Blackboard transact™

Campus Access Control Advancements

It used to be that simple locks, residence hall keys, or a door propped open after hours were the key components to campus "access control." But with today's additional focus on campus safety and security, access control is far more advanced.

In This White Paper

Opening doors—both literally and figuratively—for campus security

Securing a college or university campus begins with keeping people out of facilities where they have no legitimate business—from an administration office to a dormitory or an equipment storeroom. But, it also means providing the appropriate access for students, faculty, and staff—at all times of the day and under varying circumstances.

Limitations of lock-and-key control

Some campuses still protect their doors with mechanical locks and keys. Although they can create effective barriers, they can also have major flaws. Keys can be lost, stolen, or copied an unlimited number of times. It's even possible to use a photograph of a high-security key hanging from a police officer's belt to produce a perfect copy using a 3-D printer. Once a lock's security has been compromised, it must be rekeyed in an expensive and time-intensive process. And then new keys must be cut and distributed.

Key management can be challenging at best on a large campus with thousands of doors. Multiply that by tens of thousands of keys in the hands of students, faculty, and staff and the margin for error grows exponentially.

Open, unstaffed offices and buildings provide tempting targets for thieves and other criminals. According to FBI statistics, more than 85,000 property crimes—theft, burglary, and motor vehicle thefts—were committed on U.S. higher education campuses in 2012.[1] The losses ranged from students' personal property to sophisticated laboratory equipment.

Advantages of electronic access control

Today's best security practices call for a campus-wide electronic access control system that takes advantage of an enterprise network. Basic system components include computer software that maintains information about campus community members; key-replacing credentials that identify individuals; and readers—the new locks—mounted at critical entries. Together, they add a valuable layer of security, while addressing many of the weaknesses of mechanical key locks.

Within seconds, campus administrators or safety officials can delete a missing credential from the software. A replacement card can be created almost as quickly. There is no need to alter or replace any readers or the cards of other campus community members. Also, newer card technologies are difficult to copy.

An electronic access control system provides a college or university campus many other advantages including:

- **Campus-wide coverage:** Systems can be designed to handle even the largest campus. And satellite locations can be added to the system through the enterprise network.
- **Scalability:** Electronic access control systems can be expanded and components can be moved as a campus grows and/or its needs change.
- **Wireless capabilities:** Many readers and other system components operate wirelessly allowing them to be placed in remote facilities where it may be impossible or too costly to run cable. Readers can also be added for short-term activity such as temporary contract jobs.
- **Remote control:** Using the campus network, the access system can be remotely controlled using a smartphone or tablet—improving the productivity of field security officers.
- **Temporary access:** Visiting professionals, vendors, and others with a need for temporary

access to a specific location or set of locations can be granted access only to those locations for a limited timeframe.

Integration of systems

A unified or integrated security system is most effective. That involves integrating the access control function with other vital security layers.

Intrusion

An enterprise access control system integrates with a campus' intrusion system. When sensors in windows, walls, ceilings, and floors detect a break-in attempt, the access control system will display a campus map pinpointing the alarm site.

Video

Surveillance cameras placed throughout campus provide views of key access control readers. Integrating the two systems allows safety officials in the central command center to receive an immediate visual of alarm sites, providing valuable information before dispatching officers.

Mass notification

A mass notification system provides vital information before, during, and immediately following a man-made or weather-related emergency. An integrated access system can automatically lockdown all doors during an immediate-reaction situation. Or the system may unlock certain doors to allow egress during a fire.

Mobile tip reporting

A comprehensive mobile safety app allows campus community members to submit GPS-tagged tips with text, including picture, video, and audio plus live chat capabilities to campus security. The app can place calls with location tracking directly to the campus safety office, display a map with incident data and emergency locations to improve overall safety awareness, and even monitor the location of friends throughout campus.

Credentials and readers

Some of the more exciting updates in electronic access control technology are occurring in the individual credentials and the devices that read them.

For decades, the most commonly-used cardkeys in the U.S. included a thin stripe of iron-based magnetic particles (magstripe) on which information is written and stored. To work, these magstripe cards must be swiped through a slot on the top, side, or bottom of a reader.

Next up were contactless proximity cards that only had to be held within a few inches of the reader to open a door. They can also be printed with the holder's photo and other information, providing a combination ID badge and access card.

Technology developments led to smart cards, which contain a CPU with RAM and ROM read/write storage capability. These cards are mini-computers able to store information for different system technologies.

For example, smart cards can provide door access while also granting permission to logical resources such as computers and printers. It can also combine debit card functions to create a one-credential system found on many college and university campuses.

With a single contactless smart card, a holder can check out library books, make bookstore purchases, attend cultural or sporting events, and buy food from vending machines as well as on- and off-campus restaurants.

Newer ID credentials are using card/reader technology known as NFC or near-field communication. This has spawned a group of new contactless cards with an NFC chip embedded that can store more information and be used for more applications.

Now, native NFC-capable smartphones are able to act as a contactless keycard to readers on campuses that have adopted a one-credential system. Smartphones as access and transaction cards are already in pilot projects on major college and university campuses, providing additional convenience to students and institution staff alike. Security is also improved, as students don't have to carry multiple access/debit/credit cards or cash.

Using the native technology avoids the need for bulky clip-on peripherals or stickers on readers, or the launching of a special app on the phone when the NFC features are to be used. Also, students tend to lose their phones less frequently than access cards.

Typically, each credential type works with a reader using a complementary technology. It's not unusual for a campus to simultaneously employ several different card, credential, and reader technologies that may require students, faculty, and staff to carry multiple cards.

Changing existing—or legacy—card and reader systems to one standard doesn't have to be expensive. Fortunately, there are hybrid readers capable of reading multiple credential types—eliminating the need to re-card the entire campus. By adding hybrid readers as older units fail, a campus can make a planned migration to newer, more robust technologies.

Permissions, partitions, and zones

Enterprise access systems allow campus safety officials or human resources administrators to add various

permissions to each card, limiting which doors the cardholder may access, as well as limit the times and days access is granted. An enterprise system also permits HR to automatically update credentials when employees are hired or fired.

A Growing Market: According to one leading market research firm, the global access control market grew from just over $10 billion in 2009 to $15.4 billion at the end of 2013. Spending is expected to grow to $31.2 billion in 2019.[2] Educational institutions are prime drivers of that growth. Theft, sexual assaults, vandalism, and other crimes are leading factors in administrators' decisions to add a unified security system or expand an existing system.

Partitioning access systems allows the main users—typically campus safety officers—to monitor the entire system while giving personnel in other departments or facilities the ability to monitor and control their own space. For example, on-campus retailers and food servers might choose to set their employee access policies.

The systems also permit the creation of occupancy zones preventing people from entering a zoned area once maximum occupancy levels have been reached. For example, this is ideal for use in a parking garage when all spots are filled. Also, zones can be created for other purposes, such as turning on lights when an area is occupied and turning them off when people leave.

Audit trails

Each time an access credential is used, the reader sends information to the system controller about the owner's identity and the precise time the credential was used. That provides an audit trail for use by campus safety officials when investigating a campus incident or crime. By placing a reader inside a door, officials can also have a record of who left a facility and when.

Choosing a provider

When it comes time to install or upgrade a campus-wide electronic access control system, choose a provider offering a complete package of controllers, readers, and credentialing technology. It's also important to have a provider that can integrate the system with intrusion, video surveillance, mass notification, and other critical security layers. And the provider should be able to provide ongoing service after installation.

About Blackboard Transact

Blackboard Transact delivers the security and convenience of a single, unified credential that not only meets your campus needs, but transforms your students' overall campus experience. It provides unified transaction, security, and financial solutions—from building access and online financial aid disbursement to campus meals and on-and off-campus purchasing. For more information, visit http://www.blackboard.com/transact.

[1] *Federal Bureau of Investigation: Crime in the United States 2012. http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012/tables/9tabledatadecpdf/table_9_offenses_known_to_law_enforcement_by_state_university_and_college_2012.xls/view*

[2] *Persistence Market Research, 2014. http://www.mynewsdesk.com/us/persistence-market-research-2/pressreleases/electronic-access-control-systems-eacs-market-will-reach-31-2-billion-in-2019-persistence-market-research-1047798*