Armaan Kapoor
ECE455
Security Review #0
Part II

As we are reminded by the recent MGM breach and other contemporary security threats to the hospitality industry, it is evident that physical keys have been almost entirely phased out and replaced with digital keycards (RFID and magnetic strip variants). Today, when a guest checks into a hotel, the staff uses a computerized system to assign them a room key encoded with a unique identification number. The UID is stored in a database as a primary key, and relevant information, such as the guest's room number, check-in/check-out dates, and any access privileges they may have (e.g., access to fitness centers, parking areas, privileged elevators) are indexed in relational to their user access token. Modernization aside, key cards are conceptually quite similar to physical keys, they are essentially passive components that rely on a powered receiver (installed on each door) to emit radio waves which they absorb. They then reemit a modulated digital signature (in a process known as backscattering) which is in turn detected and processed by the reader. The reader is connected to a centralized control system, usually over the network to a server that queries a database to check whether the keycard bearer holds valid access permissions for that particular door at that specific time.

In practice, the seamless operation of a digital keycard system and other IOT devices is abstracted away from often nontechnical managers and is controlled by a Hotel Property Management System (PMS). A PMS is a comprehensive software suite that serves as the backbone of a modern hotel's operational infrastructure. Traditionally, a hotel PMS was used for tasks like reservations, front office operations, and billing. However, its functionalities have expanded to include the management of digital keycards and automated check-in and checkout processes (Oracle). Cloud-based PMS systems are serviced and maintained by SAAS providers like Oracle, who promise efficient and scalable routines in return for service fees.

The foremost critical assets of PMS systems are UIDs. If these numbers are compromised, unauthorized individuals could gain access to rooms or other secure areas. If the integrity of PMS backends/databases is compromised, the entire access control mechanism at a multibillion-dollar chain of hotels could fail, leading to unauthorized access to rooms, or even a total lockdown. The security vulnerabilities that PMS systems face can be divided into two categories. Software exploits, and physical tampering.

When it comes to a metal key and traditional deadbolt loc, an attacker can easily sneak a lidar scan of a key, 3D print a near 1:1 replica, and then obtain a functioning copy, all without the concerned party knowing a thing. Using RFID cloning devices like the *Flipper Zero* yields a similar exploit in the digital realm, allowing man-in-the-middle attackers to seamlessly clone an arbitrary number of signatures and transmit them at will. Since the key card is a passive component, a malicious broadcast and authentic key signature bear no differences from the receiver's point of view. This type of exploit is inescapable, and can rarely be mitigated without adding significant friction to consumer interaction. This being said, by applying best practices like shielding against electromagnetic waves and not leaving key cards unattended around strangers, the likelihood of a man-in-the-middle attack can be significantly reduced. Theoretically, cards themselves can probably house a two-way public-private key encryption strategy, and that way the private key can be programmed into a receiver/transmitter circuitry, greatly increasing the effort an attacker would have to go through to extract the real uid associated with a card.

For a consumer, keycards, are convenient, easier to replace in a timely manner, and occupy a smaller footprint in pockets, wallets, etc. For hotels, keycards are cheaper to produce and provide more streamlined experiences since they don't need to be collected at checkout and can be virtually deactivated. At this point, it seems as if the vulnerabilities of physical/digital keys "cancel" each other out, and the added convenience factor makes digital keys favorable, however, we have to now consider the second category, software exploits.

Let's introduce the industry standard cloud PMS management system Opera. "Oracle Opera is a critical piece of software used by almost all major hotels and resorts around the world including Maldives. [Opera] holds the personal identifying information

(PII) and financial information of every gues (Cyber Security Maldives)." Recently, a critical vulnerability was discovered in Oracle Opera, identified as CVE-2023-21932. This vulnerability is not just a minor glitch but a severe security flaw that could potentially compromise the entire PMS system. Specifically, the vulnerability is an order of operations bug in the FileReceiver endpoint.

In a typical secure system, encrypted payloads for parameters like 'jndiname' and 'username' would first be decrypted and then sanitized to prevent malicious code injection. However, in Oracle Opera, this process is reversed. The payload is sanitized before decryption, making the sanitization ineffective and leaving the door wide open for attackers. This flaw allows unauthorized individuals to inject malicious payloads into these parameters, bypassing the system's security measures. The implications are dire: unauthorized access to sensitive guest data, financial information, and even the potential for complete control over the PMS system. Oracle has issued a critical patch update, but the onus is also on the businesses to implement these patches and secure their systems.

In the age of digital transformation, the hospitality industry faces a paradox. On one hand, digital keycards and cloud-based Property Management Systems like Oracle Opera offer unprecedented convenience and operational efficiency. On the other hand, they introduce a new set of vulnerabilities that can have catastrophic consequences if not properly managed. The recent discovery of the CVE-2023-21932 vulnerability in Oracle Opera serves as a cautionary tale, highlighting the urgent need for robust security measures. The incident underscores the importance of a multi-layered approach to security, one that addresses both hardware and software vulnerabilities. It also emphasizes the critical role of regular security audits and timely patch implementations.

SOURCES:

https://www.oracle.com/hospitality/what-is-hotel-pms/#:~:text=Traditionally%2C%20a%20hotel%20property%20management,managing%20room%20rates%2C%20and%20billing.

https://people.ece.uw.edu/nikitin_pavel/papers/APmag_2006.pdf