SPONSORED CONTENT

CSO FROM IDG

HID

Why Outdated Access Control Systems Are a Big Problem

Migrating to modern physical access control systems eliminates vulnerabilities, adds multi-application capabilities, and paves the way for user-friendly mobile credentials

ACCESS CONTROL FOR BOTH PHYSICAL AND CYBER SYSTEMS is equally mission critical, but many organizations today rely on outdated technology and communication protocols that leave them exposed to potential theft of intellectual property, data breaches, and compliance violations. Security teams can take advantage of key events and circumstances, such as mergers and facilities consolidation, to win support for cost-effective and minimally disruptive physical access systems upgrades.

A recent survey of almost 2,000 members of ASIS International, a global community of security professionals, found that many physical access control systems (PACS) still rely on aging card credential technology. Almost half support low-frequency (125 kHz) proximity cards, and a third support magnetic stripe cards, both of which can be easily cloned.

Older, vulnerable PACS solutions can enable insiders, criminals, and spies to gain access to secure facilities (or parts thereof), where they may then access networked computer systems, physical assets, and/or the personnel being protected.

“It doesn’t take a government-sponsored hacker to break through these legacy physical access control systems,” says Brandon Arcement, senior director of product marketing at HID Global. “The vulnerabilities are not theoretical. Many off-the-shelf devices are available for anyone to subvert outdated systems.”

The problem goes beyond outdated credentials. Physical access control systems are made up of card readers that communicate with a controller via an access control protocol. The most commonly deployed protocol, Wiegand, dates back to the early 1980s; it is unencrypted and vulnerable to interception and cloning. Furthermore, such older systems are difficult and costly to maintain, limited in functionality and distance, and cannot be updated remotely.

A glaring weakness of older-technology PACS involves the use of proprietary software that is bound to specific hardware. This type of vendor lock-in limits an organization's ability to turn to alternative suppliers, which could improve security, reduce costs, and enhance the user experience.

Physical access control doesn't have to be the weak link

Physical security and logical security management have often evolved along separate tracks, but over the past decade some physical access security products have been incorporated into IT networks, and IT has become increasingly ingrained in the procurement, evaluation, and maintenance of physical security products.

Likewise, risk mitigation through the convergence of physical and logical access is rising to the forefront, and technology is delivering the necessary security. Second-generation smart cards such as Seos® are architected to enable virtually unlimited applications and allow organizations to manage the credentials independent of the underlying hardware.

These newer credentials can be used to manage secure identities not only for cards, but on mobile devices, wearables, and other form factors, and to connect via NFC, Bluetooth, and other communication protocols. Mobile devices and wearables are less likely to be left at home or to go unreported for days or weeks when missing, as is often the case with physical cards.

Replacing physical credential management with a digital process enables organizations to respond quickly to security issues, such as deactivating devices and deprovisioning a user's credentials over the air. Similarly, mobile credentials can be issued and updated electronically while eliminating the costs and time lags of reissuing plastic cards.

> "IT DOESN'T TAKE A GOVERNMENT-SPONSORED HACKER TO BREAK THROUGH THESE LEGACY PHYSICAL ACCESS CONTROL SYSTEMS, THE VULNERABILITIES ARE NOT THEORETICAL. MANY OFF-THE-SHELF DEVICES ARE AVAILABLE FOR ANYONE TO SUBVERT OUTDATED SYSTEMS."
>
> — Brandon Arcement
> Senior Director of Product Marketing, HID Global

Seizing on upgrade opportunities

Implementing new, more dynamic access control technologies provides many benefits over maintaining older, more static ones. The business case for an upgrade can be built around three key benefits:

1. **Increased usability and support for mobile credentials now or in the future;**
2. **Operational efficiencies in reducing card management issues, such as massive re-carding;**
3. **Greater security.**

With a solid business case, security teams can seize on specific events and circumstances to implement upgrades:

- IT network or infrastructure upgrades present an opportunity to align physical and logical access systems, practices, and processes by simultaneously implementing a physical access control upgrade that protects investments with increased security and takes advantage of new technology.
- A merger or acquisition provides an opportunity to introduce new technology rather than absorb the cost of integrating two separate legacy systems.

- Implementing a common system standard provides the means to centralize management of secure identity to ensure consistency, greater security, and a more efficient use of resources.
- Facilities consolidation, addition, or relocation often requires massive rebadging, an event that is much simpler to coordinate and manage on a single, centralized standard.

Overcoming challenges

Security teams face a number of challenges when it comes to upgrading PACS without disrupting day-to-day operations. An essential element of any upgrade plan is a complete site survey to determine what is installed where, and what it is meant to protect.

"Often there is a lack of understanding of what's in place today," says Arcement. "A full audit will reveal what is being used in terms of counts, types of devices, and what protocols are being used."

Arcement recommends the following key steps in the migration process:

- Start small with a test lab for a well-defined area, such as one floor or one building, and then expand from there.
- Establish a firm plan on where and how to begin, such as determining that new credentials go first to new employees, or to particular buildings or regions.
- Create a rebadging strategy and process. For global organizations, rebadging can be a huge, complex operation that requires careful coordination and procurement.
- Set firm target dates with management buy-in.

Most organizations have determined that a best practice for upgrades is establishing a standard for a multi-technology credential that supports older and new access systems in order to accelerate transition. However, some organizations may realize reduced costs with a wholescale transition to new single-technology cards and related infrastructure.

No time to hesitate

While many organizations today are aggressively improving their cyber strategies and defenses, physical access controls are often overlooked. Criminals and malicious insiders will always attempt to find the weak link in an organization's security defenses.

Organizations need a platform that is flexible enough to support multiple applications for managing not only physical access to buildings and spaces, but for managing logical access such as computer login. Adding new applications such as time and attendance, secure print management, biometrics, cashless vending, and more, creates opportunities to implement improved credential technology. The freedom to move access control to phones, tablets, wristbands, watches, and other wearables offers choice and convenience to end users.

The emergence of the Open Supervised Device Protocol (OSDP) fills the need for a more secure option that supports centralized management and advanced encryption, protecting the reader-to-controller communication. OSDP allows for interoperability of readers and control modules from different vendors, multi-drop installation, and constant monitoring of wiring to detect attacks.

The sooner an organization begins the transition away from legacy systems and devices, the sooner it can close security gaps. A well-planned transition strategy can reduce organizational resistance and build management support.

THE FREEDOM TO MOVE CREDENTIALS TO PHONES, TABLETS, WEARABLES AND OTHER SMART DEVICES OFFERS CHOICE AND CONVENIENCE TO END USERS.

For more information, go to **hidglobal.com/access-control**

2019-05-06-hid-pacs-outdated-ac-syst-problem-wp-en PLT-04419