WIRELESS LOCKS: LONG TERM PITFALLS VERSUS SHORT TERM GAINS

By Bill Jacobs,
Principal, Jacobs Group Consulting

Introduction

Over the last few years, wireless locks have been increasingly promoted as a convenient solution for organizations to secure doors at a lower cost. While there are use cases where wireless locksets are effective, there are a number of customer requirements to consider when determining whether to use traditional hardwired access control or a wireless locking solution. Based on broad feedback from industry-leading access control OEMs, integrators, consultants and end-user organizations who have deployed wireless locks, this paper explores the long-term TCO concerns associated with deploying wireless locks versus the potential short term cost benefits they may offer.

When are wireless locks appropriate?

There are certain situations where wireless locks are good candidates for doors and openings. Some of these scenarios include:

- Extending security to remote locations and gates where conduit and wiring may be difficult to reach the area.
- Adding security to non-critical areas, such as cabinets, utility closets, elevators and conference rooms.
- Installing in structures with poor cabling, including buildings with asbestos and other issues affecting wiring, as well as for non-critical doors in very old buildings with concrete or cinderblock walls that could make it difficult to run cables to interior doors.
- Deploying in small businesses with simple, key-based security that are seeking greater convenience (over mechanical keys) with basic security functionality.
- When interior doors are pre-ordered/prepped for wireless locks as part of a new install. In this case, running wire may still be more cost-effective, depending on whether or not the building is pre-wired for Wi-Fi, if the doors are located in high-traffic areas and many other factors.

End users overall may have the perception that they are receiving "newer" technology when using wireless devices, even though they are still limited in functionality compared to hardwired systems. A sales executive at an access control provider in the Midwest[†] stated they often receive requests for wireless locking solutions based on the perception locks are an easier and less expensive "cure all" for securing an entire building.

However, in many situations, it quickly becomes obvious that the wireless approach is not the "be all and end all" once the customer is made aware of wireless locks functionality (in comparison to hardwired security solutions), stated the sales executive. The eventual outcome has been that the dealer/integrator often sells the customer a combination of wireless locks for the appropriate openings and hardwired access control for more critical and high-traffic openings, upon analyzing the risks of the area to be secured.

Pitfalls of wireless lock technology

Due to the inherent limitations in wireless lock technology, there are a number of important scenarios where the hardwired traditional access control solutions are the best choice for optimal security. All of the industry experts emphasized that wireless locks should never be used on exterior perimeter doors or high-security critical doors/openings. Furthermore, wireless locks are weather-resistant devices, but not all are weatherproof.

[†]References: All information was culled from extensive interviews with nine of the industry leading access control system providers, system integrators, consultants and end users across the country.

Using these locks doesn't offer the same level of assurance provided as when using an exterior-rated reader and mounting all of the electronics inside the secure side of the building. Moreover, there are an increasing number of interior doors and openings that have become more important to control as the security landscape continues to heighten. These doors and openings include student housing doors along with individual dorm rooms, IT room doors and other high-value areas where there is a need for immediate control of the locking device (i.e. lockdown). Across the board, industry experts highlighted some of the most common drawbacks of deploying wireless locks beyond the recommended scope of use cases:

1. Real-time versus "almost real-time." The critical seconds during a lockdown

Wi-Fi connected locking solutions operate in an offline mode and, despite ongoing efforts by wireless lock manufacturers, they have still not overcome the issue of offline time. In offline mode, the lock database is retained in the device memory and is only updated from the host if a pre-configured event or schedule is triggered. Depending on the capabilities of the security manufacturer's software, some of these triggers may need to be configured in each lock during installation, using a hand-held programming device that typically takes 20 minutes per lock to set up.

In comparison to PoE or standard electrified locks, Wi-Fi locks use more power and can drain the battery very quickly, since "wake-up" calls and battery life are directly proportional to card access usage, events, and host database updates. For example, when modifying lock synchronization time to increase call-in frequency, the battery life is decreased. With six batteries per lock, it is easy to see how a full-time, high maintenance issue can arise. As a result, Wi-Fi systems typically constrain themselves to checking in with the head-end server once or twice per day to conserve battery usage.

Some may see a benefit to using these locks that leverage a building's existing Wi-Fi network, but despite ongoing efforts by wireless lock manufacturers, they have still not overcome the fact that it is impossible to immediately lock-down a facility or have real-time reporting with wireless locks. A vice president at an access control provider on the West Coast further explained that a major shortcoming of Wi-Fi locks is that they cannot be "woken up" with a duress button or computer. They can only be communicated with when their polling time comes around, a specific event occurs or a lockdown access card is presented to each and every door.

Wireless lockset manufacturers using closed communications channels promote their technology as enabling "almost real-time" functionality; however, these locks can still take up to 10 seconds to initiate a lockdown. Some customers have also reported wireless solutions that take up to 15 seconds to initiate a lockdown. Given these latency issues, it is important to take into consideration the following steps required for a lock to communicate to the host in the case of a lockdown or any scenario requiring the device to be online:

1. The lock needs to "wake up;"
2. A session must be established;
3. The database downloads from the host to the lock; and
4. The communication session must terminate.

A vice president with an access control provider on the West Coast stated the latency they are seeing now for a lockdown is better than previous performance, but some things you need to make sure happen right away. When there is an event in a building, such as an active shooter situation, a matter of seconds can literally be a matter of life and death. Nothing is better suited for immediate response than a hardwired solution in this scenario.

These openings also cannot "wake up" all at once, but rather they activate consecutively. Consequently, the larger the wireless lock deployment, the longer the overall delay in activating all doors for lockdown in an emergency situation. After an extensive evaluation of three top wireless lock solutions, a major university decided against using wireless for perimeter or high risk/high value spaces. Even though they determined one of the locksets to be theoretically capable, they decided not to utilize wireless locks at any locations where lockdowns are critical.

Whether Wi-Fi or connected via closed communications channels, wireless lock deployments have caused a number of "bumps and bruises" for end users over time, stated a sales executive with an access control provider in the Midwest. He explained that end users often choose to deploy locks throughout a facility, even after having been properly educated on the risks of using them on perimeter openings and other critical areas. In some cases, people have chosen to "put up with" their new wireless lock system. In some cases, they have ripped out the locks and replaced them with traditional access control. In other scenarios, they have wired the locks for Power over Ethernet (PoE), which makes it possible for real-time lockdown commands to be sent to the locks but adds significant infrastructure cost to wire the lock – thus destroying the purported cost advantages.

2. Other critical functions requiring real-time access*

- Instant programming:
  - Adding, editing and removing cardholder access. While some Wi-Fi locks can perform a host authentication function, this can take up to a minute to process
  - Changing the settings of the lock (unlock schedules)
- Door status monitoring:
  - Door forced open situations and door held open situations
  - Valid and invalid access
  - Performing an unlock or lock command in scenarios such as buzzing in a visitor from a reception desk and other cases that require control of a door outside of a regular schedule
- Event reporting, as they happen.

**When using true wireless solutions, versus PoE-enabled locksets.*

3. More performance issues

<u>Connectivity</u>

Today's wireless systems communications are much better than the systems of 20 years ago, but they are more vulnerable to interference than a hardwired system. The RF bridge from the lock manufacturers is able to connect anywhere from to 8-16 locks; however, connectivity is affected by numerous factors, including the quantity and placement of wireless bridges, building materials and ambient RF noise. A vice president at an access control provider on the West Coast added that wireless locks generally don't deliver the connectivity performance expected out of the RF bridge between the controller and wireless lock.

While wireless proponents state their devices are faster to install, it is uncertain as to whether the RF bridge will reach all of the locks or how the signal will perform without mapping signal strengths at each lock location. For example, when many locks are spread over a facility, they can be out of range from the RF bridge, or there can be interference from the walls or the air that disrupts performance. Since the RF signal is disturbed by these ambient issues, typically more hubs or other RF bridges must be added to realize the full performance of the locks, explained the vice president. This reduces the one to many economic advantages marketed by lock manufactures.

Third-party software issues

One of the founders at an access control provider in the Midwest also noted their experience has been "somewhat painful" with the third-party software/middleware that is necessary to interface their software with the Wi-Fi or IP wireless locksets. He explained they've experienced a number of issues with the third-party software, making it difficult to work effectively with their customers and provide them a positive installation experience. The founder added that they lose complete control, functionality and the trust that they've established between their software and controllers.

Features limitations

There are numerous limitations and performance issues around online versus offline solutions as aforementioned. A top industry consultant on the East Coast also noted wireless locksets offer a "keyless entry" solution but they lack some of the higher level feature sets of true access control platforms, such as large cardholder and buffered transaction storage (for access levels, time zones, auto decision making, etc.), complex lockdown behavior, double card presentation and more – all of which impacts overall access control system performance.

Quality

To drive component costs down, wireless locks are assembled from parts supplied by different vendors. This can cause functional issues, whereas remediation and enhancements can take a long time. The consultant emphasized that integrators and end-users cannot specify best-in-class peripherals since the readers, contacts, and switches are built into locks. Instead, integrators are locked into the quality offered by the lock manufacturer, whereas hardwired solution components can be purchased from several different sources and will easily work together.

The "security of the security"

Since it is easier to access devices connected to a Wi-Fi network, Wi-Fi connected locks open a new realm of security issues that integrators may not be prepared for or have control over, such as basic network security concerns. Certainly greater collaboration with IT departments is warranted for these installations. As networks security is becoming more advanced, the locks themselves have been somewhat behind in the types of security protocols put on the devices. Additionally, wireless locks can "sniff" a Wi-Fi network, exposing them to more vulnerability, added one consultant. Furthermore, locks are generally more vulnerable due to lock vendors partnering with more third-party reader and other component suppliers who do not typically build security into their products; Additionally, lock vendors allow virtually anyone to integrate with the lockset.

Conversely, panel suppliers of true access control have historically proven to be proactive about the "security of their security," and have more security protocols in place. Panel suppliers tend to be very selective regarding whom they allow to integrate with their SDK as well.

Total cost of ownership: The hidden cost of wireless locks

When assessing an access control system over time, there is a tremendous difference between the costs of a door/opening installation versus total cost of ownership (TCO) for systematic building security over many years. Installing wireless devices on high traffic, critical and/or exterior doors and openings introduces significant hidden installation costs, maintenance and overhead. In some cases, these locks may still require cabling to be run for additional wireless access points or proprietary wireless controllers, depending on the installation…though less wiring is typically required than a traditional system.

Not only do these additional costs defy the initial economic argument for using wireless locksets, but there are numerous other hidden costs of wireless locks that include:

1. Battery life and maintenance

Wireless lock manufacturers advertise that their lock batteries last one or two years under "optimal"conditions, but battery life is completely dependent on usage and event reporting set-up. Exposing battery life as a percentage of usage is a feature that the host security system manufactures must have integrated into their software. Batteries will need to be replaced far more frequently for locks placed on high-traffic doors or heavily used openings, where the radio is waking up regularly.

Battery maintenance and service calls can be extremely labor intensive, and a leading security consultant recommends proactively scheduling battery replacements across the board – regardless of usage – every six months to a year to help reduce the TCO of the locksets. For example, the manpower to replace six batteries per lock on a campus with hundreds or thousands of locks is very time consuming and human resource intensive, so any proactive approach to maintenance will help alleviate the pain but not reduce the scheduled maintenance costs.

2. Wi-Fi networks

Maintenance of the Wi-Fi network also needs to be considered for wireless locks. Also, there needs to be IT engineering for Quality of Service (QoS), which is the capability of a network to provide better service to selected network traffic over traffic. If QoS is not in place, wireless lock traffic may not be prioritized over email and video download traffic. Corporate network architectures introduce other complexities, such as switches, routers and management tools, as well as multiple points of connectivity (LANs, intranet, and more). As an executive at a system integrator explained, all of this equates to multiple potential failure points. By nature, corporate networks are inherently more costly and require ongoing maintenance. These departmental costs and charge backs are often not factored into the total cost of ownership of wireless lockset mythology.

3. Firmware updates

The world is not perfect and hardware does require firmware (FW) updates on a regular basis. With PoE locks or access control panels, applying updates and/or FW updates is fairly easy through a centralized system that communicates to the hardware. With wireless locks, a completely different approach is required. Every lock must be updated through the serial connection, and an integrator must physically connect with each lock, initiate the FW update and verify its completion – all of which can take up to 20 minutes per lock.

4. PoE cost considerations

Using PoE enables locks to draw power from the Ethernet switch in order to bring wireless devices online all the time, without draining lock batteries. On the surface, it sounds like an ideal solution to the battery life and offline problem, but PoE adds a level of additional overhead to the installation that negates the savings wireless locksets offer. To use PoE with the locks, a network device/PoE switch must be added and pulling CAT5 or CAT6 cabling to the door is required, essentially converting the solution from wireless to wired. Calculations must be performed to verify the load does not exceed the PoE switch port's power output. Some of these PoE "wireless" locks also require the OEM to write to the third-party software in the PoE environment. Another overlooked item with PoE is the fact it requires more collaboration with the IT department, as IT now becomes responsible for

a piece of security hardware and its operational uptime. Service level agreements must be in place between departments to ensure reasonable uptime and back-up power for the Ethernet switch.

A sales executive at an access control provider in the Midwest emphasized that by the time you add up all of the additional expense to use PoE, there may be zero cost savings over a traditional access-controlled door. The result, end-user organizations may unknowingly have implemented a much lesser system compared to hardwired access control.

5. Service

Consider how much easier and less expensive is it to troubleshoot and replace a reader, REX, door contact, and even the electrified lock/strike in a traditional installation. It is much more expensive to replace an integrated wireless lock than to replace a single component.

6. Additional hardware and software costs

Prior to installation, it is uncertain whether the RF bridge will reach all of the wireless locks, and it is unknown how the signal will perform. The distance between the locks and the RF bridge, coupled with potential signal interference, could require more RF bridges to be installed in order to achieve the desired connectivity. A founding partner at an access control provider in the Midwest explained that many integrators have found the cost of installations to be far more than what they initially estimated in the bidding process. Some installations also require third-party middleware to integrate the locks into the access control system. This additional software brings along its own hardware requirements, along with recurring licensing fees.

7. Training

Wireless locks require installers to learn a new skillset – especially when installing expensive doors that can be ruined by drilling. Installing (and servicing) technicians need to be trained as locksmiths to address issues related to lock mounting, locking mechanism, and keying. Labor and equipment for install are comparable.

The Bottom Line

Wireless locks deployed across an entire facility are not more cost-effective, easier or faster to deploy than traditional access control in the long run. Wireless locks should be used to augment a total building security system in selected locations where it makes sense, such as minimum-use doors and places where cable can be run only at great expense.

A vice president at an access control provider on the West Coast noted that end user customers are oversold and not properly educated on the deficiencies of wireless lock features and functionality, and the promoted cost savings is not always real. An executive at an access control provider in the Southwest suggested that best practices in the sales process should include providing end users with a detailed explanation of nuances, features, lack of functionality and ongoing operational expenses associated with wireless locks to avoid buyer's remorse when customers realize the locks are not as feature-rich as hardwired access control. Due to customer satisfaction issues with wireless locks, the executive has implemented best practices for educating the customer as a top priority in their selling process. The ideal scenario is a cost effective, solid and feature rich system for the end user.

This is achievable when a well-educated integrator is working with a knowledgeable access control manufacturer and the customer's IT department, so all parties understand the capabilities and shortcomings of all of the different wireless and Wi-Fi locking technologies.

The overall security of an area is dependent several factors in the selection of proper door hardware. These elements consist of the life safety codes, lock mechanism, its failure mode, door contacts, REX devices, frames, handing, closure, and finishes. Many independent constituents may be involved in the specification of the proper hardware for a given situation. The decision-making process is complex and not limited to just Wi-Fi or hardwired solutions.

Eroding revenues

From OEMs to integrators, dealers and installers, there is compression on revenue from the pervasive misconception that wireless locks can offer the same features and functionality of true, traditionally wired access control. Whether the decrease in revenue results from lost panel and component business and/or increased training costs, there is a new dimension in the that OEMs never before had to consider in order to salvage revenue: the challenge of competing with locksmiths to retain some of the revenue being lost due from wireless locks.

An executive at an access control provider in the Southwest stated at in addition to no longer selling as many panels, they now have to learn the lock business and then compete against large wireless lock distributors. The other difficulty, highlighted the executive is being able to participate in the revenue stream wireless locks generate. He added that the lock vendors claim they are not competing with panels, even though in reality they would like to replace controller points with locks and take over hardwired business.

As a result, access control system providers are now in the position where they must weigh the pros of becoming lock VARs to gain lock sales (along with new business maintenance issues) against the cons of losing panel sales. Does it reconcile? A founder with an access control vendor in the Midwest stated that wireless locks are causing a major flux on the business and TCO. It is too early yet to ascertain the true impact, but it will become more clear over the coming years.

***

Jacobs Group Consulting

Jacobs Group Consulting (www.jacobsgroupconsulting.com) is a team of security management professionals dedicated to providing engineered solutions for risk mitigation and asset protection. Bill Jacobs, C.P.P. and Principal Consultant, has over 32 years of experience in security management and holds the unique qualification of having been a client, thus understanding security from an end-user's perspective. He spent 15 years as Cisco System's Director of Physical Security and Integrated Building Technologies. Other direct corporate experiences include managing physical security for Apple Computer, Stratacom, and Borland International. Bill has also worked in the capacity as an Operations Manager for a large System's Integrator and a Security Consultant for another company.