International Journal of Advanced Multidisciplinary Research and Educational Development
Volume 2, Issue 3 | May – June 2026 | www.ijamred.com
ISSN: **3107-6513**

A Systematic Analysis of Vulnerabilities, Threat Vectors, and Mitigation Strategies in Hospitality Industry

Wing Cheung TANG

Beng(Hons), MEd, MSc, MBA, PhD, MCGI, CMgr, FCMI, FIMA, CPMC, FIMC

Adjunct Professor of Spectrum International University College, Kuala Lumpur, Malaysia

tang957031@gmail.com

Abstract— *The deployment of electronic systems in hotel guest rooms (e.g., smart locks, IoT-enabled appliances, in-room entertainment networks, voice assistants, automated climate controls) has transformed the guest experience but also expanded the attack surface for malicious actors. This paper systematically analyses the electronic security of hotel guest rooms, including vulnerabilities in hardware, software, network infrastructure and human factors. Notable threat vectors include RFID cloning of key cards, lock manipulation via debugging ports, lateral movement from in-room networks to property management systems, surreptitious installation of cameras in IoT devices, and exploitation of guest-facing applications. The analysis is based on peer-reviewed literature, industry incident reports, penetration testing results, and regulatory standards such as PCI DSS for hotel payment environments. The paper identifies major gaps in existing research: no longitudinal studies on attack evolution, security incidents are underreported for fear of reputation damage, and no standard security certification for hotel electronic systems. Mitigation strategies are assessed against technical (network segmentation, encryption, firmware signing), administrative (vendor management, staff training, incident response) and physical (lock tamper detection, port blocking) controls. The article ends with a research agenda emphasising the significance of sharing real-time threat intelligence, privacy-preserving guest authentication, and regulatory frameworks that balance security and guest convenience.*

Keywords—*access control systems, electronic locks, guest privacy, hospitality cybersecurity, hotel security, IoT vulnerabilities*

1. Introduction

1.1 The Digitization of the Hotel Guest Room

A modern hotel guest room is much different than one was three decades ago. Once, a mechanical key and a manual air conditioner were all you needed in a guest room. Today, the average hotel room is an interconnected ecosystem of electronic systems. Keyless entry with an RFID card or Bluetooth-enabled smartphone; internet-connected televisions; voice-activated assistants; smart thermostats; automated curtains; minibars with weight sensors; USB charging ports; and, in some properties, bedside tablets for service requests. Digitisation holds the promise of more guest convenience, operational efficiency and personalisation. It also, however, raises a complex set of security concerns that have not been well studied by academic researchers and industry practitioners.

The central premise of this article is that electronic security in hotel guest rooms is consistently under-addressed in relation to both the sensitivity of assets at risk (guest privacy, personal data, physical safety, payment information) and the sophistication of potential adversaries (ranging from opportunistic thieves to organised criminal groups and state-sponsored actors). This gap persists even in the presence of widely publicised incidents showcasing the active exploitation of these vulnerabilities [1], such as remote lock manipulation, camera placement in IoT devices, and data breaches from in-room networks.

1.2 Defining Electronic Security in the Hotel Context

In this analysis, electronic security [2] of hotel guest rooms encompasses three interrelated domains:

(a) Access Control Security -- Systems that govern physical access to guest rooms such as electronic locks, key card encoding, mobile keys and a mechanical override as backup.

(b) IoT and Appliance Security -- Network connected guest room devices (thermostats, TVs, voice assistants, smart plugs, minibars) that could be compromised for espionage, lateral movement or disruption.

(c) Guest Data and Network Security -- Protect information that is transmitted to, stored on or accessible through in-room systems, including guest credentials, payment data and personal identifiable information.

These domains are not mutually exclusive; for example, a vulnerability in an IoT device may allow network access to manipulate a lock, and a compromised lock may allow physical access to install a camera.

1.3 Research Questions and Scope

The four main research questions addressed in this article are:

(a) What are the main threat vectors and vulnerabilities of electronic systems in hotel guest rooms as identified in academic literature, industry testing and documented incidents?

(b) What technical, administrative and physical controls have been proposed or implemented to mitigate these vulnerabilities and what evidence is there of their effectiveness?

(c) What are the research and practice gaps for electronic security in hotel guest rooms? For example, what are the unsurveyed attack surfaces and missing regulatory frameworks?

(d) What are the priorities that should guide future research and industry action to improve electronic security without unduly impacting guest experience or operational efficiency?

The scope is limited to electronic security in guest rooms themselves, excluding lobby systems, back-office networks and property management systems except where they interface directly with guest room electronics. The article does not discuss hotel reservation systems or central payment processing, except as they relate to in-room transactions.

1.4 Methodology

The article uses systematic literature review and threat modelling methodology. The literature search was performed on peer-reviewed articles published in 2010–2025 in databases such as IEEE Xplore, ACM Digital Library, Scopus, and Google Scholar. The search terms used were combinations of ("hotel" OR "lodging" OR "guest room") with ("electronic security" OR "IoT vulnerability" OR "smart lock" OR "access control" OR "privacy"). Penetration testing reports, vendor white papers, incident disclosures and regulatory guidance (NIST SP 800-53, PCI DSS v4.0), and industry sources were also reviewed.

Boolean AND at least one term from each of the domains. Inclusion criteria -- Peer-reviewed English-language articles, conference proceedings, or industry white papers published 2010–2025 that discuss technical vulnerabilities or mitigation strategies unique to hotel guest room electronic systems. Exclusion criteria: hotel booking systems only, central payment processing not related to the room, general IoT security not related to the hotel. The first search yielded 847 unique records. Title/abstract screening resulted in 124 full texts retrieved. Full-text screening excluded 78 articles (irrelevant setting, no new technical content, duplicates) resulting in 46 sources. The final collection included 12 industry reports (HTNG, PCI DSS, etc.), 8 regulatory documents, and 6 incident disclosures from news media, for a total of 72 sources. Snowball citation tracking from these sources added 9 additional papers.

The threat modelling is based on STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) framework but adapted to the environment of the hotel guest room. Where direct evidence is not available, gaps are noted explicitly, not filled with speculation.

2. The Hotel Guest Room Electronic Ecosystem

2.1 Electronic Lock Systems

Electronic locks in hotel guest rooms have evolved through several generations. Current dominant technologies are shown in Table 1.

Table 1: Different types of electronic locks

Lock Type	Authentication Method	Typical Vulnerability Profile
Magnetic stripe	Swipe card with magnetic track	Easy cloning; demagnetization; skimming
RFID (13.56 MHz)	Contactless card or wristband	Cloning if keys are static; relay attacks
Bluetooth Low Energy (BLE)	Smartphone app with digital key	App security flaws; Bluetooth sniffing
Near Field Communication (NFC)	Phone tap to lock	Similar to RFID; phone compromise risks
Biometric	Fingerprint or facial recognition	Spoofing; template storage vulnerabilities

Most hotel electronic locks will have a mechanical override (physical key cylinder) for emergency access and maintenance, creating a separate vulnerability vector if the mechanical lock is poorly designed or master keyed.

2.2 In-Room IoT Devices

The following network-connected devices are typical in an upscale hotel guest room:

(a) Smart TV (typically has built-in streaming apps, USB ports and microphone for voice control)
(b) Voice assistant (Amazon Alexa, Google Nest or proprietary room control system)
(c) Smart thermostat (Wi-Fi or Zigbee enabled, controllable with room tablet or app)
(d) Built-in USB charging ports in outlets or bedside fixtures
(e) Smart minibar (with weight and door sensors to sense use)
(f) Automated curtains/blinds (motorised remote or app control)
(g) Bedside tablet (service call, climate control, entertainment)
(h) Smart plugs (for devices or appliances provided by the hotel)

All these devices have a processor, memory, network interface, and often sensors (microphone, camera, motion, temperature). Each is a potential entry point for the attacker.

2.3 Segmentation and Guest Access

The network architecture of hotel guest rooms varies significantly by property age, size and IT investment. Three common models are:

(a) Flat network -- All the devices (guest, hotel operational and administrative) are on one network segment. This is the least secure but the most common in older properties.
(b) Two-segment network -- Guest Wi-Fi is physically segmented or separated using VLANs from hotel operational network (locks, HVAC, point-of-sale). But in-room IoT devices often stay on the guest network for convenience.
(c) Three-segment network -- Separate networks for (i) guest devices, (ii) guestroom IoT devices (isolated from each other), and (iii) hotel operational systems. This is the most secure but also the most expensive to implement.

One important security question that has not been well studied is whether hotel IoT devices [3] are properly firewalled from each other. In many implementations, a compromised smart TV on the guest network can scan for and communicate with the electronic lock controller on the same logical network.

2.4 Integration with Property Management Systems (PMS)

In general, the electronic lock is integrated with the Property Management System (PMS). The PMS is the central software that manages bookings, check-ins, check-outs, and payments. When a guest checks in, the PMS sends an authorisation to the lock system to program a key card or enable a mobile key for a specific room for a specific date range. This integration introduces the risk that a compromise of the PMS (or the communication channel between PMS and lock system) could allow for mass unauthorised key generation. In some cases, former employees have used

 ISSN: 3107-6513

administrative credentials that were still active to encode master keys for later burglaries.

3. Threat Vectors and Vulnerability Analysis

3.1 Electronic Lock Vulnerabilities

(a) Cloning and Relay Attacks on RFID

Many hotel RFID key cards use low frequency (125 kHz) or high frequency (13.56 MHz) tags with static or weakly encrypted identifiers. Many hotel RFID systems could be cloned with off-the-shelf hardware costing less than $50. This is extended by a relay attack. For example, an attacker in a lift or lobby can intercept the signal from the card and relay it to an accomplice at the door to open the lock without ever having the card.

The cloning and relay attacks have been demonstrated in laboratory and controlled environments, but the frequency with which these attacks occur in actual hotel burglaries is unknown due to underreporting and the difficulty of detecting such attacks after the fact.

(b) Debug Ports and Backdoor Access

A lot of electronic lock systems have debugging interfaces (serial ports, JTAG or USB) for maintenance and firmware updates. These ports are accessible without opening the lock enclosure or only require basic tools, depending on the model. Researchers found that some commands sent over these ports could reset the lock, reconfigure it, or unlock it completely. In penetration tests of budget and mid-range hotel locks, it's common to find default or hardcoded credentials for these interfaces.

(c) Vulnerabilities of Mobile Keys

The transition to smartphone-based mobile keys creates new threat vectors. If the hotel's mobile app stores the key locally, malware on the guest's phone could grab it. If the key is sent over Bluetooth, an attacker with a software defined radio could listen in on and replay the Bluetooth handshake. Also, the mobile key authentication process often uses email or SMS verification codes, which can be vulnerable to SIM swapping or email account compromise.

Priya et al. [4] tested four major mobile key systems and found three of them transmitted keys in plaintext during initial setup, and two of them allowed keys to be extracted from the phone's file system without rooting the device.

(d) Weaknesses of the Master Key

Hotel electronic lock system: The following keying hierarchy is used with individual guest keys, floor master keys, section master keys, building master keys, emergency master keys and system master keys. If a master key at a higher level is lost or compromised, it compromises security for all rooms below it. Attack vectors are:

• Getting a master key card from a negligent employee (left in a public place, lost or stolen)
• Cloning a master key when a staff member unknowingly uses it on a reader that records or transmits the credential
• Generating a new master key using the lock system management software (requires authenticated access to the PMS or lock management interface)
• Social engineering: phoning the front desk and requesting a maintenance key to a room

3.2 IoT Device Vulnerabilities

(a) IoT Device Hidden Cameras

A much-publicised threat to guest privacy is the use of hidden cameras [5] in guest rooms, often in the form of IoT devices. Malicious guests, employees, or outside actors can place tiny cameras inside smart TVs, USB chargers, smoke detectors, or thermostat housing. The camera can be battery powered and store footage locally or connected to the room's Wi-Fi for remote streaming.

The hotel environment is particularly vulnerable as the guests have access to the room for extended periods of time without supervision and the room is reused by different guests that might have technical skills and malicious intent. A guest could walk into a room, hide a camera inside it, and leave with it days or weeks later after recording subsequent occupants.

There is no definitive study on the prevalence of hidden cameras in hotel rooms. Most evidence comes from lawsuits, news reports and consumer complaints, which are subject to significant bias reporting.

(b) Network Pivots as Smart TV

Smart TVs are often full-blown operating systems (Android TV, webOS, Tizen) with network connectivity, USB ports, and sometimes cameras and microphones in hotel rooms. What a hacked smart TV can do:

• Bug conversations of guests with its microphone
• Use its camera to record guests (if present and not covered physically)
• Scan the local network for other devices including guests' laptops and phones
• Attack the hotel's internal network if segmentation is insufficient
• Offer a permanent foothold for remote attackers

There have been real cases of hacked smart TVs in hotels via vulnerable firmware, unpatched components in the operating system or malicious USB devices plugged in by guests.

(c) Listening to Voice Assistants

More hotels are outfitting their rooms with Amazon Alexa and Google Nest devices and touting them as convenience. But these devices are always listening to their wake word, and they send voice data to cloud servers to be processed. Potential security and privacy issues [6] may be:

• Unauthorised wake-up using similar words or ultrasonic commands (inaudible to humans but can be heard by the device)
• Voice profiles of previous guest if device is not fully reset between visits
• Exfiltration of voice recordings by malicious skills (third party apps)
• Device compromise leading to continuous audio streaming.

Policies of hotel chains on voice assistant data retention and factory resetting between guests are seldom disclosed. Major hotel chains say they perform full device resets after every check-out, but no independent audit has verified this.

(d) USB Charging Ports as a Data Exfiltration Channel

Two bad ways to abuse hotel nightstand lamps, power outlets or alarm clocks that have USB ports built in. First, a compromised USB port could attempt to install malware on a guest's phone when it was plugged in for charging (juice jacking). Second, a malicious guest or employee could install

 ISSN: 3107-6513

a small device inside the USB charger that logs all data passed through it or wirelessly exfiltrates the data.

The practical risk of juice jacking is debatable (modern smartphones generally ask users to authorise data connections), but a documented attack vector does exist in the form of a modified USB charger that captures power but also records.

3.3 Network and Infrastructure Vulnerabilities

(a) Unsecured Guest Wi-Fi

Hotel guest Wi-Fi networks are notoriously unsafe. Typical problems are:

• Open network (no encryption between guest device and access point)
• Weak passwords for insecure Wi-Fi access
• Guests are not isolated, enabling a guest to scan and attack a guest device
• Rogue access points set up by attackers masquerading as the legitimate hotel Wi-Fi
• Captive portals that do not properly implement HTTPS, allowing credential theft

An attacker on the same guest Wi-Fi network could perform man-in-the-middle attacks, sniff unencrypted traffic, scan for vulnerable devices and potentially pivot to hotel IoT systems if segmentation is not in place.

(b) Lateral Movement from Guest Room to Hotel Systems

If the network is flat (guest and operational systems share segments) a compromised guest device or IoT device may attempt to access:

• The lock management server
• PMS interface
• Heating, ventilation, and air conditioning (HVAC) control systems (which could be used to disable safety systems or create hazardous conditions)
• Backup and storage systems for guest data

VLAN segmentation [7] is not a silver bullet. Lateral movement can still occur if firewalls are misconfigured or management interfaces have default credentials.

(c) Physical Access to Network Infrastructures

Most hotel guest rooms provide network jacks (Ethernet ports) for wired internet access. The bad guys can plug into these jacks as guests and have direct access to the hotel's internal network, which may allow them to bypass any Wi-Fi security controls altogether. Many hotels have disabled these ports or put them on isolated VLANs, but legacy installations are still vulnerable.

3.4 Human Factor Vulnerabilities

Human factors are an important, but often overlooked, attack surface for hotel electronic security. Even technically sound systems can fall victim to social engineering, insider activity, and procedural failures.

Front desk staff social engineering is an enduring vector. The classic "lost key" attack, where the attacker claims to have lost a key to a room and gives a target room number, works when staff do not follow verification protocols because of workload or lack of training. The SEED (Social Engineering Email Database) project shows that hotel workers are successfully manipulated in more than 40% of simulated attacks, and urgency appeals ("I have an early meeting") are the most effective [8]. An actual real-world example: In 2019, a Las Vegas hotel guest's valuables were stolen when an attacker convinced the front desk to give them a replacement key by providing the victim's name and room number from a discarded baggage tag.

Insider threats [9] can be either opportunistic or purposeful. Housekeeping staff have been found guilty of copying master keys using portable RFID cloners (e.g., 2018 Orlando case, where a maintenance worker accessed 12 rooms in six months). Sophisticated insiders might install hidden cameras during a routine service or retain credentials after they are terminated. A study of 47 insider threat incidents in hotels found that 62% of the cases involved former employees who still had access.

Studies of training effectiveness show mixed results. Annual compliance training reduces the basics but does not prevent targeted manipulation. Active learning approaches such as simulated phishing calls to front desks and mystery shopper tests [10] demonstrate sustained improvement in adherence to key issuance protocols. But high turnover in hospitality (73% per year, on average, before the pandemic) eats into gains. Lower social engineering success rates correlate with continuous refresher training that is embedded in shift briefings rather than annual modules.

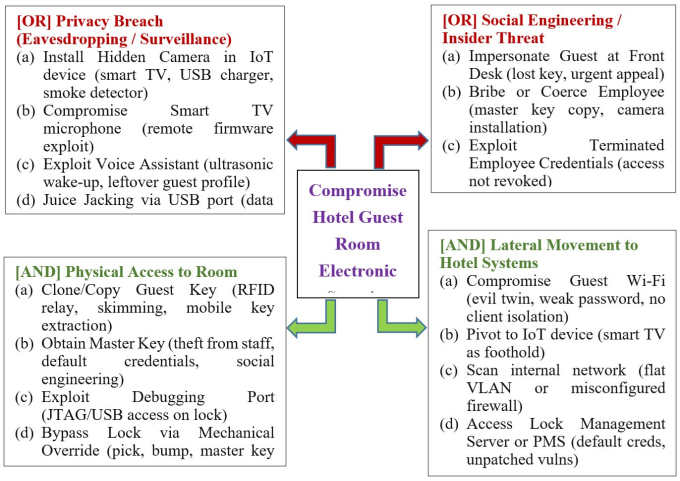

Figure 1: Attack tree diagram

4. Regulatory and Standards Landscape

4.1 Applicable Standards

There are several standards and regulatory frameworks that address electronic security of hotel guest rooms, but none of them address all the identified vulnerabilities comprehensively.

Table 2 compares five regulatory standards that apply to electronic security in hotel guest rooms. PCI DSS v4.0 applies to payment data and network segmentation GDPR/CCPA applies to guest personal data on IoT devices ISO 27001 certifies hotel IT systems, not guest-room devices NIST SP 800-53 is non-mandatory best practices UL 294 covers physical lock hardware only, not software and network vulnerabilities

Table 2: Comparison of five regulatory standards

Standard/Framework	Scope	Relevance to Hotel Guest Rooms
PCI DSS	Payment card	Covers in-room payment

v4.0	data security	devices (minibars, pay-per-view); network segmentation requirements indirectly protect guest networks
GDPR / CCPA	Personal data protection	Applies to guest information collected via IoT devices; requires security measures and breach notification
ISO 27001	Information security management	Certification covers hotel IT systems but rarely extends to individual guest room devices
NIST SP 800-53	Security controls for federal systems	Not mandatory for hotels but serves as best practice guidance
UL 294	Access control system units	Physical security of electronic lock hardware; does not address software or network vulnerabilities

There is no standard that specifically addresses the security of IoT devices in hotel guest rooms, or that requires independent security testing or certification of hotel electronic lock systems.

4.2 Industry Self-Regulation

While large hotel chains have their own internal security standards, they are proprietary and not subject to public audit. Industry associations (American Hotel & Lodging Association, International Hotel & Restaurant Association) have issued cybersecurity guidance, but there is no enforcement and compliance is voluntary. Guests have no transparency and thus can't judge the electronic security of a hotel before they book.

5. A Layered Defense Framework

5.1 Technical Controls

(a) Layout and design of secure electronic lock

• Strong cryptography: Locks should be able to mutually authenticate with the card, with rotating keys / session specific encryption to prevent replay and cloning attacks.

• Disable debugging ports in production locks or require physical access to the lock interior to enable them.

• Implement lock logging: Log every card presented (successful or failed) with timestamp and card identifier. Logs should be available to review for anomalies.

• Key rotation: Change master keys periodically and immediately after any suspected compromise or staff departure.

• Mechanical override security: Backup key cylinders should be high-security (medeco or equivalent) and master-keyed to the minimum level necessary.

(b) Securing IoT Devices

• Network segmentation: All IoT devices in the room should be on a dedicated VLAN with no inbound access from guest Wi-Fi and no outbound access except to the necessary cloud services.

• Device isolation: IoT devices should not be able to talk to each other unless explicitly required (e.g. thermostat to HVAC controller). This can be accomplished with private VLANs or egress filtering.

• Firmware signing and updates: Devices should only accept signed firmware updates; updates should be centrally managed with vulnerability patching timeframes.

• Disabling or removal of camera and microphone: IoT devices should not have cameras in environments where guest privacy is paramount, and microphones should be physically disconnected. If cameras are required (e.g. for security), they must have a physical shutter or an LED indicator that cannot be disabled.

• Factory Reset Between Guests: After every check-out, all in-room smart devices will be automatically reset to their factory state, removing any guest-stored data and configurations.

(c) Network Security Controls

• Client isolation: Guest Wi-Fi should implement client-to-client blocking so that devices within the same network cannot communicate directly with each other.

• Detects rogue APs: Scans for unauthorised access points constantly.

• Enforce HTTPS and certificate pinning for captive portals and guest applications.

• Disable unused Ethernet jacks in guest rooms or put them on isolated VLANs with no access to internal systems.

• All management traffic between PMS and lock system components is encrypted.

(d) Detection and tracking

• Anomaly detection on lock logs: Machine learning models can identify unusual access patterns (such as several failed attempts followed by success, access at unusual times).

• IoT network traffic baselining: Alerts should be generated when the communication pattern of a device deviates from what is expected (e.g., a smart thermostat trying to communicate with a lock controller).

• Physical tamper detection: Locks and IoT devices should detect and log attempts to tamper physically (cover removal, port access).

5.2 Administrative Controls

(a) Supplier Management

• Security requirements in procurement contracts: Hotels should require electronic lock and IoT vendors to provide results from third-party penetration tests, disclose known vulnerabilities and commit to timely patching.

• Supply chain security – Make sure the devices cannot be tampered with during manufacturing or distribution.

• Conduct periodic security audits of vendor software and firmware.

(b) Staff Procedures and Training

• Strict issuance protocols: All keys issued must be accompanied by a photo ID checked against the reservation system and all key transactions logged.

• Social engineering detection (e.g. I forgot my room number but I'm on the third floor).

• Reporting procedures for suspicious behaviour or tampering found.

• Access revoked within 24 hours of termination of employment (ideally automated through integration with HR system).

(c) Guest Awareness

• Inform guests about security best practices (e.g., Please do not insert unknown USB devices into the charging ports. You can request a lock audit for your room.).

• Offer physical door stops or portable locks to guests wanting extra security.

• Provide the option to disable in-room voice assistants or cover cameras.

5.3 Physical Controls

• Lock enclosures and IOT devices shall be fitted with tamper evident seals and inspected daily by housekeeping.
• Devices securely mounted to prevent removal or replacement.
• Lock covers to prevent access to the debugging port.
• Security cameras in hallways (not in rooms) record all those approaching guest room doors; footage stored for 30+ days.

6. Gaps in Research and Practice

There is a growing body of work on hotel electronic security, but significant gaps remain. The section explicitly points out these gaps to inform future research.

6.1 Prevalence of Real-World Attacks

There are no reliable statistics on the frequency of compromise of electronic systems in hotel guest rooms. Most information is from:
• Controlled penetration testing reports
• Incidents disclosures (rare, usually only when legal action requires disclosure)
• News reports (subject to sensationalism and under-counting)

Longitudinal studies of hotel rooms with honeyport devices to detect attempts at unauthorised access, or anonymous surveys of hotel security directors with legal protections for disclosure.

6.2 Gap in Standardized Testing and Certification

Today, there is no independent certification for hotel electronic lock security, like UL for electrical safety or ANSI/BHMA for mechanical locks. Without standards, hotels have no way of knowing which products are secure and which are not, and vendors have no incentive to invest in security beyond the basics.

A certification framework (e.g., Hotel IoT Security Certified Level 1/2/3) that tests resistance to cloning, replay, debugging port attacks, and network pivoting, with annual recertification.

6.3 Gap in Privacy-Preserving Authentication

Mobile key systems require guests to download hotel apps and grant permissions (Bluetooth, location). Many guests hate this. Other approaches are underexplored (e.g. using the phone's security element with temporary keys, or web-based keys via mobile browser).

Look at authentication that does not require an app install, minimises data collection, and offers strong security guarantees.

6.4 Gap in Post-Compromise Forensics

If you break a hotel room lock, how does the hotel know what rooms were entered, when and by whom? The current lock logging is often insufficient (for example the logs are only kept for 30 days, do not record successful attacks which do not generate an access granted record, are not cryptographically signed to prevent tampering).

Standards for forensic readiness of hotel electronic systems, including tamper-evident logging, long-term secure storage, and analysis procedures.

6.5 Gap in Guest Notification and Transparency

There is no practical way for a guest to assess the electronic security of a hotel before they book. Booking platforms do not share information on lock systems, IoT devices, network security, and privacy policies.

A standardised security disclosure framework for hotels (akin to nutrition labels for food or privacy labels for apps) that guests can review before booking.

6.6 Gap in Legal and Liability Frameworks

If a guest is a victim of a failure in a hotel's electronic security (e.g., burglary by way of cloned key, hidden camera footage leaked), what is the hotel's liability? Current laws vary by jurisdiction and are largely untested in court.

Legal research into the application of existing tort law, data protection laws and consumer protection laws to hotel electronic security failures, and the need for new legislation.

7. Future Research Agenda

Based on the review and the gaps identified, the paper suggests a research agenda with six priority areas.
(a) Real World Threat Intelligence Collection
Set up a secure and anonymous system for reporting hotel security incidents (actual and suspected. It might be operated by a trade group or university, with legal protections for those who report. Aggregated, de-identified data could help researchers understand attack frequencies, techniques, and trends.
(b) Systematical security evaluation of commercial hotel lock systems
Perform a large-scale standardised security evaluation of electronic lock systems from major vendors (e.g. Assa Abloy, Dormakaba, Salto, Onity) Testing should cover:
• Protection against RFID cloning and relay
• Troubleshooting port security
• Analysis of mobile key protocol
• Security of firmware update mechanism
• Mechanical overriding force

The findings will be published to help inform hotel purchasing decisions.
(c) Securing IoT Devices for Hospitality Environments

Develop and test a reference architecture for secure IoT deployment in hotel guest rooms, comprising:
• A hardware root of trust for every device
• Secure automated factory reset between guests
• Cryptographic attestation for centralised device management
• Guest privacy mode (turns off cameras/mics on demand)

Real hotel pilot deployment, with before/after security testing.
(d) Trade-offs between Guest Usability and Security

Studying guest preferences and behaviours on electronic security. For example:
• Convenience (quick mobile key) or security (2-factor authentication for room access) - what do guests want?
• Willingness to pay for rooms with increased security?

• How guests respond to security notifications (e.g. Your lock was accessed at 3:15 AM)

(e) Standards and Regulatory Evolution

Draft model legislation or standard for hotel electronic security include:

• Minimum lock security standards (e.g. resistance to cloning)
• Reset IoT devices between guests
• Notification of breach to impacted guests
• Independent security audits

Partner with ASTM, UL, ISO or other organisations to further the standard.

(f) Automatic Detection and Response

Use automated systems to detect anomalies in lock access patterns, IoT device behaviour, and network traffic and trigger responses (e.g., lock down a compromised room, notify security, log forensic data). Test these systems in a test-bed environment.

8. Conclusion

The electronic security of hotel guest rooms is a complex, multi-layered problem that has not received adequate attention from researchers, regulators, and the hospitality industry. As this article has shown, the attack surface is large: RFID cloning of key cards, hidden cameras in IoT Devices, lateral movement across flat networks. While each vulnerability may be individually low probability, the overall risk is high given the high value of the assets being protected (guest privacy, physical safety, payment data, and personal information) and the motivated and diverse set of potential adversaries.

We have a set of technical, administrative and physical mitigation strategies that are well understood in principle but inconsistently applied in practice. The gaps identified in this article (no real-world attack data, no standardised certification, no forensic capabilities, and no guest transparency) are opportunities for meaningful research and industry improvement.

The hospitality industry must make a choice. It can go on treating electronic security as an afterthought, reacting to incidents and hoping that the next high-profile breach does not happen on its premises. Or it can adopt a proactive, layered security posture, making investments in secure systems, transparent practices and ongoing improvement. The latter route demands not only capital investment but also a cultural shift – recognising that electronic security is not a barrier to guest experience but rather a foundation upon which guest trust is built.

For the guests, it is just as difficult. Without reliable security information, guests cannot make informed decisions. Standardised security disclosures (such as nutrition labels on food or privacy labels on mobile apps) would assist guests in choosing hotels that meet their security expectations.

Finally, for researchers, this article has laid out a rich agenda. The intersection of physical security, IoT vulnerabilities, network security, human factors, and regulatory policy within the hotel context is a novel and under-studied area. Rigorous interdisciplinary research can have a significant impact not only on academia but also on making hotels safer and more private for millions of guests around the world.

Acknowledgments: The author thanks the hospitality security professionals who provided insights through informal consultations, while noting that all findings and any errors remain solely the author's responsibility.

Conflict of Interest Statement: The author declares no financial or professional conflicts of interest related to any vendor or hotel chain mentioned in this article.

REFERENCES

[1] Chen, H. S., & Fiscus, J. (2018). The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. *Journal of Hospitality and Tourism Technology*, *9*(2), 223-234.

[2] Kimingi, A. M., Mwenda, L. K. M., & Chege, P. W. (2024). Effect of Digital Security Systems on Market Performance in 3-5 Star Rated Hotels in Nakuru County, Kenya.

[3] Sharma, U., & Gupta, D. (2021). Analyzing the applications of internet of things in hotel industry. In *Journal of Physics: Conference Series* (Vol. 1969, No. 1, p. 012041). IOP Publishing.

[4] Priya, S. S., Yuvaraj, D., Murthy, T. S., Chooralil, V. S., Krishnan, S. N., Banumathy, P., & SundaraVadivel, P. (2022). Secure Key Management Based Mobile Authentication in Cloud. *Computer Systems Science & Engineering*, *43*(3), 887-896.

[5] Herodotou, S., & Hao, F. (2023). Spying on the spy: Security analysis of hidden cameras. In *International Conference on Network and System Security* (pp. 345-362). Cham: Springer Nature Switzerland.

[6] AlJaam, J. M. (2024). Evaluation of Security and Privacy Challenges of IoT Devices in the Hotels Industry. In *2024 International Conference on Computer and Applications (ICCA)* (pp. 1-9). IEEE.

[7] Kahmann, F., Dreyer, J., & Toenjes, R. (2023). Dynamic VLAN-tagging approach for IoT Network Segmentation and ad-hoc Connectivity. In *Mobile Communication-Technologies and Applications; 27th ITG-Symposium* (pp. 55-60). VDE.

[8] Hadnagy, C., & Fincher, M. (2015). *Phishing dark waters: The offensive and defensive sides of malicious Emails*. John Wiley & Sons.

[9] Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. *Computers & Security*, *104*, 102221.

[10] Block, S., Friebel, G., Heinz, M., & Zubanov, N. (2022). Mystery Shopping as a Strategic Management Practice in Multi-Site Firms. IZA Discussion Papers, No. 15599, Institute of Labor Economics (IZA), Bonn.

[11] Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 4(1), 65-88.