Ensure that the security assessment is performed by a neutral third party security firm, in conjunction with in-house resources.
- Engage a neutral third party security firm with which to collaborate on secure design and development activities, as it pertains to your unique threat model. Security should be built into the development lifecycle throughout, not simply addressed upon the conclusion of a given development initiative. By understanding security risks as they are introduced at each stage of the development process, proper controls can be strategically built into the system, thereby enabling an organization to architect mitigations accordingly and effectively minimize risk.

About the Authors

ISE's Executive Partner Ted Harrington is co-chair of the HTNG Door Lock Security Working Group, and a regular speaker on security topics at HTNG events around the world.

Founded in 2005 out of the PhD program at the Johns Hopkins' University Information Security Institute by first hacking the Texas Instruments RFID platform used in automobile immobilizers, ISE is a security research and consulting firm that performs manual, white box security assessments. ISE's research division has contributed several groundbreaking findings to the research community, including by being the first company to exploit the iPhone, Android OS, ExxonMobil SpeedPass, Diebold eVoting Machines, and numerous others. ISE's most recent research discovered systemic issues in wireless routers[iv], network attached storage[v], and web browsers[vi]. ISE is the organizer of the first -ever router hacking competition *SOHOpelessly* Broken[vii] at esteemed security conference DEF CON, as well as the organizers of DEF CON's newest concept, IoT Village[viii]. ISE executives and analysts contribute thought leadership through many outlets, including as speakers at security events such as BlackHat, DEF CON, RSA, DerbyCon, BSides, CanSecWest and more.

---

[i] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[ii] http://cwe.mitre.org/top25/

[iii] https://github.com/LinkLayer/BLEKey

[iv] http://securityevaluators.com/content/case-studies/routers/soho_router_hacks.jsp

[v] http://www.infoworld.com/d/security/network-attached-storage-devices-more-vulnerable-home-routers-247875

[vi] http://securityevaluators.com/content/case-studies/caching/index.jsp

[vii] www.sohopelesslybroken.com

[viii] www.iotvillage.org