HAGER COMPANIES
Published on Security Today, Digital Edition - June 2017

The Access Control Dilemma - Balancing Security, Convenience and Budget

by Gordon Holmes

Anytime a key is lost, particularly a master or grand master key, the integrity of the system is immediately compromised.

Physical access control has long been a key element of many facilities' security strategies. Noticeably the technology behind access control has continuously evolved, creating solutions that offer more security and convenience than ever before. From magstripe to contactless technologies and mobile credentials, the variety of solutions on the market can make selecting the right platform overwhelming. Choosing an access control system depends on the end user's differing needs and requirements. While there's no one-size-fits-all solution, the goal is to balance security and convenience for each facility, while complying with prevailing building and life safety codes and meeting budget considerations.

When comparing different brands and solutions, it is imperative to find out from the end user's perspective how people will flow through the facility and to which areas these people should have access – and at what time of day.

In order to bridge any potential gaps in the access strategy, architects, distributors and general contractors will all need to be involved to ensure a smooth implementation process.

There are many different features with access control, and the technologies behind the platforms are ever-changing. When selecting the right access control solution for a facility, it is important to look at the evolution of these platforms – from mechanical keys to contactless technologies to the latest and greatest "intelligent" systems available on the market today.

MECHANICAL KEYS

Traditional keys have been used for access control dating back 6,000 years. While this low tech solution might seem obsolete, there are still many advantages to using the traditional mechanical key as part of one's access control strategy. Locks and keys have worked well through the ages; they are easy to install, readily available and offer a simple and relatively secure access control solution.

However, anytime a key is lost, particularly a master or grand master key, the integrity of the system is immediately compromised. Carrying around more than one key is another adverse facet of using the traditional key as an access control solution. Keys can become a workable solution when there is a small number of people and/or doors or when they are used as part of a more comprehensive access control solution.

MAGSTRIPE TECHNOLOGY

Magstripe cards were first developed in the 1960s by International Business Machines (IBM) for U.S. government security purposes after IBM developed a way of adhering the magnetic tape with digital computer data to a plastic card via a hot stamping method. It took a few more years of research and development but IBM's engineering team created a machine that could quickly use the magstripe technology to create ID cards that were then utilized by banks, hospitals and other businesses.

CONTACTLESS ACCESS CONTROL

The 1990s saw the emergence of contactless technologies. Proximity (prox) cards addressed some of the limitations of magstripe technologies. Prior to prox cards, physical contact between the readers and the credentials was required making it cumbersome and inefficient for end users, while demagnetized cards and physical wear on readers became time-consuming and costly for administrators.

The low frequency, 125 kHZ technology of the card allows for the card's data to be detected when presented a few inches from the reader. These contactless cards offer remarkable reliability and longevity. Prox technology relies on radio frequency (RF) signals sent out from the reader. The cards themselves simply consist of an antenna, a capacitor, and a chip that stores the card's unique ID number. When the card is presented to a lock, the reader translates the information from the card into a digital format read by either the lock circuitry itself (in a stand-alone environment) or a host panel/computer that makes the decision to authorize or deny a person's entry. Prox technology can also be incorporated into diverse credential types such as key fobs, bracelets and wristbands, meaning users no longer require a physical card shaped credential.

While prox systems changed the access control industry by ushering in the proliferation of electronic access control due to lower maintenance costs, increased user convenience and new options for credentials, the technology still had its limitations. One of the largest of these is the technology's widely-known security vulnerabilities. While prox systems will keep incidental visitors out, anyone with intent to breach the system can do so relatively easily. The credential is unencrypted, static and can be read in the clear, making it easy to clone or forge a card without the card holder ever knowing. The cloned card can then be used to open any door available to the original holder. There is also no direct means of determining if a system has been compromised, essentially worsening matters by providing a false sense of security. Another limitation is that prox cards cannot be encoded with anything other than the standard unique ID. While this might not seem like a major setback, newer technologies, such as smart cards, are able to store more information than just an ID number, such as a cashless vending debit value or a biometric template.

SMART CARDS & NETWORK LOCKING SOLUTIONS

Smart cards answer all the looming security questions posed by prox cards because they are encrypted. What does encrypted mean? The United States Department of Defense (DoD) approved Advanced Encryption Standards (AES) for smartcard technologies. AES is an encryption algorithm that has become the de facto encryption standard for commercial transactions in the private sector. This means that the cards and the readers talk the same encrypted language that cannot readily be hacked.

Some smart card systems have the capacity to both read and write information to the card at the lock or reader. This provides much better data security while creating greater flexibility for use in various applications. Multiple sectors on the card allow for storage beyond access control, including biometrics and cashless vending.

Smart cards used in some networked system provide flexibility by using smart credentials to transmit data between offline devices and head-end systems. This can be termed "virtual" networks. All user related information is stored on the smart credentials which act as carriers for the network. This eliminates the need to have wired or wireless locks at every secured opening and drastically reduces the overall cost of the access control system. Deciding between a virtual networked or wireless solution (or a combination of the two) will determine how the system is connected and updated. Smart technology can also be incorporated into diverse credential types such as key fobs, bracelets and wristbands, meaning users no long require a physical credit card shaped credential.

In cases where the possibility of immediate lockdown of an entire campus or facility is needed, either hardwired or wireless locks will need to be used. They also allow the user to lockdown an entire building very quickly by cutting access to all cards on the system while still granting emergency responders access.

CONCLUSION

Depending on the size and type of the structure being secured, along with knowing whether immediate lockdown is a prerequisite, will guide in correctly choose the product mix needed to secure a facility, whether it be purely mechanical, mechanical and standalone electronic, virtual networked or wireless/hardwired. Some manufacturers design their products and systems with scalability built in - meaning that as a facility's security needs evolve they can upgrade their locking hardware with minimal aggravation and expense. Leveraging these new technologies provides a unique opportunity for contract hardware distributors, security dealers and installers to assist end users in customizing their access control system.

Gordon Holmes is a product manager covering the commercial hinges, electrified product lines as well as Hager powered by Salto access control line. He can be reached at gholmes@hagerco.com.