ACCESS CONTROL Trends & Technology 2011

June 2011

Supplement to: *Locksmith Ledger International, Security Dealer & Integrator, Security Technology Executive*

The NEXT GENERATION of Access Control

Mobile Devices are Literally Opening the Door to New Technologies

Also in this Issue:

- Web-Based Access Control: The Right Choice for Small Business
- Keeping Tabs on Personnel During an Emergency
- For Integrators: Access Control Selling Checklist

CYGNUS BUSINESS MEDIA
CYGNUS SECURITY MEDIA

ACCESS CONTROL Trends & Technology 2011

June 2011

Supplement to: *Locksmith Ledger International, Security Dealer & Integrator, Security Technology Executive*

JUNE

10

14

21

On the Cover

Feature Articles

New Products

Advertiser's Index

Company Name	Reader Service No.	Page #	Web Site URL	Tel#
Altronix Corporation		S20	www.altronix.com	(888) 258-7669
Cogent Systems	460	S19	www.cogentsystems.com	(626) 325-9600
DKS Doorking, Inc.	455	S9	www.doorking.com	(800) 826-7493
DSX Access Control Systems	462	S23	www.dsxinc.com	(214) 553-6140
JLM Wholesale	461	S21	www.jlmwholesale.com	(800) 522-2940
Kaba Access Control	452	S5	www.kaba-access.com	(800) 849-8324
Keri Systems Inc.	457	S13	www.kerisys.com	(800) 260-5265
Linear Corp.	463	S24	www.linearcorp.com	(800) 421-1587
Marks USA	453	S7	www.marksusa.com	(800) 526-0233
Paxton Access	454	S8	www.paxton-access.com	(877) 438-7298
RCI - Rutherford Controls	458	S15	www.rutherfordcontrols.com	(800) 265-6630
SALTO Systems Inc.	451	S3	www.salto.us	866 GO SALTO
Sargent Manufacturing Company	450	S2	www.sargentlock.com	(800) 727-5477
Security Door Controls	456	S11	www.sdcsecurity.com	(800) 413-8783
Southern Lock & Supply Co.	459	S17	www.southernlock.com	(800) 237-2875

Visit Cygnus Security Media on the Web at www.securityinfowatch.com

ACCESS CONTROL TRENDS & TECHNOLOGY 2011

CYGNUS BUSINESS MEDIA

Published by
Cygnus Business Media, Inc.
Phone: 800-547-7377
Fax: 631-845-2736

3 Huntington Quadrangle, Suite 301N., Melville, NY 11747 USA
Phone: (631) 845-2700 • Fax: (631) 845-2736

3030 Salt Creek Lane, Suite 200, Arlington Heights, Illinois 60005
Phone: 847-454-2702 • Fax: 847-454-2759

12735 Morris Road, Deerfield Point, Bldg. 200, Suite 180
Alpharetta, Georgia 30004 • Phone: 800-547-7377

EDITORIAL

Editor-in-Chief, Security Technology Executive—Steven Lasky
Editor-in-Chief, Locksmith Ledger International—Gale Johnson
Editor, Security Dealer & Integrator—Deborah L. O'Mara
Editor-in-Chief, SecurityInfoWatch.com—Geoff Kohl
Managing Editor, Security Technology Executive—Paul Rothman
Managing Editor, Locksmith Ledger International—Emily Pike
Associate Editor, Security Dealer & Integrator—Natalia Kosk
Assistant Editor, SecurityInfoWatch.com—Joel Griffin

ART & PRODUCTION

Art Director—Kayla White
Production Manager—Jane Pothlanski

ADVERTISING

Publisher, Security Technology Executive—Steven Lasky
Publisher, Security Dealer & Integrator—Carol Enman
Publisher, Locksmith Ledger International—Nancy Brokamp

CYGNUS BUSINESS MEDIA

CEO, John French
CFO, Paul Bonaiuto
EVP Digital, Tom Kohn
SVP Digital Revenues, Paul Caplan
EVP Public Safety & Security, Mike Martin
VP Sales, Scott Bieda
VP Manufacturing, Tom Martin
VP Audience Development, Julie Nachtigal
VP Technology, Eric Kammerzelt
VP Human Resources, Ed Wood
Corp. Production Dir., Brett Apold
SVP Cygnus Expositions, Rob Brice

New Products

Wireless Portable Reader

Ingersoll Rand Security Technologies has introduced the WPR400 Wireless Portable Reader, which is fully compatible with the supplier's Schlage AD-Series and PIM400. The unit includes a cache mode option for offline applications ranging from attendance, event admission, checkpoints, signal testing, mustering, perimeter expansion, and more. The reader is also field-configurable to work as a Wireless Portable Signal Tester, making installation of wireless access control systems easier and faster. Comes with rechargeable battery and charger.

www.securitytechnologies.ingersollrand.com

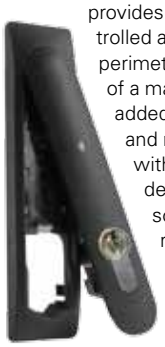
Select eInquiry #464 at www.securityinfowatch.com/ste/einquiry

PIV-Compliant Access Control Solution

HID Global, in conjunction with recently acquired ActivIdentity, has released ActivEntry 2.4, and access control solution that meets Personal Identity Verification (PIV) standards and certifications as mandated by Homeland Security Presidential Directive 12 (HSPD-12). The latest release adds a new service application programming interface (API), enabling Physical Access Control Systems (PACS) vendors to integrate enrollment capability directly to the solution's Validation Service. The solution also integrates reader configuration and audit management into the access control console. **www.hidglobal.com**

Select eInquiry #465 at www.securityinfowatch.com/ste/einquiry

Electronic Rack Handle



The RCI 3525 Electronic Rack Handle provides a secondary layer of controlled access to compliment existing perimeter security. The functionality of a manual latching system with the added benefit of electronic locking and monitoring can be combined with any third-party access control device for a basic self-contained solution. The unit does not require separate controls and software, therefore providing a simple and cost-effective cabinet retrofit. It can also be managed via a networked rack control and monitoring system for access control over the Internet.

www.rutherfordcontrols.com

Select eInquiry #466 at www.securityinfowatch.com/ste/einquiry

Dual Technology Prox Readers

Secura Key announces its new Dual Technology Proximity line, including both standalone and Wiegand output readers. The weatherproof units are compatible with Radio Key and 26-bit HID proximity credentials. Wiegand output readers include the RKDT-WM (mullion-mount) and the RKDT-WS (switchplate configuration). The RKDT-SA-M standalone mullion reader controls 65,000 cards, and also includes a Wiegand output. Also available in a switchplate configuration, RKDT-SA-S.

www.securakey.com

Select eInquiry #467 at www.securityinfowatch.com/ste/einquiry

FIPS 201-Compliant Access Control

Kaba Access Control has introduced the E-Plex 5800 series FIPS 201-compliant standalone access control system. The series incorporates a range of options and features to accommodate a variety of preferences and applications. The system can be as simple as enrolling FIPS 201 cards right at the reader without requiring any software, or using software to check card validation against the Federal Bridge PKI, import photos, set access schedules, retrieve audit trail, etc.

www.kaba-ilco.com/access_control

Select eInquiry #468 at www.securityinfowatch.com/ste/einquiry

Door Controller Product Line

Samsung Techwin America has added several standalone controllers and Wiegand-output readers to its access control line. The new devices employ various combinations of 125 KHz proximity or 13.56 MHz contactless smart card credentialing, keypad access based on personal identification numbers (PINs), and/or fingerprint biometrics. The new models include the SSA-S2000 Stand-Alone Single Door Controller with 125 KHz proximity and PIN access, and vandal-resistant SSA-S2000V (pictured), the SSA-S1000 Weatherproof (IP68 rated) Stand-Alone Single Door Controller, the SSA-S2100 Stand-Alone Single Door Controller for up to 20,000 ID users, the SSA-S3010 Stand-Alone Single-Door Controller with fingerprint recognition, and more.

www.samsung-security.com

Select eInquiry #469 at www.securityinfowatch.com/ste/einquiry

Virtual Access Control Appliance

PlaSec has launched the PlaSec Virtual Appliance, which enables end-users to deploy their systems in a virtual environment. Deploying an access control system in a virtual environment such as VMware's vSphere platform eliminates the need for a physical hardware appliance (such as the supplier's enterprise appliance, as shown) to operate the system, enabling end-users who have already invested in virtualization to leverage that investment with their security system design. The scalable appliance offers solutions for single-site applications up to multi-regional enterprise deployments. It is available through either a perpetual (CAPEX) or subscription (OPEX) software licensing model. **www.plasecinc.com**

Select eInquiry #470 at www.securityinfowatch.com/ste/einquiry

Wireless Keypad Series Alarm Lock's Networx

The Netpanel Wireless Prox and/or PIN Code Keypad series from Alarm Lock with two-door controller is the wireless version of its Trilogy DK/PDK3000 Digital and HID-Reader Keypads, ideal for strikes, mags, electric latch retraction exit devices, etc. The controller supports two keypads for back-to-back use or two-door systems. Additionally, it has a Weigand input so other approved Weigand output readers can also be used.

www.alarmlock.com

Select eInquiry #471 at www.securityinfowatch.com/ste/einquiry

Intelligent Door Closer

The Norton SafeZone Intelligent Door Closer from Assa Abloy creates a zone of safety around door openings in hospitals, healthcare facilities and other environments. It uses patent-pending technology to sense movement around the opening of a door and hold it open, enabling patients, elderly, disabled and other slowly moving persons to go through a door safely and comfortably. The unit combines an on-board motion sensor with an adjustable door closer. When the sensor detects motion in either direction around the door opening, it prevents the door from closing. **www.nortondoorcontrols.com**

Select eInquiry #472 at www.securityinfowatch.com/ste/einquiry

Residential Deadbolt and Lever Locks

Yale Locks & Hardware, an Assa Abloy Group company, has introduced new deadbolt and lever locks in the Yale Real Living portfolio of residential access control and home security solutions. Available with either a sleek capacitive touchscreen or pushbutton key pad, the locks support both Z-Wave and ZigBee, allowing them to integrate into a range of home control and security systems. Features include voice assisted programming in English, Spanish and French; personalized access-control scenes for up to 250 users; and access to all user programmable settings are available to the controller interfaces via select user interfaces.

www.yalelock.com

Select eInquiry #473 at www.securityinfowatch.com/ste/einquiry

Occupancy Indicator Deadbolt

Arrow Lock has added the Arrow Occupancy Indicator to the E Series Grade 2 Arrow Deadbolt, which provides secure privacy control in areas requiring visual notification of use, particularly restrooms, darkrooms and clean rooms. The deadbolt utilizes a large external viewing window to signal when a room is in use or vacant. Under emergency circumstances, an emergency key has override capability to unlock a door from the outside via an exposed external slot. Available eight finishes: bright brass, satin brass, antique brass, satin bronze, dark oxide bronze (oil rubbed), nickel plated, bright chromium plated, and satin chromium plated.

www.arrowlock.com

Select eInquiry #474 at www.securityinfowatch.com/ste/einquiry

New Products

Gate Operator Controller

Linear LLC's APeX Gate Operator Controller is now used in all of the supplier's Gate Operators, including the SL Slide Gate Operator, the SW Swing Gate Operator product series, and the LRA residential Swing Gate Operator. The controller features easy setup and programming, and built-in firmware that works with all gate types with no dipswitches or potentiometers to adjust. Additional improvements include an anti-tailgate feature, automatic close command, expanded radio reception range and more. **www.linearcorp.com**

Select eInquiry #475 at www.securityinfowatch.com/ste/einquiry

Hosted Access Control

Kantech's hattrix security solution offers a flexible hosted model that enables companies to remotely control their own security online in real-time or a customizable, managed solution that turns over some or all security responsibilities to a Managed Service Provider (MSP). The system offers end-users a solution without the infrastructure and training costs of traditional access control, and provides dealers and integrators additional recurring revenue through system hosting and management. **www.kantech.com**

Select eInquiry #476 at www.securityinfowatch.com/ste/einquiry

Stainless Steel Solid Body Padlocks

American Lock Co., a division of Master Lock, has introduced American Lock Stainless Steel Solid Body Padlocks. Built to provide the highest security under extreme weather and harsh conditions, they withstood rigorous testing to attain ASTM grade 6 status. Designed with complete corrosion-resistant construction, the padlocks are ideal for heavy-duty industrial and marine applications. They offer custom made-to-order options to fit any application, with a stainless steel exterior and stainless steel and brass internal components. **www.americanlock.com**

Select eInquiry #477 at www.securityinfowatch.com/ste/einquiry

Integrated FIPS Access Control Solution

Authenticard is a FIPS-201 compliant, high assurance access control solution based on an integration between AccessNsite, a multi-platform PACS management system from Quintron Systems; Farpointe Data's card reader technology; Mercury Security's Open Access Platform and Codebench's PIVCheck software suite. The solution validates PIV, TWIC, CAC and FRAC cards each time the card is presented to a door reader, ensuring that cloned or forged cards do not gain access. **www.quintron.com; www.codebench.com; www.farpointedata.com; www.mercury-security.com**

Select eInquiry #478 at www.securityinfowatch.com/ste/einquiry

By Brad Jarvis

The NEXT GENERATION of Access Control: Virtual Credentials

Mobile devices are literally opening the door to new technologies

With virtual credentials, hotel guests can check-in and receive a room key directly onto their mobile phones before arriving at the hotel.

For decades, we have carried our identities around on magnetic stripe (magstripe) and smart cards, but in today's mobile world, we now have the opportunity to embed them on a variety of portable devices. This will enable us to use products like smart phones, USB tokens, memory sticks and microprocessor-based SmartMX cards to open doors, buy tickets and execute other secure transactions. In order for this to work, however, we need a new way to securely provision identity and embed it into these portable devices.

There has been considerable news recently about mobile commerce developments, including reports that Microsoft is adding Near Field Communications (NFC) short-range wireless communication technology to its Windows Phone mobile operating system, and that Google, RIM and Apple are all preparing mobile payment and wallet systems. Similarly, the ISIS coalition (AT&T Mobility, T-Mobile USA and Verizon Wireless) has announced plans for the first pilot mobile commerce network using smart phone and NFC technology. Juniper Research has estimated that half a billion people worldwide will use their mobile devices as travel tickets on metros, subways and buses by 2015.

These and other initiatives will enable us to load our mobile devices with credentials that provide various levels of facility access, eliminating the need to carry a card, while making it easier for security managers to control who is entering and exiting monitored access points. It will also be possible to use these portable credentials to make other contactless transactions as well, such as cashless payment and transit ticketing, data transfers including electronic business cards, and gaining access to online digital content. Users will also be able to have multiple virtual credentials on a single device. For example, it will be possible to use a portable device to access a secure facility and also make cashless payments at the facility's canteen.

NFC Pilot Takes Flight

One early example of these applications is the first hotel pilot of NFC technology at Clarion Hotel Stockholm in Sweden. The hotel worked with HID Global parent Assa Abloy, Choice Hotels Scandinavia, TeliaSonera, VingCard Elsafe and Venyon, a fully owned subsidiary of Giesecke & Devrient, to replace the hotel's room keys with NFC-enabled mobile phones. The technology makes it possible for hotel guests to check-in and out using their mobile phones. The goal of the pilot is to get feedback from guests and employees using the NFC phones for a variety of services.

In the Clarion Hotel application, guests check into the hotel and receive a room key directly onto their mobile phones before arriving at the hotel. They book their rooms the

The mobile application enables two-factor authentication. A user enters their PIN on the above screen, then they tap the phone to the reader for access.

usual way, receive confirmation on their phones, and can also check-in on their phones before arrival at the hotel. When check-in is complete, the digital hotel room keys are delivered to the mobile phone. On arrival at the hotel, guests may then skip the check-in line, go directly to their room, and gain entry by holding the mobile phone close to the door lock.

Guests can also access other services via the mobile phone and, on leaving the room, check out using their mobile phone. The doors lock automatically.

NFC is one technology for presenting portable identities in these and other access control and mobile commerce applications, but there are many more. All of these technologies share the common need to operate within a new, more robust access control infrastructure.

Moving Beyond the Traditional Smart Card Model

Over the last 20 years, 125 kHz RFID proximity (or Prox) cards and readers have become a de facto standard for physical access control. They offer customers the optimum in cost and convenience, but are less secure than the contactless technology that subsequently emerged in the early 2000s.

The latest 13.56 MHz read/write contactless solutions enhance security through data encryption and mutual authentication, and also support multiple applications such as biometric authentication, cashless vending and PC log-on security. Contactless solutions have provided reliable service for nearly a decade while becoming the standard for efficient, secure and effective access control.

Now, the industry is developing a new access control architecture for a new era of advanced applications, mobility and heightened security threats. This architecture will enable a new class of portable identity credentials that can be securely provisioned and safely embedded into both fixed and mobile devices. This will improve security while enabling the migration of physical access control technology beyond cards and readers into a new world of configurable credentials and virtualized contactless solutions.

Managing the coming generation of portable, virtualized credentials involves a number of complex steps. In one typical example, a server would first send a person's virtualized credential over a wireless carrier's connection to the person's mobile phone. To

HID's SIO platform introduces a portable credential methodology based on a secure, standards-based, technology-independent and flexible identity data structure.

"present" the person's virtualized credentials at a facility entry point, the phone is held close to an NFC-enabled secure access control reader.

Throughout the process, there must be a way to ensure that the credential is valid. Both endpoints, plus all of the systems in between, must be able to trust each other. In other words, there needs to be a transparently managed chain of trust extending from one end to the other. This chain of trust requires the creation of a trusted boundary within which all cryptographic keys governing system security can be delivered with end-to-end privacy and integrity. This is the only way to ensure that all network endpoints, or nodes (such as credentials, printers, readers and NFC phones) can be validated, and all subsequent transactions between the nodes can be trusted.

One of the first such bounded environments is HID Global's Trusted Identity Platform (TIP). At the heart of the TIP framework is the Secure Vault, which serves known nodes within a published security policy. TIP establishes a scalable framework and delivery infrastructure for delivering three core capabilities: plug-and-play secure channels between hardware and software; key management and secure provisioning processes; and integration with information technology infrastructures. The environment can also support multiple usage models such as cloud-based applications that require service delivery across the Internet without compromising security.

With the establishment of a trusted boundary, it now becomes possible to deploy a new generation of readers and credentials that enable the use of portable virtual credentials on mobile devices, while also providing advanced security and performance functionality. This next-generation platform must go beyond the traditional smart card model to introduce a new, portable credential methodology based on a secure, standards-based, technology-independent and flexible identity data structure. HID Global calls this data structure the Secure Identity Object (SIO), which can exist on any number of identity devices and works with a companion SIO interpreter on the reader side.

Device-independent data objects and their companion interpreters behave like traditional cards and readers, but use a significantly more secure, flexible and extensible data structure. They offer three key benefits: First, because they are portable, they can reside on traditional contactless credentials and many different mobile formats, ensuring interoperability and easy migration. Second, their device independence enhances trusted security by enabling them to act as a data wrapper to provide additional key diversification, authentication and encryption while guarding against security penetration. And third, since they use open standards, these device-independent identity objects improve flexibility and can grow in security capabilities while traditional architectures remain stuck in a fixed definition.

Interoperability and Migration

Next-generation readers using standards-based, device-independent data structures will enable access control solutions that can operate on multiple device types with varying security capabilities. It will be possible for an identity object stored on one device to be ported to — and interoperate with — another device, with ease and without strict constraints.

Research reported in an AVISIAN 2010 survey shows that 90 percent of end-users believe that adding new applications with minimal investment is important; and 53 percent of respondents stated that they are not satisfied with the solutions to accomplish this in today's market.

Trust-Based Security

Next-generation access control readers and credentials will also be able to provide an additional layer of security on top of device-specific security. Secure objects will act as a data wrapper and provide additional key diversification, authentication and encryption, while guarding against security penetration.

The objects will be bound to specific devices by using device-unique properties, which will prevent card cloning. 93 percent of end-users in the AVISIAN survey said a key requirement was having multiple layers of security on cards or credentials — especially when other applications and private data were present. 37 percent of industry providers said they were not satisfied with available solutions.

Additionally, next-generation readers will incorporate EAL5+ Secure Element (SE) hardware to ensure tamper-proof protection of keys and cryptographic operations. They also will include such features as velocity checking to provides breach resistance against electronic attacks, and active tamper technology to protect against physical tampering of the reader.

Standards-Based Flexibility

The coming generation of reader platforms using device-independent data structures will also use open standards such as Abstract Syntax Notification One (ASN.1, a joint ISO/IEC and ITU-T standard), a data definition that allows for an infinitely extensible object definition. This definition can support any piece of data, including data for access control, biometrics, vending, time-and-attendance and many other applications. This will enable card and reader systems to optimize deployment flexibility and grow in security capabilities, unlike solutions with fixed-field data structures that remain stuck in a fixed definition.

Another benefit of device-independent extensibility is the flexibility it brings the developer community. The interpreter portion of the system takes care of mapping data to supported devices, which means the developer need only focus on generating and transacting (reading/writing) the secure objects. The days of the vending-machine developer having to learn about intricate credential-technology sector terminology and key rules is over.

Additional Considerations

In addition to enabling credential portability, the coming generation of reader and card platforms will forge new territory in the area of sustainability. Intelligent power management will reduce reader power consumption by as much as 75 percent compared to standard operating mode, and manufacturers will move to the use of recycled content.

Next-generation reader platforms will also improve usability and performance by including features such as multi-mode frequency prioritization, which will increase transaction performance while improving card management. These reader platforms also will include a variety of improved user notification features.

Device-independent data structures deployed on next-generation readers within a trusted boundary will enable the migration of physical access control technology beyond traditional cards into a new world of configurable credentials and virtualized contactless solutions that can be securely provisioned, no matter where they are or how they are connected. This model will also enable users to add levels of security, customize security protection, and extend system capabilities without having to overhaul the device infrastructure and applications.

Finally, this new approach will significantly improve overall system security while creating a more easily extensible access control system infrastructure that can also support a new era of more convenient, virtual credentials that can be embedded into phones and other portable devices. ■

Brad Jarvis is Vice President of Strategic Product Initiatives for HID Global Corp.

By Lester LaPierre

ACCESS CONTROL: A Checklist for Selling New Systems

A guide for security integrators

As a professional security integrator, it is only a matter of time before you receive the highest compliment from one of your customers when they say: "We need a completely new access control system, and we want you to design and implement it."

Along with the vote of confidence comes a huge responsibility. It can be a daunting task, especially if the system required is substantially larger than what is already in place. But if you approach it methodically, you can reduce error and ensure that your customer gets the exact system they require.

Listen to the End-User

Questions to ask include:

- What is the short-, mid- and long-range vision for the access control system? Is it based on open standards, like 802.11b/g or 802.3af, for the most affordable infrastructure? Is it scalable enough to support possible mergers and acquisitions?

- What type of credential(s) will be used? How many are issued? What type of format will be used, and can it support a projected card-holder population? Is it controlled to ensure there are no duplicate IDs?
- What investment has already been made? Is the current system upgradeable?
- What assets does the end-user have, and what value do these assets have in relation to the operation or business? These range from physical assets like computers to patient records, employee records and client data.
- Have the assets changed, requiring higher levels of security? Perhaps the locks and/or key system needs to be changed as well.

Observe the End-User

Essentially, the integrator should be trying to find out about the culture at the end-user's location. It can range from an open, accommodating environment, to one with strict and limiting access controls. There will always be a conflict between convenience and security — the challenge is to create procedures and rules that balance these disparate goals.

Did you observe the employees holding doors open for each other? If so, how are they able to verify their current employment status? Did they open the door for persons carrying large packages? If so, did they check their IDs? Did visitors sign in at the reception desk? Did they wear ID badges? Were they escorted by staff members? Did students have a habit of leaving their dorm rooms unsecure? If so, what sort of liabilities fall on school administration if a theft occurs and they knowingly allowed that practice to continue?

Conduct a Site Survey and Security Audit

Walking through a customer's facilities can be invaluable when developing a comprehensive access control plan. Here are a few things to look for:

- **Mechanical Security:** If the openings are not mechanically secure, any additional funds spent on electronic access control are wasted. The following must be addressed before moving forward on an advanced access control system: Are the doors, frames, and hinges in good condition? Are they rugged enough for the application and durable enough for the traffic? Are the frames mortar-filled?
  > What key system is in use? Is it a patented, high-security type? How often are locks re-cored? How many master keys have been issued? Have any been lost? How easy is it to reproduce the keys?
  > Is there accommodation for the handicapped to ensure compliance with the Americans with Disabilities Act (ADA)?

> Are cross-corridor fire doors in place? Do they have magnetic door holders tied to the fire system?

- **Identify Assets and Value:** Many consider assets to be tangible items that can be sold for quick cash. But assets include anything that someone might want to steal or destroy, and vary among end-users. The important thing is to put a price tag on the loss of the asset, plus the cost of lost productivity and potential liability that could result.
- **Identify the Threat:** Consider the end-user's surroundings: Have you noticed any evidence of gang activity? Have you noticed an increase in shuttered businesses? If so, perhaps an increase in perimeter security is in order, potentially including increased lighting, cameras and gated access.
- **Evaluate the Facility(s):** This will help you identify product options. How old is the building? Does it have architectural or historical significance? How thick are the walls? Was asbestos used as an insulating material? If so, it may be difficult and costly to install conventional, wired access control devices. Perhaps a WiFi solution will be a good alternative.

Be sure there is a reasonable accommodation for the handicapped to ensure compliance with the Americans with Disabilities Act (ADA).

Get the Technical Details

For each opening requiring access control, you'll need the following details to ensure you order the right product for the given application:

- Does the door swing in or out? Is it left- or right-handed?
- What's the finish of the existing hardware? What's the lever style? Would the end-user prefer a more modern look?
- How is each door expected to operate? Ensure that an operational narrative is written for each opening that covers the following conditions, and have the customer sign off on it. This should include: normal state; authorized/unauthorized access and egress; monitoring and signaling; and power failure, fire alarm and mechanical operation.
- Determine where to place access control equipment. This could be Telco and IT closets, server rooms or administrators' offices. Make sure your staff will have access for installation, and later for service and maintenance. Also, make sure there is enough space on the wall to mount access control panels, interface modules and power supplies.
- Determine network coverage. Are IP drops where you need them? Is there sufficient WiFi coverage where you need it should you opt for WiFi locksets?

Ensure Code Compliance

Several agencies have issued codes and standards over the years to enhance life safety, improve privacy and reduce fraud. They need to be factored into an overall access control plan, and include the ADA, the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SarbOx or SOX).

Building Codes and Standards include: Model Building Code (IBC) — Amendments, Occupancy; Life-Safety (NFPA 101) — Means of Egress; Fire (NFPA 80) — Retro-fitting, Sprinkler Systems; Accessibility (ANSI A117.1) — Operators, Credentials; and Electrical (NEC NFPA 70) — Installation, Wiring, Products.

Validate the Security Requirements

Different applications and clients have differing security requirements. Verify these needs with the end-user *before* starting the system design; otherwise, you could be in for a lot of extra work. The following considerations should be factored into an overall access control plan, as they have a direct impact on product selection and system configuration:

- **Lockdown:** Is lockdown capability needed in the interior or just the exterior — or at all?
- **Real Time:** Is real-time communications to the access control system a critical requirement? Perhaps it is for perimeter doors, but what about interior doors? What if you could save the end-user $1000 per door by specifying a WiFi lock instead?
- **Monitoring Requirements:** How much monitoring does the end-user need? In most cases, a door position switch will suffice; however, some clients want to know that the door is both closed AND secured — these are not necessarily the same thing.
- **Audit Trail Requirements:** How important is it to know who and when someone entered a building or room? For code compliance, this feature is always mandatory, such as accessing computer rooms, personnel records and patient records; however, some companies use audit trail reports to validate employee activity.
- **High-Security and Classified Areas:** For increased security, there are several options. Is multi-factor authentication a requirement, such as card and PIN or even a biometric verification? Should there be a two-man rule?
- **Special Considerations:** Some areas, like memory treatment centers for Alzheimer's patients, require valid access credentials from both sides of the door — keeping the right people in

and the wrong people out. This requirement takes different hardware than a typical free-egress lock or exit device.

Determine Business Requirements

Consider the final details that will allow you to complete your system design:

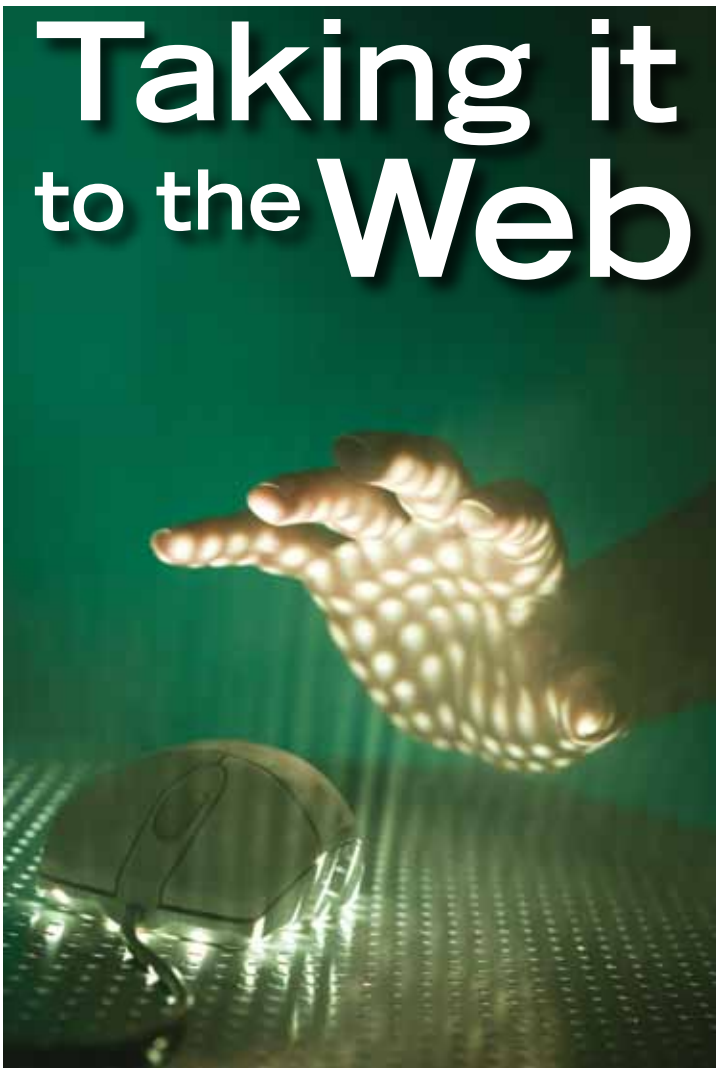
- **Aesthetics:** Many high-profile building owners use architectural design to make their facilities stand apart. This extends to the interior space as well. So, is a black wall reader the right choice? Or will an elegant lock with integrated card reader and designer lever be a better option?
- **Infectious Disease Control:** Some locks and doors are available with an anti-microbial finish designed to inhibit the growth of bacteria.
- **Turnover:** What kind of turnover does the facility experience? Heavy turnover would be difficult to manage with a PDA-programmable offline lock; however, one-card systems program access privileges onto the card, virtually eliminating the need to tour the doors to reprogram them. Of course, online solutions could address this as well.
- **Applications:** It is inevitable that a variety of applications will converge into a single system. That's why it is important to select an access control system that can grow by providing application support for parking access, visitor badging, integrated video and other needs as required.
- **System Management:** It is important to determine who, how and where the end-user will manage the new access control system. For enterprise-class systems, it might mean multiple departments will manage their own people, while a system administrator will maintain and manage the main, centralized system.
- **Budget:** You ultimately need to know your customer's budget; however, with all the upfront research, your findings might be beyond their initial scope. This is how long-term planning comes into play so you can develop a priority list over several phases to ensure the end-user gets the access control system that fully meets their requirements. ■

Access control equipment can be placed in server rooms.

Lester LaPierre is Director of Business Development, Electronic Access Control for ASSA ABLOY Door Security Solutions.

By Eyal Shebiro

Taking it to the Web



© Getty Images

Why Web-based access control systems are the right choice for small businesses

Traditionally, the access control systems market has been dominated by large facilities that require comprehensive and complex installations. Access control system installation opportunities can be hard to come by for security and locksmith providers who focus on small businesses. Small business owners typically need to secure fewer doors — and at a lower cost than what is possible with traditional access control technologies.

It is simple — these products do not work for small businesses because they are not designed for them. A gap has traditionally existed in access control system features, wherein the entry point for making effective use of the technology starts with securing a minimum of four doors. And since most products offer more than what many smaller end-users actually need, they tend to cost more than what end-users are willing to pay.

Think about how many small businesses have less than four entry points. These represent missed access control opportunities. In the past, this gap has limited the ways in which locksmiths can expand in the lucrative market of businesses with three or fewer doors to protect.

Fitting Individual Needs

Many small business owners recognize the need to ensure the security and safety of their property, employees and end-users but are forced to rely on conventional lock-and-key or keypad systems. The demand for more advanced systems certainly exists — many end-users I work with have voiced their frustration at the lack of an adaptable system that works for them.

However, recent product advancements are turning this under-represented group into an eagerly enthusiastic end-user base. Great strides have been made in the development of products and technologies that can meet the needs of businesses with fewer doors to protect. What's more, these new solutions provide end-users with more benefits and features than other keyless entry technologies, creating opportunities to upsell without overselling. The proliferation of these products has created a momentum shift in the access control industry, with a greater frequency of business owners with fewer than four doors to secure requesting similar security solutions.

So what kinds of features can persuade these business owners to jump from keys to keyless? Three words: simple, flexible and scalable.

Access Control from Anywhere

The complexities of managing and operating large-scale access control systems created additional obstacles that, until now, have hindered broad market adoption. Smaller businesses generally do not have the capital to hire a full-time employee with the necessary technical skills to run a server-based access control system. They seek an easy-to-use

master system that features a simple point-of-entry tracking and reporting feature, but instead they are stuck with complicated systems that are beyond their technical competency. Thus, managing traditional access systems has often required system operators with qualifications in information technology to complete relatively routine tasks, like securing doors, managing access and sites, and pulling reports to meet compliance requirements.

Fortunately, the tide is changing. Recently developed Web-based access control solutions provide both locksmiths and operators with an elegantly simple solution. Web-based access control enables one or more operators to control the system from anywhere via a browser. They can easily add or remove security functions and privileges on individual keycards and entry-points, creating an entirely customizable solution.

Web-based access control systems like this are simple enough for office managers with very basic computer skills to operate and maintain, and they typically require less than 30 minutes of training. In addition, these systems typically do not require IT expertise for installation.

For example, a law firm sought an access control system for its office's shared entrance. The firm previously relied on a tangled mess of keys to control the entrance, which made managing access difficult. As a result, the law firm decided to convert to keyless entry and ultimately chose Honeywell's NetAXS-123 system for better point-of-entry control.

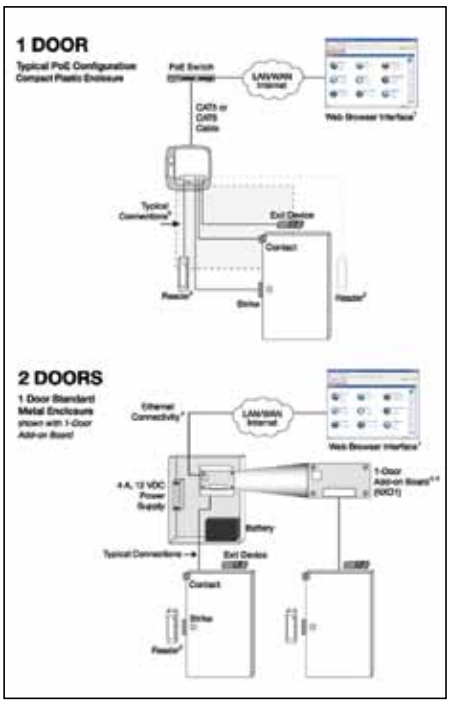
The Web-based access control system provides a greater degree of control over the office's entrance, and enables system managers to easily complete tasks like adding or removing people from the system at any time or changing card access — all via the Internet.

Web-based access control systems also greatly reduce operating costs. System controllers are not tied to one PC and are not handicapped every time the PC has an issue. Browser access eliminates the need for dedicated control PCs and the expenses associated with operating systems, servers and software licenses. It also nullifies the risk of virus infections and computer issues like hard drive crashes or system lock-ups. As the old saying goes, time is money, and any time that business owners must dedicate to training or operating the system is time that could be better spent running their business.

One Door at a Time

Locksmiths can also benefit by offering end-users Web-based access control systems that are suited to grow with their business. The Web-based access control system described above is an ideal solution because its flexibility allows it to easily accommodate the addition of more doors. Thus, it is necessary to offer systems that can add doors with simple installations — this, in turn, will increase future revenue potential.

Systems with add-on boards can be mounted directly on top of



Single or two-door upgrades or better can be easily configured with Web-based access control systems.
Diagram courtesy Honeywell

control panels via a board-to-board connector, which means they do not require extra wires or cables to connect. This provides simple expansion capabilities — adding a door does not require re-wiring the system or changing out the enclosure. Instead, you simply add on to what the end-user already has in place.

Smaller end-users will likely want to focus on protecting one door at a time; therefore, expansion should be quick and painless. System startup for a single door with a common application system can be completed in 20 minutes or less, meaning end-users can spend less time focusing on the installation and more time running their business.

Access control systems can also benefit from having a small enclosure footprint, which speeds up the installation process and is ideal when space is limited. Generally, plastic enclosures are smaller and more compact than conventional metal enclosures, allowing them to be mounted in convenient locations instead of taking up space in a storage room or closet.

Another example: A health club was looking to integrate an addition to its existing access control system. The club installed NetAXS-123 to control access to a bike cage, giving members and employees a secure area to store their bikes. To integrate NetAXS-123 with its existing system, I simply added a router as an access point and wirelessly connected the bike cage to the main system with basic programming. This easy process capitalized on the system's Web-based capabilities.

Locksmiths seeking to recommend electronic access control should opt for Web-based access control solutions to penetrate the small and mid-sized market. Capabilities like plug-and-play installation and power over Ethernet (PoE) free business owners from the expensive and laborious installation process that can include tearing up walls and rewiring. Plug-and-play features allow the installer to tap into existing infrastructure and wiring. With PoE, installers only need one wire to the panel and will not need to run separate power. The wire to the panel enables power for the strike, reader and input devices.

A Win-Win Situation

Remember, features sell and help deepen your relationships with your end-users. Outfit your end-users with access control systems that match the nimbleness of the businesses they run. End-users are looking for a system simple enough to operate without technical prowess, priced to match their needs and designed to adapt as their business grows. Business owners will benefit from the solutions they receive, while locksmiths can unlock the power of the Internet and benefit from providing additional services. ■

Eyal Shebiro is the owner and operator of Locks in the City, a security and locksmith services provider based in New York City. He can be reached at eyal@locksinthecity.com.

By Bill Patterson

PASSING MUSTER: What You Need to Know About Mobile Mustering

Hand-held computers keep personnel records in reach during an emergency

Keeping track of all evacuees is a prime concern during the mustering process.

Imagine an emergency scenario — fire, bomb threat, gas leak — in which you need to evacuate your building or campus. The proper alerts have been sounded, people have migrated to the mustering location and first responders are on the scene. How do you know if everyone made it out? And where are the ones who remain inside?

In the past, security personnel may have grabbed a printed emergency evacuation list on the way out in order to facilitate the manual counting and sorting of employees. Progressing to laptop computers helped automate the process, but laptops often take precious minutes to start up and are

data-dependent on the physical access control system (PACS), which may not be online during an emergency.

Mobile mustering, which uses mobile handheld computers that work online or offline, is the newest mustering tool available. The hand-held units are equipped with card readers to quickly scan IDs and assess mustering progress and statistics.

© Thinkstock/George Doyle

With mounting pressure to account for workers during an emergency, mustering must be part of an organization's emergency plan.

Local or PACS Mustering

There are two types of mobile mustering — local and PACS. The former works as an autonomous system that uses hand-held computers to log in and out people at a job site or facility. Local mustering is often helpful for temporary locations like construction sites, where it is important to track entry and exit from a location, but installing hardwired card readers is not feasible or is cost-prohibitive. Time-stamped reports can also be uploaded from the hand-held unit to track hours and billing.

PACS mustering, on the other hand, works in conjunction with hard-wired readers and access control systems. During an emergency, a security agent can use the hand-held computer while evacuating and have the latest available data from the PACS. The unit can then be used at the muster point to scan cards and to assess who remains in a facility.

An advantage of PACS mustering — particularly on larger campuses with multiple buildings or floors — is that the system automatically logs the location where the cardholder last swiped his or her ID to gain access to a building or floor. This is helpful for narrowing down the location of a missing employee.

"Mobile mustering creates an added layer of security and safety capability with flexibility to deal with many situations, both planned and unplanned," says Dave Sylvester, vice president of business development for DAP's parent company, Roper Industries. "Linked to an access control system or identity management system, the mobile application enables routine security controls and, in the event of an emergency, provides site managers with a tool to efficiently account for personnel."

Mobile Mustering Online or Offline

In PACS applications, mobile mustering can be used online — while wirelessly connected to the access control system — or offline, which is especially important during emergencies like fires or explosions that could compromise the integrity of the system.

When used offline, the hand-held units retain the last available data from the PACS, enabling the security officers to continue scanning IDs and updating the information. When the system is back online, the hand-held units automatically sync with the PACS, instantly updating the system data.

The hand-held computers also retain cardholder data including photos and contact information. If employees forget their cards while they are evacuating the building, their identity can still be verified even when the system is offline.

Ready, Reliable and Rugged

With mounting pressure from OSHA to account for workers during an emergency and budget reductions shrinking security forces, mustering must not only be part of an organization's emergency plan, it also must be accomplished with fewer resources. Choosing a system that is ready to perform, reliable and rugged will help you get the most from your investment.

The basic requirements for mobile mustering include a rugged, lightweight hand-held computer that can function as a mobile reader. It should be capable of reading formats including smart cards, PIV, PIV-I, HID Prox, iClass, Mifare and bar codes.

The ability to read PIV and PIV-I cards is particularly important for government agencies, which are required by the White House's Office of Management and Budget (OMB) 11-11 to have a PIV-compliant access control system and have a disaster recovery plan in place. A mobile reader that is PIV/PIV-I-compliant is essential for these customers to comply with their disaster recovery plans.

A mobile application of an existing PACS can provide the greatest flexibility and functionality. Hawkeye Technologies, for example, packages mobile mustering as a component of its mobile client applications for AMAG Technology, an access control, IP video and intrusion detection company. In addition to mobile mustering, users of the mobile application can control locks, doors, video surveillance, alarms and more from a hand-held computer from DAP Technologies.

Because emergency situations evolve quickly, data integrity is the top priority in mobile mustering. When integrated into a PACS, the ability for the system to capture and continually update data online or offline from multiple mobile handhelds safeguards data and ensures reliable information.

The computer for mobile mustering should be able to withstand the elements and rough treatment since they are likely to be used outside. Rugged handheld computers should be sealed against dust and liquids to at least IP65, operate in temperatures ranging from (-4°F to 122°F (-20°C to 50°C) and survive a 1-meter drop to concrete. They also should offer a sunlight viewable display.

Mobile mustering offers many advantages for both local and PACS applications. At the end of the day, however, it comes down to this: Quickly tracking employees and first responders during crisis situations can save lives.

Bill Patterson is the National Account Manager, Security & ID Management, for DAP Technologies (www.daptech.com). He can be reached at b.patterson@daptech.com.