ACCESS CONTROL 2019

TRENDS & TECHNOLOGY

Supplement to *Locksmith Ledger International, Security Business, Security Technology Executive*

www.LocksmithLedger.com, www.SecurityInfoWatch.com

New Solutions Emerge as Technology Evolves

July/August 2019

ENDEAVOR BUSINESS MEDIA

FIND EVERYTHING UNDER THE SUN.

SECURITY LOCK DISTRIBUTORS

Helping you do your job...better.

SECLOCK.COM | 800-847-5625

MASTER WHOLESALE DISTRIBUTOR OF ALL ASSA ABLOY PREMIUM DOOR HARDWARE BRANDS

hes ASSA ABLOY · SECURITRON ASSA ABLOY · Adams Rite ASSA ABLOY · ALARM CONTROLS ASSA ABLOY

Request information: www.SecurityInfoWatch.com/10215009

TRINE ACCESS TECHNOLOGY

SPECIALIZED SOLUTIONS
ELECTRIC STRIKE SERIES

THE SMALLEST ELECTRIC STRIKE IN THE WORLD DOES IT AGAIN!

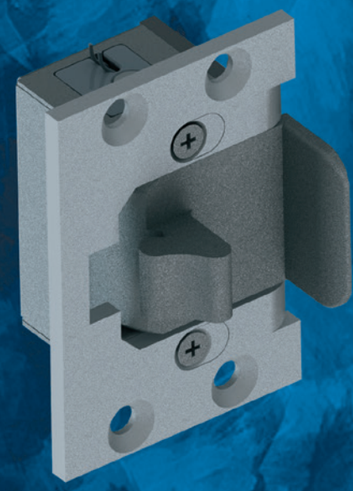
3275VRP-LC

THE BEST SOLUTION

FOR VERTICAL ROD DEVICES

- PATENTED ANCHORING PIN SYSTEM INCLUDED

3250SOM-LC



STRIKE-O-MATIC™

THE ONLY ELECTRIC STRIKE SOLUTION FOR THE DOR-O-MATIC™

- ALUMINUM & DARK BRONZE FACEPLATES INCLUDED

- CUSTOM INSTALLATION TEMPLATE AND SUPPORT PLATE INCLUDED
- BHMA GRADE 1 HEAVY DUTY STAINLESS STEEL MECHANISM
- LC100 PROVIDED

SOLUTIONS ONLY TRINE CAN PROVIDE!

VISIT TRINEONLINE.COM FOR MORE DETAILED INFORMATION

Request information: www.SecurityInfoWatch.com/10215438

ACCESS CONTROL 2019
TRENDS & TECHNOLOGY

COVER STORY

TECH FEATURES

COLUMNS

ADVERTISER'S INDEX

This index is supplied as a service to our readers. The publisher assumes no liability for omissions or errors.

ACCESS CONTROL
TRENDS & TECHNOLOGY 2019

ENDEAVOR BUSINESS MEDIA

1233 Janesville Ave., Fort Atkinson, WI 53538.
Phone: 847-454-2700, Fax: (847) 454-2759 • (847) 454-2700
Access Control –Trends & Technology 2019 is a supplement to *Locksmith Ledger, Security Dealer & Integrator* and *Security Technology Executive magazines.*

PUBLISHER
Group Publisher.....Nancy Levenson-Brokamp
nbrokamp@endeavorb2b.com

EDITORIAL
Editorial Director.....Steve Lasky
Editor, Security Business.....Paul Rothman
Editor, Locksmith Ledger.....Gale Johnson
Editor, SecurityInfoWatch.com.....Joel Griffin

ART & PRODUCTION
Art Director.....Bruce Zedler
Production Manager.....Jane Pothlanski
Audience Development Manager.....Terri Petitt

SALES CONTACTS
Northeast US & Eastern Canada | Janice Welch
800-547-7377 ext. 6288
janice@securityinfowatch.com

Midwest | Brian Lowy
800-547-7377 ext. 2724
brlowy@endeavorb2b.com

Western US & Western Canada | Bobbie Ferraro
310-800-5252
bobbie@securityinfowatch.com

Display/Classified | Kristy Dziukala
800-547-7377 ext. 1324
kdziukala@endeavorb2b.com

SUBSCRIPTIONS CUSTOMER SERVICE
Toll-Free (877) 382-9187; Local (847) 559-7598
Email: Circ.SecDealer@omeda.com

REPRINTS
To purchase article reprints please contact
Brett Petillo at Wright's Media:
877-652-5295 ext. 118
or bpetillo@wrightsmedia.com

ENDEAVOR BUSINESS MEDIA,LLC
Chief Executive Officer | Chris Ferrell
Chief Revenue Officer | Scott Bieda
Chief Operations Officer | Patrick Rains
Chief Technology Officer | Eric Kammerzelt
Corporate Marketing Officer | June Griffin
Vice President, Accounting | Angela Mitchell
Director of Finance | Jessica Klug
EVP/Group Publisher | Amy Mularski
VP, Production Operations | Curt Pordes
General Counsel | Tracy Kane

Who Says Nothing's New?

By Steve Lasky

In a world dizzy with fast-changing security technology; a place that exudes digital muscle and data-driven analytics, is cutting-edge access control even a thing? You best believe it is.

While access control systems have seem staid and conventional the last decade or so compared to flashy video surveillance device innovation and systems powered by analytics and Artificial Intelligence, make no mistake, physical access control technology is in its renaissance.

In the annual *Access Control Trends & Technology* supplement for 2019, the diversity and forward-thinking innovations that are revolutionizing the face of physical access control are presented by those driving that change. The IT-centric systems that have given rise to the wonderous development of IoT on such a massive scale are now dominant in an industry that once viewed bar codes as cutting edge.

Kellen Duke, the Head of Deployments and Security for Proxy, says that moving from physical key cards to electronic key cards is causing a radical shift in the economics of access control. Vendors charging customers per-credential pricing made some sense when credentials were tied to a physical key card. Now that user credentials are 100% software it's possible to create thousands or millions of credentials in seconds and pricing models for access control need to adapt. He adds that customers should be wary of paying for smartphone-based credentials and increasingly should favor pricing models that give them unlimited, free credentials so they can provide access to all their employees, contractors, and visitors without incurring any additional fees.

Angelo Faenza, who is Vice President of Campus Electronic Access Control Solutions for ASSA ABLOY Door Security Solutions writes that as EAC solutions have grown in sophistication, the campus locksmith is no longer the sole gatekeeper for installing and upgrading door locks. Today, access control affects IT departments, facilities managers, campus police, sustainability directors and more. Thanks to advanced technologies, EAC systems can address the needs of these multiple stakeholders and provide a cohesive approach to managing the broad spectrum of projects and components that fall under their purview.

These are just two of the many insights you will be able to read in this special supplement. From cloud-based solutions to emerging biometrics and wireless devices, physical access control is not your father's Wiegand anymore. ■

It's in this current environment that PACS now operate—with functions that are core to risk management and mitigation and focusing on interoperability—using open platforms as a building block to ongoing integration.

Image Courtesy of BigStock.com

The Next Great Phase of Physical Access Control

Interoperability forges a critical connection to IoT devices and peripherals

By Per Björkdahl, Bob Dolan

Proprietary systems, closed operating platforms and integrations that require extensive software reprogramming or modifications are finally falling out of favor in the physical security industry. A new horizon based on network-connected and IP-based products is in sight, with the promise of leveraging billions of devices soon. The digital transformation is here, and an industry that embraces and plans for seamless connectivity will be well-poised to take advantage of this rapidly changing landscape.

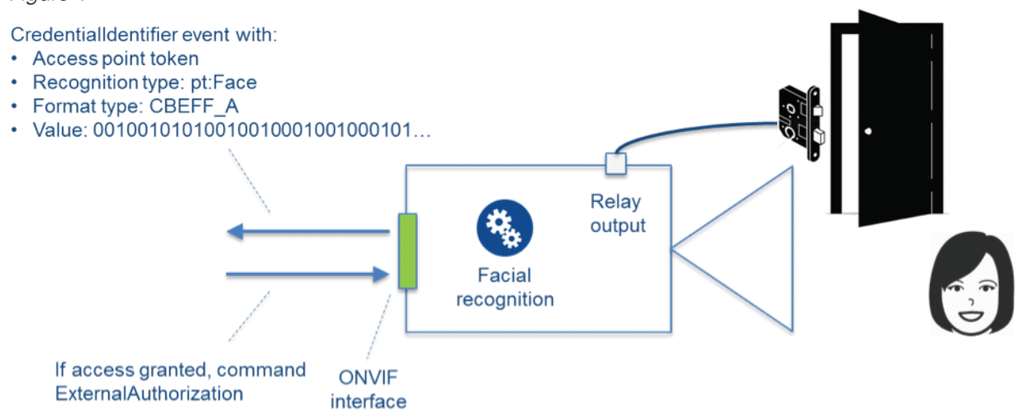
End users are vying for ease of operation and the ability to select and upgrade products without expensive rip-and-replace scenarios, thus forcing siloed systems and proprietary technologies into things of the past. Hardware and software organizations are working together, partnering in technology and implementation. New cybersecurity processes are becoming embedded in security, surveillance and automated processes—from product conception to final commissioning.

Customers want to pick and choose among appropriate technologies—ones that work best for the application and not those simply dictated as a result of the existing infrastructure. They also want to be able to handle every security task they deem critical or essential from their current management system, without costly add-ons.

Today's end users are also demanding convenience and seamless connectivity from device-to-device. They want to know what the system will do, how much it will cost to operate and how it is suited to technology refresh and upgrade strategies. They are well-versed in their risk management profiles and look to select a holistic solution that meets their current and upcoming objectives.

In physical access control systems (PACS), which have advanced rapidly in areas such as the cloud and integrations for video and intrusion, the next logical step is the ability to support emerging devices and peripherals. Open protocols, standards and industry-accepted conformant products that focus on unbridled interoperability between manufacturers and vendors will be critical as advanced technology, such as analytics and ancillary devices, enter the realm of physical security and access control.

Figure 1



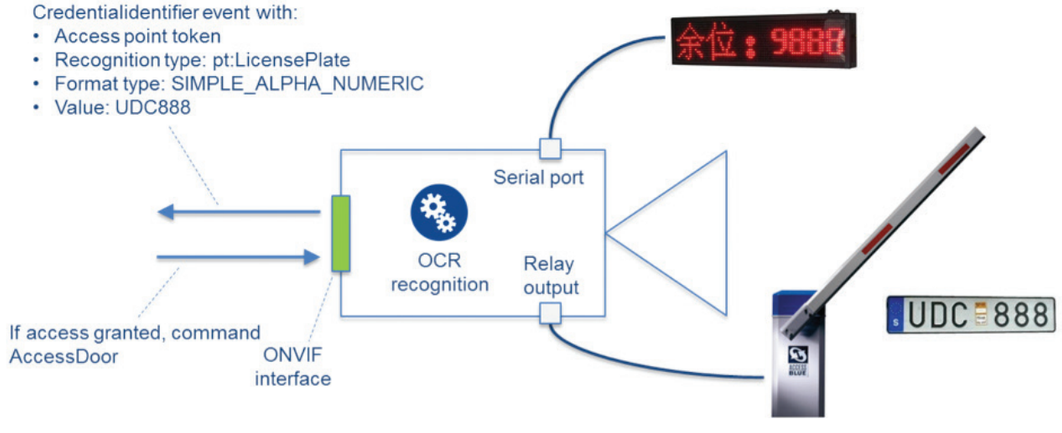
Smart Cities, Buildings and Spaces

According to Statista, a provider of market and consumer data, in 2019, the total installed base of Internet of Things (IoT) connected devices was expected to reach 26 billion; by 2025 the research company projects the number to amount to more than 75 billion worldwide.

Statista defines the IoT as a "vast network of smart objects which work together in collecting data and autonomously performing actions." This network connects people to everyday things in their lives, whether it's their home automation system, video cameras or access control notifications. Now and in the future, the term IoT will encompass a dizzying array of smart objects working together to gather and analyze data and information—and automatically performing the designated actions. Machine to machine (M2M) technology, as well as deep learning and artificial intelligence will further escalate this trend.

IP physical access control is also seeing increased market interest for innovative new identification technology and door control solutions such as license plate recognition; iris, fingerprint and facial recognition; mobile credentials/wireless locks; door interface units and input/output (I/O) and relay

Figure 2



boards that enable and control these and other devices.

It's in this current environment that PACS now operate—with functions that are core to risk management and mitigation and focusing on interoperability—using open platforms as a building block to ongoing integration. A single, unified vision for access control will be the next logical continuum in the move to smart cities, spaces and buildings, fostered by standards, common interface protocols and open systems.

ONVIF is an organization whose mission is to facilitate the standardization of interfaces that enable interoperability between IP-based physical security products. Application and extension of the ONVIF open platform is the next step in the future of IoT functionality as it continues to move in the direction of incorporating ancillary devices, peripherals and exterior technologies from different manufacturers.

The overall mission of ONVIF is to establish a common communication interface for all security devices and clients, across security disciplines, systems and vendors. Standardized interfaces promote and encourage effective interoperability, regardless of brand and with openness to all companies and organizations. ONVIF profiles and conformant products can support one or more of the following Profiles: Profile A for broad access control configuration (credentialing, management); Profile C for basic access control; Profile G for edge storage and retrieval; Profile Q for quick installation; Profile S for streaming video; and Profile T for advanced video streaming.

Currently, ONVIF access control Profile C and Profile A cover an access control unit (ACU) device and an access control management client and allow for the mixing and matching of access control devices and clients within a system. Newer technologies on the periphery require interfaces between these new devices and the ACU or the access control management software, which are not yet covered by existing profiles A, C and S.

The orchestrated and purposeful migration to a new body of work is the cornerstone of the continuing development of IP and network-based systems. This next point of study in PACS from ONVIF would enable additional types of products, such as surveillance cameras, gate controllers and other input systems to do credential identification and interact with various types of management systems from different manufacturers—further driving the adoption of ONVIF interfaces in the PACs and video surveillance space. The new directive will also increase the potential contracting use cases for systems integrators and end-user customers in physical access control through broader solution sets available from manufacturers.

> New cybersecurity processes are becoming embedded in security, surveillance and automated processes–from product conception to final commissioning.

Biometrics/License Plate Recognition

In the example of facial recognition (Figure 1), the example shows an existing video camera with facial recognition capability and a relay output port. The use case is a scenario where an entrance door to a building has a camera that can read facial biometric data and sends the data to a client, possibly unlocking the door if instructed by the client to do so. With the new profile interface, the camera is capable of relaying biometric data to the client where it is authorized. The client then sends back a signal that access is granted or denied.

In the example of license plate recognition technology (LPR) (Figure 2), the LPR subsystem usually includes an auxiliary gate, ground coil and LED display device. The LPR machine is equivalent to the license plate reader. Through the optical character recognition (OCR) function, the vehicle license, brand, color and other attributes are automatically output.

As with the facial recognition example, the interface between the devices and the client does not specifically control the decision. The device simply passes credential information (e.g., card number, license plate number, biometric data, etc.) to a client that can make the access decision.

The interface takes the intelligence from the external device and allows communication of the specific access control device into the system. In the future, it may also be possible for combinations of information, data and decision making from a wide range of devices, not just access control and video.

The widespread and cascading benefits of the ability to integrate new ancillary systems, peripheral devices and remote technologies can have significant impacts throughout the entire security industry.

For users, open devices provide the flexibility to specify optimal products for specific needs without being locked into a certain vendor. Users can integrate control panels and management software from different manufacturers, rather than remain pigeonholed to a technology or solution. In addition, open systems promote lower total cost of ownership and future proofing, with nearly unlimited choices of hardware and software. An ONVIF conformant video management software, for instance, will allow users to integrate ONVIF conformant devices from different hardware manufacturers. With software that supports both ONVIF and proprietary application programming interfaces (APIs), users can choose to use the ONVIF interfaces for certain functionalities and the proprietary API for other features at the same time. Having ONVIF conformant products is like having an insurance policy that protects the end-user's technology investment.

For systems integrators and specifiers, ONVIF conformant products

provide flexible, cost-effective and future-ready systems. Systems integrators can select products from different interoperable vendors while focusing on seamless integration. This also opens a tremendous opportunity to expand its core business into new competencies by giving customers additional value-add solutions.

For manufacturers and software providers, the benefits include the ability to provide greater product innovation and less time to market, as well as easier market acceptance, access to projects and the ability to forge new technology partnerships.

> The overall mission of ONVIF is to establish a common communication interface for all security devices and clients, across security disciplines, systems and vendors.

For software developers, implementing ONVIF specifications instead of various brand-specific interfaces to address basic functionalities can free up time to focus on developing innovative solutions.

Cyber Readiness

While ONVIF does not set security policy, many industry-proven cybersecurity measures can be included in the common interface established by ONVIF. Among these are Certificate Based Client Authentication; Keystores and TLS servers. There are also best practices, such as forcing a default password change or out-of-the-box hardening. ONVIF and other standards groups help ensure and deploy real-time security by including industry-accepted and established cybersecurity measures in profiles and standards.

In addition, the upcoming body of work targets edge devices that do not themselves take the access control decision and therefore do not need to store any sensitive data. The core purpose is to take some credential input, pass it on to an access control unit or management system that evaluates if the credential has the correct permissions and returns the decision to the new device which grants or denies access.

All types of different systems, whether facial recognition, license plate recognition, door stations or other remote devices, can maintain their own communication protocols and manufacturers can integrate conformant products. Ancillary product vendors can grow their products more effectively and access control manufacturers have the ability to control many more devices because they can communicate over a standard protocol.

Smart Spaces

The future is intelligent spaces, with hundreds of different systems, devices, sensors and peripherals working together. Gartner defines smart spaces as physical or digital environments populated by humans and enabled by technology, which are increasingly connected, intelligent and autonomous. Safe/smart city deployments and IoT systems are helping to accelerate the acceptance of interoperability over proprietary systems.

Integration is more effective when it creates a holistic ecosystem based on a common technology platform that can easily and securely add new devices and peripherals. ONVIF is continuing to develop its next level of work in this critical area.

In the future, as part of PACS management, we may see dynamic identity that authenticates the person and not just the credential. To enable a single digital identity that is authenticated across logical and physical environments, security organizations need a combination of digital capabilities including facial recognition, video analytics and IoT sensors.

We can speculate about the future, but ONVIF is preparing for it, working to integrate ancillary systems to access control and video surveillance and embracing new remote technologies and the IoT. ■

About the authors:

Per Björkdahl *is the current Chair of the ONVIF Steering Committee and has been since the fall of 2012. Per is involved with ONVIF's conformance initiatives and represents the member-driven organization as a speaker at trade shows and other technology events and to the media at large. His professional career includes a lifelong commitment to technical convergence with Axis Communications and companies like TAC (now part of Schneider Electric), advocating for the acceptance of communications standards in the building automation industry. Per has worked in the physical security industry for more than 25 years and was an early supporter of IP technology within the industry. Per is currently Axis Communications' Director of Business Development, a position he has held for more than 16 years.*

Bob Dolan *is the Director of Technology for Security Solutions at Anixter. He brings with him over 29 years of sales, management, and technical experience in the physical security industry. After working with end-users and integrators for many years, Bob earned his RCDD (Registered Communication Distribution Designer) certification from BICSI (Building Industry Consulting Standards International) in 2009 and his CPP (Certified Protection Professional) from ASIS in 2012. Bob is also the Vice Chairman of the ONVIF Technical Services Committee.*

Image Courtesy of BigStock.com

3 Surprising Benefits of Access Control

Implementing access control solutions that go beyond security can be a game changer for most organizations

By Angelo Faenza

The primary function of access control solutions has historically been quite literal—controlling access to openings and points of entrance and egress. But today, access control is becoming much more than a door, lock and key. Not only does it involve securing openings in all manner of new technologies, but it also includes optimizing a variety of facility functions. Today, access control is a multi-dimensional ecosystem that can address a full spectrum of operational needs. To demonstrate how this comes to life, let's visit a typical university campus and examine how the evolving nature of access control makes an impact.

Driving Cost Efficiencies

Access control and energy utilization go hand-in-hand thanks to emerging technologies. Lighting systems can be activated by a user swiping their credential to enter a room, and heat and air conditioning can be controlled based on the number of users badged into a room. These integrated functions prevent lights from remaining on in empty rooms or HVAC systems from consuming large amounts of energy at times when classroom buildings aren't in use. Activating operational systems only when they're needed reduces energy usage across an entire facility, and ultimately, costs.

Openings themselves can also be a driver of energy savings, particularly when low-energy electromagnetic locks are installed. For example, ASSA ABLOY's newly released Securitron M380E with EcoMag technology provides an 80 percent reduction in energy consumption over previous models of electromagnetic locks. Utilizing access control products such as the Eco Suite of energy efficient products from ASSA ABLOY Group brands throughout a facility can have a significant impact on energy and cost reduction. Connecting various facility operations with low-voltage or Power over Ethernet (PoE) solutions can also reduce energy usage and overall cost. Further cost savings are possible thanks to the fact that access control solutions can connect to these networks without a campus having to add new infrastructure.

The SARGENT Passport 1000 P1 and P2 locks support multiple credentials and allow seamless migration from the magnetic stripe cards that are widely used today to mobile credentials and higher security smart cards without having to change the locks.

HES K100 cabinet locks with Aperio technology can be used to ensure that only authorized credentials can gain access to secure cabinets.

"By integrating data from event and classroom scheduling systems, a campus can automate its access control system to manage how faculty and students engage with different buildings across campus," says Jason Higley, Managing Partner at Detrios. "For example, using Detrios DAX, an electronic access control (EAC) system can be set to only unlock buildings and rooms during off-hours if there is an event in that space. This provides the added benefits of increased safety and security by restricting access to spaces that aren't scheduled for use, as well as reduced energy consumption by limiting the number of spaces that are considered occupied. At scale, this type of program can drive incredible energy and cost savings."

Access control can also drive cost efficiencies by protecting supplies and equipment. Electronic credentials record who entered certain rooms and when, so access to labs and storage rooms can be monitored. Further, EAC systems can be programmed to only allow certain individuals to enter spaces with sensitive assets. At the campus clinic, for instance, access to medication and supplies storage can be restricted and monitored, helping to reduce diversions or losses of these valuable materials. Server rooms and all types of tech equipment can be secured with access credentials as well, making them less prone to damage or theft.

The wide variety of locks available allows access control systems to secure valuable assets in a range of applications, such as cabinets. For example, HES K100 cabinet locks with Aperio technology can be used to ensure that only authorized credentials can gain access to secure cabinets. With this technology, equipment and other valuable assets can be secured in classrooms, laboratories and any type of educational facility. For example, Berklee College of Music utilizes HES K100 cabinet locks to store and secure audio equipment. According to Nick Costa, Technical Operations Manager at Berklee, since the deployment of the HES K100 cabinet locks there has been zero property loss in areas where the locks were installed.[i]

Additionally, re-keying locks and providing new metal keys can be expensive compared to providing a credential for an EAC system, specifically a student ID card. Reprogramming or replacing these types of cards is typically less costly in terms of both materials and the time it takes facilities staff to make mechanical

upgrades. In addition, students are less likely to lose their student ID card, which is required for almost everything they do on campus.

Streamlining Operations

As EAC solutions have grown in sophistication, the campus locksmith is no longer the sole gatekeeper for installing and upgrading door locks. Today, access control affects IT departments, facilities managers, campus police, sustainability directors and more. Thanks to advanced technologies, EAC systems can address the needs of these multiple stakeholders and provide a cohesive approach to managing the broad spectrum of projects and components that fall under their purview.

> Installing flexible access control systems allows facilities to upgrade as newer solutions become available, such as mobile credentials, while maintaining the same infrastructure.

"Today's access control decision-maker isn't one person, but rather a committee," says Jim Primovic, Director of Sales, Campus EAC for ASSA ABLOY Door Security Solutions. "This group is motivated by the notion that EAC systems can provide new ways of achieving greater safety for students, faculty and staff. For example, campus police can analyze credential data to see who used entrances and exits in dormitory buildings to investigate criminal activity and increase safety."

Access control also streamlines operations by future-proofing a facility, essentially implementing nimble technology that won't need to be replaced in a matter of months or years. For example, universities don't want to invest in electronic cards only to have them become obsolete, particularly given the time and cost associated with making system upgrades across campus.

Installing flexible access control systems allows facilities to upgrade as newer solutions become available, such as mobile credentials, while maintaining the same infrastructure. The SARGENT Passport 1000 P1 and P2 locks support multiple credentials and allow seamless migration from the magnetic stripe cards that are widely used today to mobile credentials and higher security smart cards without having to change the locks. Similarly, the Corbin Russwin Access 700 PWI1 and PIP1 locksets feature a migration path to higher security and mobile credentials. All of these solutions use existing IT infrastructure, including PoE and WiFi, thereby reducing complexity and allowing campuses to easily evolve their access control and security when they're ready.

Improving the User Experience

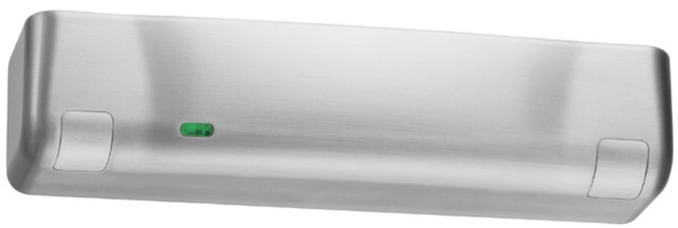
The Internet of Things and the ubiquity of mobile and wireless technologies are changing expectations about how people live and work in any given space. Whether using Wi-Fi while flying across the country or logging onto a hotspot while taking a cab across town, today's on-the-go society expects a seamless, connected experience at all times. Universities are under increasing pressure to meet these expectations, as Gen Z students are the first generation to have had the internet and mobile phones since birth.

With cutting-edge solutions, like mobile and biometric credentials, EAC systems can help meet these changing expectations, as people of all ages have grown accustomed to frictionless movement. For example, access control systems can now sense a credential up to 20 feet away from an opening so that the entry point is already open when the user approaches, all without them having to swipe a card or take the phone out of their pocket.

Over time, biometrics will make for an even more seamless experience, as users' own features, like a fingerprint or retina, become their credentials. In the campus environment, this will be particularly attractive for athletics departments, where student-athletes want a fluid experience from training facilities to locker rooms without having to keep a card or a phone on them.

Further, in today's age of Amazon, package delivery and the issue of package theft has become a growing issue that affects the experience students and faculty have on campus. As a result, cabinets and lockers for secure package delivery are becoming an increasingly valuable solution for campuses as an alternative to having packages left at residence hall entrances where they're at risk of theft or misplacement. Package delivery centers filled with smart lockers that feature touchscreens and keyless access, such as Luxer One package lockers, enable greater security and peace of mind.

"As e-commerce grows and package delivery continues to be the norm, this technology will be a true game-changer," says Tyler Hansen, who leads higher education and university lockers at Luxer One. "This is an example of how thoughtful integration of security and access control technology can improve the experience of people living and working on campus."



ASSA ABLOY's newly released Securitron M380E with EcoMag technology provides an 80 percent reduction in energy consumption over previous models of electromagnetic locks.

Thus, by integrating access control in ways that move beyond only entrances and exits, facilities managers and campus stakeholders can improve the user experience from the perimeter of a university to the innermost lockers in a building on campus.

At the Forefront of What's Next

Technological advancements have transformed access control and the way facilities can use it. It's no longer just about security—access control involves holistic management of a facility's operations.

EAC systems drive cost efficiencies by reducing energy usage indoors and locks and by automating lighting and HVAC systems. They protect valuable assets and reduce costs associated with re-keying locks—all of which improves a facility's bottom line.

By bringing together security staff, IT experts and other stakeholders, state-of-the-art EAC systems streamline operations across large facilities. They achieve not only safety goals, but other facility priorities too, including staying ahead of inevitable technological changes. And, access control can revolutionize the user experience, particularly as people everywhere expect a more seamless, connected experience at work, school and throughout their daily lives.

Implementing access control solutions that go beyond security doesn't have to be a daunting process. With the right partners and solutions, the best EAC systems can deliver more value and better outcomes for users, decision-makers and the integrators at the center of it all. ■

About the author:

Angelo Faenza is Vice President of Campus Electronic Access Control Solutions for ASSA ABLOY Door Security Solutions, as well as General Manager for PERSONA. Angelo has spent 27 years in sales and sales management roles with various divisions across ASSA ABLOY Group brands, in both the traditional mechanical door and hardware space, as well as the software and electronic access control space. Angelo is a member of several industry forums and working groups and was part of the founding team for the Open Security Exchange. He is also an active member of numerous higher education groups and participates in and presents often to industry groups.

TOTAL COST OF OWNERSHIP

How to Assess True Cost Differences of Various Security Entrances

When you are looking at the costs of any product or solution, it is not enough to look at the price tag on what you're purchasing. There are also intangible costs and other factors that have an impact on the bottom line.

Image Courtesy of BigStock.com

When you consider security entrances or access control it pays to look at the full picture of what your costs will be

By Mark Perkins

In planning a comprehensive security program, every choice you make has consequences. Because budgets are never unlimited, costs need to be balanced carefully against needs to make sure you are properly protected against risk, threats and liability.

When you are looking at the costs of any product or solution, it is not enough to look at the price tag on what you're purchasing. There are also intangible costs and other factors that have an impact on the bottom line. For example, in addition to capital expenditures, you need to factor in annual operating costs and any additional staff or other resources you will have to deploy along with your new product. Only when you understand the full value of each product or solution you are considering, will you have a complete picture of what it will cost your organization.

This is certainly true for security entrances. Security entrances are a smart choice to provide both the entry and the access control for a campus or facility. However, when it comes to controlling access, there are many different types of needs and differing levels of security depending on the location and function of the entry. There's also a wide range of security entrances; some are more budget friendly, others more attractive architecturally and some offer greater levels of control.

4 Levels of Security that Impact the Bottom Line

When considering security entrances as part of your security plan, the first step is to learn about the different levels of security they provide in terms of mitigating intrusion. Essentially, they protect a facility at four levels, all of which relate to the number of people who can enter at once: crowd control, deter, detect, and finally, detect and prevent. These levels ultimately have an impact on the bottom line, which we will discuss later in this article.

Level 1: Crowd Control – Crowd control simply limits the number of individuals who can enter at any one time. Waist-high tripod turnstiles, for example, only allow one person to enter at a time; however, it is possible for someone to climb or jump over the turnstile to enter. They do not have any sensors or alarms to detect and alert staff when intrusion attempts happen. They are typically used in locations that are less secure, or which are well-manned by individuals checking the identification of each person trying to enter.

The next three levels – deter, detect, and detect and prevent – relate to the issue of tailgating, or a second person entering on the same ID verification as another person. Some security entrances can deter tailgating, some detect when it does happen, and others actually go as far as to prevent it from happening in the first place.

Level 2: Deterrence — A full height turnstile, due to its height of over 7 feet, is designed to deter intrusion attempts. Its basic construction and robust design make it a favorite of exterior, fence line applications. Its working principle allows one person at a time to enter on a valid authorization. While it cannot be jumped over, a full height turnstile does not have any sensors to detect the presence of people or objects: this means that two determined (and relatively slender) individuals could go through together in the space designed for a single person (otherwise known as "piggybacking"). Therefore, full height turnstiles are usually the first layer of defense, relegated to the fence line with video cameras. If they are installed inside a building, supervision by security staff is strongly recommended due to the possibility of piggybacking.

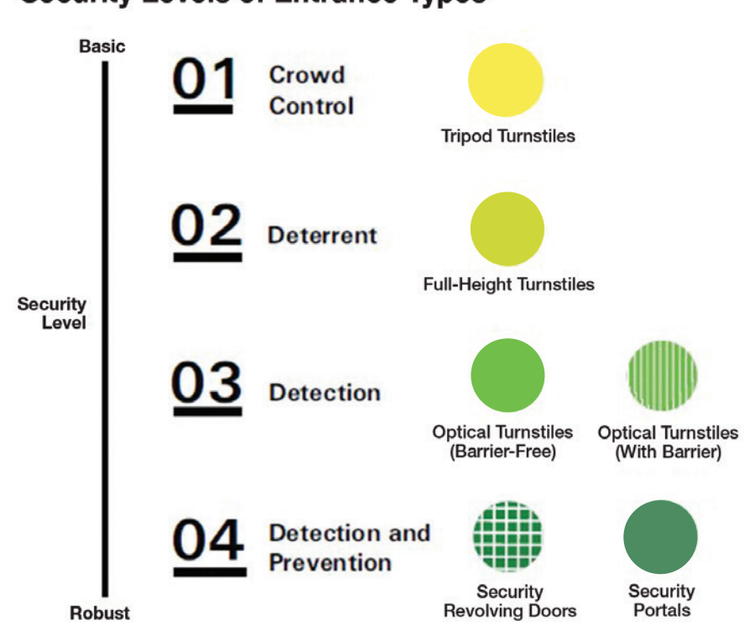


Figure 1: The 4 Levels of Security for Security Entrances

Level 3: Detection — The next level, detection, is represented by optical turnstiles, which provide a meaningful difference beyond deterrence. These entrances are always intended to be used inside, typically in a lobby for allowing employees and registered visitors to enter. They include sophisticated sensor technology that enable them to detect when someone passes through the entrance, along with how many individuals move through on a single authorization. When someone tailgates behind an authorized user, the turnstile issues an audible alarm to alert security staff to intervene quickly. Since optical turnstiles cannot prevent someone from tailgating, it is strongly recommended that security staff be present at all times. This has a great impact on the true cost of this solution year-over-year.

Level 4: Detection and Prevention — Finally, the highest level of security entrances, which can detect and also prevent tailgating and piggybacking completely, includes security revolving doors and mantrap portals. Because they are so good at identifying an intruder and rebuffing them, these types of sophisticated doors do not require any supervision. This potentially creates a rapid return on investment.

Now that we have reviewed the four levels of security that are provided by security entrances, you can see the breakdown in *Figure 1* above:

Examining the True Cost Differences

When it comes to looking at the *cost differences* between these four levels of security entrances, it is essential to compare and consider all the associated costs that you will incur when each type is installed and beyond. As stated earlier, in each of the first three security levels you will likely need to hire security personnel in order to prevent tailgating or other unauthorized intrusions from happening (the

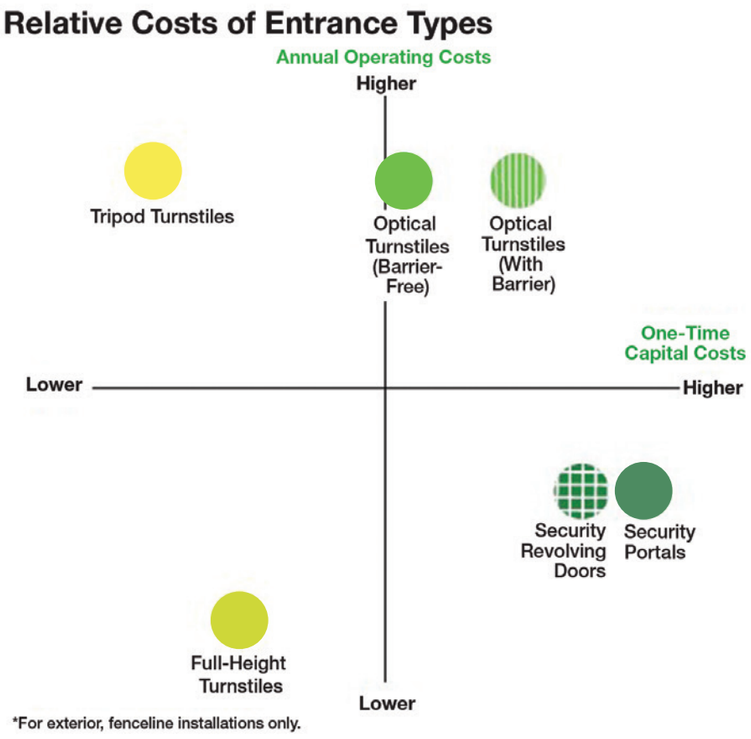


Figure 2: The Relative Costs of Security Entrances by Capital Expenditure vs. Annual Operating Costs

one exception are full height turnstiles deployed outside at the fence line).

Understanding the need for officers to be deployed in conjunction with security entrances helps to clarify the full cost of your choice of security entrance or other solution. Beyond the capital expenditure for the purchase, the installation, and initial training for administrators and users, you will be responsible for the ongoing operating costs. These include not only maintenance, repairs, and electricity, but also the need for guard supervision in order to truly prevent intrusion.

Take a look at this matrix below and you can see how the different types of entrances compare for capital expenditures vs. ongoing expenses. There is quite a difference! If you look at the "x" axis, one-time capital costs increase from left to right. You can see that tripod turnstiles and full height turnstiles, per unit, cost a lot less up front than optical turnstiles, security revolving doors and mantrap portals. See Figure 2.

Then look at the "y" axis, which is expressing the annual operating costs, and you'll see something interesting: the less expensive tripod turnstiles and also the optical turnstiles cost quite a bit more per year than the security doors (shown in the bottom right quadrant)! The full height turnstiles are assumed to be outdoors on a fence line with no guards; if they were used indoors, they would need a guard and would be represented to the right of tripod turnstiles in the top left quadrant.

The Upfront Costs Can be Deceiving

Ultimately, it can often be more cost-effective to install an entrance that does not require the ongoing presence of a guard to prevent unauthorized entry or tailgating. For example, if you have a data center where it is critical to limit entry to only those with the highest authorities, it makes sense to choose a security revolving door or mantrap portal for that location. While these products may have a higher initial price than a standard access control reader and maglock or turnstile, at the end of the year your total costs for that entry will be lower than if you had to hire an officer to staff that entrance full-time.

It is also important to be aware that while security guards do increase the level of deterrence and security at an entrance, they are by no means infallible. "Social engineering" is the term used to describe the variety of clever ruses used by criminals to get past even the most diligent guard. These scams are astounding in their variety and inventiveness and demonstrate that there is virtually no guarded entry that cannot be breached by a determined (and skillful) criminal.

When you are considering security entrances, or access control in general, it pays to look at the full picture of what your costs will be. Working with a responsible and knowledgeable integrator or manufacturer will help you take a deep dive into these details and many more to make the best choice for your organization. ■

About the author:

Mark Perkins, Vice President of Enterprise Security Accounts has over 25 years of sales and operations experience in the automatic door and physical security industries, including work with Stanley Access Technologies, Automatic Systems, and now over 15 years' experience at Boon Edam. Mark is currently leading business development initiatives across the USA and Canada, and assisting the Boon Edam U.S. operations in managing its global account customer base. He is known for his entrepreneurial spirit, having lead multiple startup companies, and has several patent's to his credit.

Biometrics Define the New Frontier of Access Control

Security managers are looking to improve security and increase convenience

By Consuelo Bangs

Innovative technologies and techniques in the field of identity management are enabling change in the world of traditional security and facilitating the migration from physical credentials (access control proximity cards and smart cards) to digital, electronic ones. Threats, unlike any previously imagined have become real and commonplace; from cloned credentials to compromises of underlying communications between traditional security components. To meet these threats requires the ability to secure and confirm one's identity for authorization of access rights, to transmit that identity securely and quickly, all the while ensuring privacy and trust.

Innovators are creating new

business opportunities along with new technical and ethical challenges while strengthening the traditional modes of security. System architects require an even greater knowledge of information systems on top of a foundation in physical security to deploy trustworthy software and hardware components.

Security managers are looking to improve security and increase convenience. They are seeking ways to grow employee satisfaction by transforming the process of entry into a frictionless experience, while asserting stronger

> Biometrics is the use of one's own unique physical or behavioral characteristics for identification and authentication

authentication which prevents identity misuse. With regulations getting stricter for data centers, bank vaults, and other high value areas, biometrics are becoming a must for two-and three-factor authentication scenarios. In recognition of the low costs and risk of duplication, the traditional card and pin do not hold up for the security requirements needed by today's customer.

Physical security is becoming not only a general facilities concern, but more fundamentally an Information Technology (IT) concern. Protection of company assets is impossible without considering their value in an IT infrastructure, beyond the level network security with firewalls and anti-virus applications. Preventing access to physical machines and networking using biometric credentials is in keeping with a broader industry trend to phase out easily compromised techniques such as passwords and pins. Traditional access control systems permit physical access to premises based on the receipt of a recognized card number and allow logical access to a network or application based on the receipt of a recognized username and password. The person is not identified, but rather the card, username, and password are recognized. Adding biometric identification gives security managers certainty that the individual is physically present and that the credential cannot be shared or cloned.

Security no longer involves simply physical access; it now must embrace digital access and the authorization to execute transactions and services using personal devices. Examples include leveraging biometrics built into mobile devices such as a mobile phones and electronic wearables to provide real-time requests for authorization to complete transactions, access systems, or to move data. Electronic objects and networks which may be connected and accessed using personal electronics include:

- The onboard computer system in vehicles, such as automobiles and scooters
- Medical devices, both external and inside the body
- Financial accounts, payment systems, and healthcare systems
- Entertainment platforms, such as video games and television
- Exercise equipment
- Luggage tracking
- Home appliances and HVAC Systems
- Access control door readers with Bluetooth technology

In the world of digital security these are all considered "connected objects." Biometric solutions play a mission critical role in the new world of "connected objects" to provide verification and trust (certainty) of an individual's identity for frictionless, secure physical and digital access. Biometrics provides assurance that only an authorized individual can access their "connected objects." This provides peace of mind, guaranteeing that a bad actor can't take control of a vehicle's onboard computer, a loved one's medical device, or access a secure area or network in the workplace.

Biometrics Defined

Biometrics is the use of one's own unique physical or behavioral characteristics for identification and authentication. Where you go, your biometrics goes. Biometric technology includes a capture device whether it be a camera, an optical sensor (contact or contactless), a keyboard or a microphone to acquire an individual's raw physical characteristic (raw data). This data is then converted into a reference template, a digital representation typically using mathematical algorithms that are patented and proprietary.

Biometric characteristics include face, iris, palm, fingerprint, finger vein, voice, gait, and keystroke patterns. Unlike passwords, biometrics are the only method that establishes a definitive link between our physical and digital identities. The biometric identifier, the reference template, may be a string of numbers or a random number. Biometrics verify and identify a person for the access control system to determine the rights or privileges (access, services, etc.) assigned to that individual.

Biometrics Used in Advanced Access Control Systems

We need our biometric identity to travel with us seamlessly in the physical and digital world; we require our identity protected, secured and available when and where we need it. Critical to the protection and securitization of one's biometric identity is the assurance that it cannot be stolen, cloned, corrupted and it remains under one's control. The biometric identity owner determines when, where, and how it may be used. An interesting way to accomplish this is using innovative technology that employs one biometric technology, such as facial recognition on a personal device, to decrypt an electronic container to release a second stored biometric technology such as iris or fingerprint for live matching to the biometric owner.

Critical to providing security is a public key infrastructure (PKI). PKI technology provides the mechanisms for mutual authentication between "connected objects," such as personal

digital devices, the onboard computer of your car, etc. PKI technology also provides the ability to encrypt the communication channel between digital objects, an internal network and access to cloud technologies.

Authorization for access must include biometric authentication of the individual initiating the request for access, the digital transaction. PKI only provides half the security needed to protect the IT infrastructure. It provides securitization of the communication channel and mutual authentication between digital objects or networks. But PKI is unable to authenticate the individual human initiating the connection to the digital device or "connected object." This could provide the means for an unauthorized individual to gain access into the digital or virtual workplace.

> We need our biometric identity to travel with us seamlessly in the physical and digital world

Critically important to system integrators who specialize in the installation and maintenance of access control systems is the understanding and education of their personnel in how to properly implement existing security features to secure the access control system itself and its network communication. This includes but is not limited to:

- Working with the customer's IT department to assign certificates (PKI) for mutual authentication between the host of the access control software and the access control panels that manage the door.
- Configuring the biometric devices and all elements of the system that communicate on the network to connect to backend software wirelessly or using a wired network executing TLS 1.2 security.
- Enforcing password rules and role assignments to prevent unauthorized access to the access control management software.
- Disabling any existing default username and password accounts once the system had been tested and accepted.

Managing Complex Security Environments

Security professionals are often challenged trying to effectively manage security operations where there are multiple physical access control systems, different biometrics systems, and multiple trusted sources. Reconciling these issues in order to have a robust security ecosystem is becoming easier with standards by organizations like the Physical Security Interoperability Alliance (PSIA).

In a typical enterprise organization, an employee is on-boarded their identity documents required for employment eligibility are stored electronically and may be associated with some form of biometrics. This is normally managed by a human resource system or identity management system. As part of the on-boarding process the employee is enrolled in a local access control system, a logical access system such as Active Directory, and assigned access rights and privileges to buildings, networks, and applications. When mergers and acquisitions take place, large companies must manage multiple access control systems. As employees travel to different office locations, redundant data entry, enrollment, into the local access control system and/or logical access system takes place. This can result in a second credential based on different card technology which may be assigned a different domain and username to access the physical and network access issued to the employee.

The PSIA has defined its Physical Logical Access Interoperability (PLAI) specification which addresses this problem by normalizing identity data and allowing the transfer of an individual's assigned credentials across disparate access control platforms. There are two components to PLAI, an Agent and an Adapter. The PLAI Agent interfaces with the HR system or Identity Management System where the employee was first on-boarded and assigned an identity in the Active Directory and a membership in a network domain.

The second component is the PLAI Adapter, which interfaces with the Agent and a specific access control system or biometrics system. For example, if a large enterprise organization has four different physical access control systems (PACS), each would have a PLAI Adapter, which would normalize the identity data. It would then send it to the Agent, allowing it to share across the security ecosystem. One trusted source to provide the identity data is an important feature, allowing a much more robust security infrastructure. ■

About the author:

Consuelo Bangs, Senior Program Manager, IDEMIA Identity & Security USA, LLC. Consuelo Bangs brings over 40 years' operational and management work experience: 20 years as a program manager, project manager, implementation specialist and business development specialist of biometric access control solutions; eleven years as project manager and consultant for process improvement and work re-design; and thirteen years in education. Currently she coordinates the requirements definition of IDEMIA access control products with engineering to meet commercial and government customer requirements, provides pre-sales and after sale support of customized projects. She holds a Bachelor of Science from the University of Virginia, a Master of Science Degree from The George Washington University and held an IEEE Certified Biometrics Professional certificate.

Access control solutions have also moved to the cloud which has brought added convenience and reduced infrastructure cost.
Image Courtesy of BigStock.com

Strategies in Wire-free Access Control and Unique Functionalities

Many companies can leverage an access control system to optimize their business, improve operations and save money.

By Steve Burk

Manufacturers across the security marketplace have made great progress over the last couple of decades incorporating increasingly innovative IP technology into electronic locks and access control management systems. This has resulted in solutions that are easier to use, more scalable, more affordable, and extend beyond physical security to improve overall operations.

Trending in Access Control: Mobile & Cloud Solutions

The use of mobile phones has steadily increased and it's not just Millennials relying on mobile technology. As the smartphone has gained popularity, so have mobile access control applications. In fact, it's essential for any access control manufacturer to offer either a mobile key application, an integration that serves the same purpose – or both.

Mobile keys have gained popularity in a variety of verticals, especially hospitality, education, coworking, and multifamily housing. Mobile keys are popular because users can quickly be added or deleted and are more secure than mechanical keys because a mobile key cannot be duplicated. As part of an overall electronic locking solution, mobile keys can eliminate the hassle and enormous costs associated with mechanical key loss and replacement.

End users want the power to use their smartphone to bypass the front desk when checking into a hotel room or to come and go at work or an apartment building. It only makes sense to incorporate a device that an end user relies on throughout the day into any physical security solution they would use at work or home.

Access control solutions have also moved to the cloud which has brought added convenience and reduced infrastructure cost. Cloud access control solutions can be implemented with no software installation or the added expense of a fully wired electronic product. In some solutions, all that is needed is an online device with an internet connection. Cloud access

control solutions typically offer end users better functionality and performance, scalability, reduce costs, and almost eliminate the need for maintenance.

One of the top markets for cloud access control solutions is coworking. Mechanical keys make it extremely hard to effectively operate in this vertical. Coworking spaces have so many varying needs to address – providing access to common areas, private offices, public events, late-night or early-morning hours, and numerous users with schedules that typically vary by the day, week, or month.

With a cloud-based access control management solution, coworking administrators can grant access on a regular – even hourly – basis and can quickly add or delete users from anywhere via an online management platform. This not only allows for more efficient operations but also enables management to track and monitor room usage and enables them to optimize occupancy.

Of course, in today's world, security is always top of mind. Any access control provider worth considering should incorporate the latest cybersecurity protections into a mobile or cloud solution, including the latest in encryption technology as well as rigorous certifications and adherence to international standards including ISO 27001.

But, How Much Will It Cost?

With today's leaner workforce - including both security and IT departments - it's important that critical access control operations can be easily managed and maintained without the need for specialized highly technical support. Deploying highly flexible, simplified electronic access control provides the opportunity to extend centralized management and control features to applications that traditionally were otherwise limited to mechanical key solutions. The best news is that with these advances in technology, electronic access control has been shown to return significant ROI when compared to the costs of operating mechanical keys.

A cloud-based access control system, for example, requires little to no infrastructure. All that is needed is an internet connection and a battery-powered lock (that can typically be installed on an existing door in just minutes). This means that a modern access control solution is available to almost any-sized business.

Even large enterprise businesses can migrate to IP-based access control for a fraction of what it used to cost. Hybrid solutions are available that combine the best of wired and wire-free systems. Instead of incurring the cost of wiring every door, class-leading data-on-card read/write credential systems allow for updating access rights at key entrance points that are often placed somewhere in the building where all users must pass (an entrance door, a security gate, an elevator, etc.).

When the user subsequently presents their credential to an interior door, even though it's a stand-alone electronic lock, the credential, and the lock communicate with each other sharing the most up-to-date access information including any "blacklist" users who should no longer be allowed access. These systems can operate even during a power or network outage, ensuring secure access in any scenario.

This can represent considerable savings for a building with interior doors as it means less expensive installations for those doors. If you consider the typical building, there are significantly more interior doors than exterior door thus the savings can accumulate quickly.

Interestingly, electronic access control has expanded well beyond just doors. Advances in electronic cylinders have made the same technology available to control access to lockers, drawers, and cabinets which can all be incorporated into an electronic access control system that's managed by a single platform.

Benefits Beyond Physical Security

In addition to security, electronic access control also provides another valuable benefit: information. Management teams are always looking for data that can help them make informed decisions. The business intelligence available in a modern access control management solution can provide insight into employee behavior, property usage, room usage, high traffic times, high traffic areas, space optimization, and much more.

Additionally, good access control solutions can help companies lower their carbon footprint and save energy. Let's consider hotels. Energy usage in hotels is one of the highest operating expenses they incur. A great deal of energy in hotels is wasted by heating and cooling empty guest rooms. A modern access control solution integrates into existing guest room systems (HVAC, electric, etc) and enables hotels to conserve energy by activating or deactivating those systems when the room is occupied or empty. By knowing when a guest is not in a room, a hotel can save a tremendous amount of money – in some cases 25-40 percent on energy costs.

Electronic Access Control Can Improve Your Security and Your Business

Recent advances in electronic access control have been impressive and have fully leveraged the use of smartphones and cloud technology. Innovators throughout the industry continue to improve upon the technology and functionality in both electronic locking hardware, software, and management systems. With these advances, most companies can leverage an access control system to optimize their business, improve operations, provide a better user experience, and save money.

About the author:

Steve Burk leads the marketing team that drives the continued growth and expansion of SALTO's electronic access control hardware and software security products across North America. With more than 25 years as a sales and marketing leader, Steve prides himself on understanding the customer's journey and finding ways to help customers improve their businesses.

Mobile access technology enables other use cases that aren't possible with today's keycards.
Image Courtesy of iStock

Smartphone Access

Is Accelerating the Transition Away from Cards and Fobs

Mobile access technology enables other use cases that aren't possible with today's keycards

By Kellen Duke

When you enter the lobby of the recently opened Salesforce Tower in San Francisco, the tallest building west of the Mississippi River, things look a little different from the typical commercial property. Tenants and visitors breeze through the turnstiles, swiping smartphones to gain access. At elevator dispatches, people tap their phones to call an elevator to their floor. And upstairs, people seamlessly access secure doors using their mobile devices. If this scene is any indication, it's time to plan for the advancing tide of smartphone access technologies.

What's Driving Smartphone Access Adoption

The iPhone was released 12 years ago this summer and Bluetooth-enabled phones have been around even longer. But it's only recently that this technology has matured enough to use in mission-critical physical security applications. Today, the technology is ready, and adoption is accelerating due to the confluence of three interconnected trends.

First, enterprises and property owners are looking to make access control easier to manage. The average company loses 2.6 cards/fobs for every 10 employees every year. For larger organizations, replacing thousands of cards each year creates an enormous amount of manual work removing the old cards from the access system, adding the new cards to the system, and physically delivering the cards to employees all over the world. Moving to mobile access significantly reduces the manual effort of security personnel to respond to a loss incident. Employees are also far less likely to lose their phone, which they own, and report the loss sooner and that reduces the risk of someone gaining access with a stolen phone.

Another key driver of smartphone access is that it offers a better end user experience. One of the primary complaints office workers have about access cards (45.4% of people surveyed) is that you always must carry it with you. Put another way, people are more likely to leave their card at their desk than their smartphone. Another common end user complaint is that they need to carry more than one card because their landlord's access system doesn't interoperate with their company's system, or because they visit multiple office locations that use different access technology. Mobile access consolidates multiple cards into an electronic wallet that lives on the device so there's no reason to fumble with multiple plastic cards again.

Because access cards live electronically on the device, it's no longer necessary to physically deliver a card or badge to someone to give them access. That can have a big impact on the experience of visitors to the office. Previously, visitors have had to wait in line at the security desk in the lobby to sign in and receive a temporary badge or QR code to go upstairs. Now, hosts can send their visitors a temporary access card directly to their phone. When the visitor arrives, they simply tap their phone to access the turnstile and meet their host upstairs on their floor. These access cards expire after a specific amount of time and can provide only the access the visitor needs--say, to go from the curb to the 37th floor one time but nowhere else.

> Another key driver of smartphone access is that it offers a better end user experience.

Finally, and this shouldn't come as too much of a surprise, the encryption and tokenization capabilities of software running on the supercomputers people carry in their pockets trumps RFID cards. Many card formats can be easily cloned and others that are more secure are cost prohibitive, especially when you consider how frequently employees lose cards. Smartphone access technology makes it more challenging to execute a replay attack to gain access. And the technology opens novel new security options like biometric authentication using the facial recognition or fingerprint recognition technology on many smartphones today that can ensure the user holding the device is in fact the person who has access to the building.

Beyond the Door: Other Common Use Cases

Mobile access technology enables other use cases that aren't possible with today's keycards. One of the most exciting new applications of the technology is automated tailgating technology. It works by sensing the signal of authorized devices passing through secured doors, even if the user forgets to swipe their phone by the reader when following someone through the door. If the number of people passing through the door--as measured by an automated people counter--is higher than the number of signals, an alert can be triggered and sent to the security team to follow up using the company's incident response process.

Mobile access also opens new possibilities that go beyond access control. Consider the potential to integrate this technology into your calendar system for booking meeting rooms. If no one shows up to a meeting on the calendar for 10 minutes, the system can automatically remove the hold on the room and open it up for someone else to book during that time. Or if the room isn't booked and people jump inside for a quick meeting, it can sense their signals and automatically book the room, so others know it's not available. This is just the start of many exciting new use cases that range from quickly accounting for workers during an emergency to providing real estate teams with occupancy analytics for making the most of office floor plans.

Keys to Making a Mobile Access Project Successful

Smartphone access technology has been around for several years and some organizations that were early adopters of the technology found it difficult to make it work for them. Early attempts at smartphone access proved unreliable in the field, which is a showstopper for a critical function like access. Another issue with early attempts was that they sometimes required the customer to replace

their control panels or access control software. That's a deal breaker for many organizations due to the significant investments they have in these technologies, along with workflows they have built on top of them and integrations between these technologies and other systems. For example, controllers often interface with other building systems beyond electronic locks.

To make full use of smartphone access and its possibilities for smart building use cases, the technology must be able to integrate to other systems in an intelligent API-driven way. With a set of open and documented APIs, a customer or integrator can build any integration they want to other systems, whether other access technologies, conference room software, visitor management, emergency response software, or anything else the customer can imagine. Open APIs also ensure that the technology does not lock you into a proprietary ecosystem and is future proof for use cases or technology integrations you may not be able to foresee today.

Lastly, moving from physical key cards to electronic key cards is causing a radical shift in the economics of access control. Vendors charging customers per-credential pricing made some sense when credentials were tied to a physical key card. Now that user credentials are 100% software it's possible to create thousands or millions of credentials in seconds and pricing models for access control need to adapt. What that means is that customers should be wary of paying for smartphone-based credentials and increasingly should favor pricing models that give them unlimited, free credentials so they can provide access to all their employees, contractors, and visitors without incurring any additional fees. ■

About the author:

Kellen Duke is the Head of Deployments and Security with Proxy. Before Proxy, Kellen worked on the Global Security teams for both Uber and WeWork. Prior to his work in the private sector, Kellen managed security programs for Sandia National Laboratories and United States Investigative Services. Kellen is a certified Crisis Negotiator and CPR/First Aid instructor and has a degree from Saginaw Valley State University.

Just last month, the vpnMentor's research group's team of hacktivists discovered the network of The Pyramid Hotel group, which included Marriot and several of top hotel brands across the country had been penetrated.
Image Courtesy of BigStock.com

Physical security at risk as cyberattacks target vulnerable systems

Hackers penetrate the network of The Pyramid Hotel group compromising the door access control systems

By Steve Lasky

Much like the daily government outrage or presidential tweet, ubiquitous cyber-system breaches have become mind-numbing in their frequency, rendering them almost invisible in their urgency. While the prime-time breaches like those at Equifax, Target and Sony Pictures tend to grab the headlines and reveal the seemingly endless vulnerabilities of traditional IT network systems, there are also a growing number of insidious attacks that are now creating huge implications with regards to the vulnerabilities of network-centric physical security systems.

Just last month, the vpnMentor's research group's team of hacktivists discovered the network of The Pyramid Hotel group, which included Marriott and several other top hotel brands across the country, had been penetrated. The Pyramid Hotel Group utilizes Wazuh – an open source intrusion detection system that was on an unsecured server. The hack revealed a cybersecurity leak that included information regarding their operating systems, security policies, internal

John Carter, co-founder and CTO of ReconaSense,

networks, and application logs and, at the same time, left the door wide open on vulnerabilities in the giant hotel brand's network that could enable cyber criminals to launch massive future attacks.

The data leaks included all sensitive information that we've come to expect from such an attack:

- Server API key and password
- Device names
- IP addresses of incoming connections to the system and geolocation
- Firewall and open ports information
- Malware alerts
- Restricted applications
- Login attempts
- Brute force attack detection
- Local computer name and addresses, including alerts of which of them has no antivirus installed
- Virus and Malware detected on various machines
- Application errors
- Server names and OS details
- Information identifying cybersecurity policies
- Employees' full names and usernames
- Other telling security data

Expanding Threats, New Risks

However, what makes this attack most concerning to those in charge of physical access control systems – especially those charged with securing hotel and resort facilities – the information reaped from the hotels' databases allows any would-be attacker the ability to monitor the hotel networks and, according to the vpnMentor team: "gather valuable information about administrators and other users, and build an attack vector targeting the weakest links in the security chain. It also enables the attacker to see what the security team sees, learn from their attempts based on the alerts raised by the systems, and adjust their attacks accordingly."

The White Hat hackers added that, "It's as if the nefarious individuals have their own camera looking in on the company's security office." They said that in a worst case scenario the leak not only put the hotel networks at risk, but also endangered the physical security of hotel guests and other patrons since bad actors could now potentially compromise multiple devices that control hotel locking mechanisms, electronic in-room safes along with other physical security devices tied to the networks.

After the news of this chilling hotel data breach broke in Forbes magazine, John Carter, co-founder and CTO of ReconaSense, a provider of physical security intelligence and next-gen risk-adaptive access control that offers the industry an advanced security and risk intelligence platform that incorporates artificial intelligence (AI) on an artificial neural network (ANN), admits that despite physical security risks that threaten lives and sensitive data, too many organizations still keep physical security data isolated from infosecurity data. In many cases, a physical wall literally separates a Network Operation Center (NOC) and physical security teams from sharing intelligence.

"Attackers who gain physical access to a computer can further invade and wreak havoc across multiple connected IT systems - and vice versa. In this latest hotel systems breach, cybersecurity flaws expose critical IT data as well as physical security systems such as key cards, video cameras, motion detectors, and other devices that ensure guest and employee safety. AI-powered solutions can detect anomalies and identify threats across an entire security infrastructure (IT and physical) before a breach occurs, enabling teams to go beyond managing siloed data and alerts to achieving true situational awareness and rapid response capabilities," says Carter.

" They said that in a worst case scenario the leak not only put the hotel networks at risk, but also endangered the physical security of hotel guests and other patrons…"

Finding the Right Solution for the Threat

Carter, who is a former NASA engineer, SIA Board Member and Homeland Security Advisory Group chair, has been involved in the security and access control space for more than 25 years. His background provided insights into the world of cyber and network vulnerabilities as physical access control and video surveillance began to migrate into the IP space. He says that as he and those he has worked with along the way saw where this convergence of physical and logical technologies was taking the industry, it mandated that the way physical security vendors approach solutions require they tread in both worlds. He advises that they create technologies that would move beyond traditional reactive methods to robust proactive and analytical solutions.

"At ReconaSense we decided to go out and build a system, first and foremost, that is an open platform. From my days being on the Security Industry Association board of directors and driving open standards for so long, it only made sense to start from the very beginning with an ability to deal with the open systems and physical security that we are all familiar with, but do it with an eye towards complete interaction with cybersecurity technology. We need to be able to communicate and alert, not just the obvious breach where my system will tell you a couple of things and your system tells me a couple of things, but a real handshake, a real discussion, so to speak, between systems," Carter stresses. "We have built the system using artificial neural networking and artificial intelligence as a layer above all of the standard systems that we are all used to: physical security, access control, video systems, intruding detection, data systems, and even weather plug-ins at this point. We've done it with an eye towards looking at things that are not traditional policy breaches."

Carter points out that the ability to incorporate artificial neural networking, where an access control system is learning and training itself to "think" and identify unusual activity that has not broken the defined policy, but provides a scoring matrix that can evaluate risk is a step towards making physical security systems behave analytically.

"When you look at it (physical security systems) in conjunction with a cyber system, they do very much the same thing, looking at the trends, and the habits, and the use of traffic on them, and when they would expect traffic, what files would expect to be hit, and how they would expect those to be looked at and used and manipulated throughout the day. We do the same thing with the physical side and with our cyber-side protection," Carter says.

Owning the Data and Analyzing It

The hard truth is that many physical security departments rely on an IT department to protect hard data or information – basically leaving cyber network protection to the cyber-side of the house.

"When we look at what happened with the Pyramid Group, we see that really didn't take place. Our system is like a cyber-based system; constantly monitoring the activity of the data systems that we manage and control. That's critical. It is just as critical as being able to lock down a door in an active shooter situation. It is just as critical as being able to dispatch life safety in a physical security event because the data that we're protecting, just like the cyber side of the equation, is life safety, is human assets," Carter adds.

Carter is adamant about bringing the sophistication and analytic levels of access control systems on par with advanced video surveillance where data-gathering and analytics are scored, and risk dashboards enhanced as a result. He alludes to the fact that many organizations face insider threats that escapes conventional security and risk analytics until it is too late.

"If you look at the hospitality groups, like the one that we just read about, they're open to public areas. There's a lot of activity that is going on, where no rules are obviously being broken, or nothing is being scored, evaluated, or monitored by an AI security-controlled system," says. Carter. "If you assess video analytics, you're looking for specifics. You might count the number of people that cross a line. You might look for a crowd gathering. You might look for particular license plates. But unless it is breaking a rule, you don't do anything with it. It is crucial now that we do a lot of associations on the physical security side. Say for instance, that a staffer has started coming in later in the evening or coming in on holidays when nobody else is around. That staffer can do that because your role-based access control system allows him to do that, because it can't adapt to risk."

With advanced AI and learning-based access control systems evolving in the market, Carter is confident the access control environment can now provide the missing link between data and pro-active analytics. He adds: "doing that has made the IT people interested because they see it now more as security information, not just physical control."

Security versus Convenience

The vpnMentor team calculates after reviewing data going back as far as April of this year when The Pyramid Hotel Group's servers were either being set up, reconfigured or subject to standard maintenance, indications are that the server was compromised and left open for attack. While records show that Pyramid Hotel Group was quick to rectify the vulnerability, the fact remains that the hospitality sector is not subjected to the same stringent regulatory cyber-risk pressures as others like finance and banking, and therefore may not be as proactive in their security approach.

Security consultant, Distinguished Fellow at the Ponemon Institute and former CSO of Boston Scientific, Lynn Mattice, is vehement that breaches like this are not acceptable and can no longer be ignored.

"With so many cyber breaches having occurred over the last decade and the extensive news coverage they have received, corporate leadership no longer can claim ignorance about their responsibilities relative to maintaining the security over their IT software, hardware and networks." Mattice claims. "Failure to maintain effective security controls over the intellectual capital of their enterprises in today's hyper-connected cyber world rises to the level of gross negligence and is a breach of the fiduciary responsibility of corporate executives and their boards of directors."

For Carter, the breach of the Pyramid Hotel Group and its impact on the access control system was the perfect storm.

"There is always an exciting push out there to say, 'I am using open-source systems, open source data' - databases like the one that was used. It was improper configuration and procedural approaches to utilization of technology that was certainly at fault. But even with the technologies that are there, even if you create something that works, so to speak, as an open source that can be implemented and utilized, people that are creating that should, by default, put them in lock-down situations not open to the public," admonishes Carter. "When you have a wide-open system, you lock down your perimeter and you work back from there. Then you determine who has procedural access to it, or physical access to it, or data access to it. I think so many locations start with wide open because they consider it to be convenient. When you do that and you walk away and you leave it that way, and you're using a third party company to install it that might not be up to speed on the latest approaches to protect information, then this is the kind of the thing that can happen. The technology that they used is convenient. It is open. It is all those things, but it is not necessarily designed for the environment that they utilized it for."

> The hard truth is that many physical security departments rely on an IT department to protect hard data or information…

About the Author:

Steve Lasky is the Editorial Director of Endeavor's SecurityInfoWatch Security Media, which includes print publications Security Technology Executive, Security Business, Locksmith Ledger Int'l, and the world's most trafficked security web portal SecurityInfoWatch.com. He is a 32-year veteran of the security industry and a 27-year member of ASIS. He can be reached at steveo@securityinfowatch.com.

Showcase of Security Products

Aiphone

Aiphone's updated JO Series video intercom enables homeowners and small businesses to control front-door access onsite or from virtually anywhere using a cloud-based mobile app. The new entry-level unit also has built-in options for recording visitors. It uses both a hard-wired, in-home master station with a 7-inch screen with wireless control inside or outside a home or business via mobile app. The affordable JO Series is available at a one-time cost without long-term contracts or fees. Both the video door station and inside monitor have a clean, modern design providing an attractive solution to match home or office décor.

Request more info: www.SecurityInfoWatch.com/21068292

dormakaba

The new Argus Optical Swing Lane from dormakaba comes in three models, including a compact model for limited space installations. Modular design elements include colors and materials for top covers, side and profile parts as well as drives and door leaves. From a compact model perfect for installation with limited space to exquisite illuminated objects with sophisticated sensors and seamless design, each Argus swing lane creates a striking, secure first impression.

Further information at www.dormakaba.us.

Request more info: www.SecurityInfoWatch.com/21069568

DSX

The DSX Mobile Command app brings the power of the DSX Workstation to an Apple or Android smartphone. The Mobile Command feature allows the activation of custom predefined commands, the locking/unlocking of doors, control of alarm points and the monitoring of system events from a mobile but secure application. Global functions such as building, campus and district lockdown, incident response reconfiguration and even repetitive chores such as momentarily unlocking a door or granting access to a gate can be programmed into Command buttons for easy activation.

For more information go to http://www.dsxinc.com

Request more info: www.SecurityInfoWatch.com/12426790

Request to Exit Switches

The CM-9800 Series Request to Exit switches from Camden Door Controls are IP 66 rated, as well as ADA and ROHS compliant. The capacitive touch switches offer color-selectable LED illumination, with vandal and weather resistant cast metal construction, and an adjustable 0 to 60 second relay timer. Switch illumination is highly visible in low light conditions and is easily activated by either the switch or door (locked) status.

Request more info: www.SecurityInfoWatch.com/21082071

Access Control Appliance

Continental Access, a division of NAPCO Security Technologies, has released the CA-ASA Access Control Appliance. Now featuring a 256GB Solid State Drive and 8GB of RAM, the compact network appliance runs on an embedded OS, and comes pre-installed with the latest version of CA4K Integrated Access Control Enterprise Software with full Native Client and Web Client Interface, providing integrated access, locking, alarms and video, and fast installation.

For more information on the Access Server Appliance, contact Continental Access at 1.800.645.9445, email salesinfo@cicaccess.com, or for specs or a training class or webinar go to Continental Access www.cicaccess.com/seminars.

Request more info: www.SecurityInfoWatch.com/12393669

Codelock

KeySecure by Codelocks is a new range of simple and effective key control cabinets. Control access and manage keys with only authorized users entering a single or unique code. Secure key control is an essential element to maintaining the security of buildings and vehicles. The rigid-built cabinets with mechanical or electronic digital coded locks provide an enhanced secure enclosure for keys, fobs and padlocks. The cabinets offer varying options from wall mounted, freestanding, self-closing, clear fronted cabinets and adjustable hook bars eliminating bunching and tangling of keys and padlocks. Key Management Made Easy. Visit Codelocks at GSX Booth 4015.

www.codelocks.us/keysecure

Request more info: www.SecurityInfoWatch.com/12426760

Showcase of Security Products

Alarm Lock's ArchiTech LocDown N90L Wireless Locks

Amityville, NY – The Alarm Lock Division of Napco Security Technologies, Inc.features the keyless school security measure for controlling access to classrooms, or any doors, in an emergency, with its ArchiTech® Wireless Access Locks with remote keyfob-activated lockdown, securing one lock or a global lock group, in seconds, at the first hint of trouble. Once lockdown is activated, a bright red strobe light is illuminated on the inner door to give occupants, i.e., sheltering in place, greater peace of mind that the door is securely locked down.

Please contact us at 1-800-ALA-LOCK, visit www.alarmlock.com or ask any Alarm Lock Representative.

www.SecurityInfoWatch.com/12416915

Salto NEO Cylinder

The SALTO NEO electronic Cylinder is designed for doors where fitting an electronic escutcheon is not possible or required and can be installed on standard doors, server racks, gates, cabinets, electric switches, sliding doors and more. It is available in an extensive range of models to suit almost any kind of door. The unit's reengineered clutch system design makes efficient use of energy, dropping consumption to impressively low levels resulting in 110,000 cycles with just one set of batteries. The product is IP66 rated to be weather resistant, making it especially suitable for the outdoors in even harsh environments.

For more information go to www.salto.com

Request more info: www.SecurityInfoWatch.com/21078608

DoorKing's new 900 MHz Wireless Access Control Products

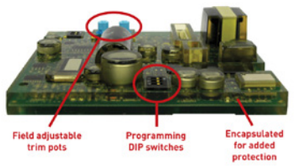
DoorKing's new 900 MHz wireless access control products allow integrators to add access points easily and inexpensively just about anywhere access control is needed on a property.

Wireless access control is extremely popular because of the cost savings it provides. Hard wired systems require conduit and wire runs which are very expensive, especially if the runs are lengthy, outdoors or have to cross sidewalks or roadways.

For more information go to www.doorking.com/900mhz

Request more info: www.SecurityInfoWatch.com/21069747

Enhanced Weather Protection for Entry Phones



For entry phone applications requiring an extra layer of protection against moisture, vehicle exhaust, pool chemicals or extreme temperatures, Enhanced Weather Protection (EWP) from Viking Electronics includes a circuit board potted in urethane or thermoplastic. The potting material will not crack in cold weather, protects against moisture and condensation, and is an excellent electrical insulator. Other features include internally sealed push-to-call buttons, dip-switches and volume control pots. Additional gaskets for speaker, mic and faceplate make them IP66 compliant.

Request more info: www.SecurityInfoWatch.com/21085657

HID Credential Management Service

AUSTIN, Texas, June 18, 2019 – HID Global®, a worldwide leader in trusted identity solutions, announce it has added the **HID Credential Management Service** to its growing offering of **cloud-based identity solutions**. The service simplifies the issuance and management of trusted Public Key Infrastructure (PKI) certificate-based credentials. The PKI credentials can be used by a broader range of organizations for convenient and secure multifactor authentication and converged physical access to facilities, as well as digital signing and encryption of emails and documents.

The HID Credential Management Service includes everything needed to issue and manage the lifecycle of digital identity and high-assurance credentials using a cloud delivery model. It removes PKI complexity and enables a wider set of authentication use cases than nearly any alternative in the Identity and Access Management (IAM) market. Most operating systems and browsers automatically recognize these certificates, ensuring the digital identity issued by the HID Credential Management Service can be used as a foundation for achieving zero trust security. Endpoint authenticator options include smart cards and USB tokens, mobile app authenticators and converged badges for accessing facilities and IT systems.

For more information about HID Credential Management Service, please click here.

Request more info: www.SecurityInfoWatch.com/21085255