

Protecting School Perimeters

Today, locks and keys alone aren't enough to keep a school's perimeter secure against unwanted or uncontrolled visitors. From problems with non-custodial parents in a grade school to unauthorized residence hall guests on a college campus, controlling access with greater certainty is the first line of defense to keep a facility secure.

Schools and colleges of all types and sizes are becoming more aware of the security risks posed by unauthorized access and are taking proactive steps to prevent a broad range of potentially threatening or dangerous incidents. In the K-12 field alone, each of the more than 100,000 public and private schools may have between eight and 20 doors that require perimeter security. Multiple-building college campuses present a more complex situation, with different types of buildings requiring different levels of security.

Not All Security Needs Are Equal

Not every door has to be a controlled entrance, nor is it always necessary to have 100 percent, 24-hour positive control. The doors to a grade school or middle school may be open during the time students are arriving and then locked down during the school day, as well as after hours. Effective access controls and a monitored main entrance provide the required security during school hours, while some form of electronic access control and a secure credential system allow after-hours access for authorized individuals. Other doors can remain locked unless monitored by a teacher or staff member as part of an activity.

Sorting out the Security Levels

One way to reduce the complexity of security decisions is to organize the key elements into levels that form a Security Pyramid.

The base of the pyramid, *Level 1 (Mechanical Access/Egress Control)*, represents the fundamental mechanical locking system that restricts free access or egress through an opening. It includes keyed locks and other mechanical products. At this level, security is focused mainly on protection from threats such as theft or vandalism and on providing a physical barrier to intruders. However, if any part of this mechanical base is weak, the higher levels of a system's security can be compromised. It also provides the physical latching needed to secure an opening so it meets fire safety codes.

At *Level 2 (Electronic Access Control and Key Management)*, standalone, programmable, battery-powered locks are networked through software to provide audit trail capability and time-

based scheduling for restricting access. Patent-restricted keyways provide the key control that is necessary for high security. This is particularly true for sophisticated electronic systems, which generally still have a mechanical key override. With a patented keyway, a school's administration or university's security department controls the key blanks as well as the key cutting equipment. To minimize security breaches from key misuse, these keys should be tightly controlled, assigned to as few people as possible, and audited regularly.

Level 3 (Networked Access Control and Biometrics) incorporates biometric products that can verify hand geometry, fingerprints or face characteristics to ensure that only persons who actually are authorized can gain access to a particular door. In a network they may be combined with various sensing and monitoring products placed around the opening or integrated into the latching and locking mechanism to detect, deter and delay an intruder and also signal that a breach has occurred. While not yet widespread, some schools are using biometric access control to eliminate the need to issue cards or keys to teaching or administrative staff members for after-hours access.

Level 4 (Facility Integration) covers all the previous levels plus additional areas managed by software solutions, such as time-and-attendance systems, personnel scheduling systems, and data capture techniques. These can reduce the need for security staff or monitors, provide audit trails to resolve problems, speed response time if a problem occurs, minimize maintenance, and make it possible to create a central command and control area when appropriate.

On-line access control systems have become common on college and university campuses, and school districts are now beginning to move in the same direction. Integrated access control systems that incorporate on-line access control, CCTV/DVR, alarm monitoring and badging are taking their place in schools at all levels.

Security Solutions

Commonplace open key systems offer little real protection. Duplicates are readily available at hardware stores and mall key shops, and lax key control can lead to security problems. Restricted key systems offer somewhat greater security because key distribution is controlled. However, unless the keyway is patent-protected, a "Do Not Duplicate" stamp on the key provides little real protection. With a patented keyway, anyone other than the manufacturer who makes key blanks available is in violation of Federal patent laws. These are restricted further when the manufacturer agrees not to sell a specific patented key configuration to anyone else within a defined geographic area. With these levels of security available, it is important to know what level is desired and select the proper keyway.

Moving into electronic locking, there are many variations available, each providing a different combination of security and convenience. Schools that desire more control options than are available with mechanical key systems may use magnetic stripe or proximity cards or i-Buttons. Electronic locks that are used with these credentials often have the ability to restrict access to certain individuals, during specific hours or days, or for limited periods of time. Some also incorporate audit trail recording that can be helpful in investigating incidents of theft or vandalism.

Although these locks may be hard-wired into a network, the same results can be obtained with standalone computer-managed (CM) locks, which are networked by using a Palm Pilot or other PDA to download data from a computer. This eliminates the cost and problems associated

with hard-wiring, especially in existing buildings. The battery-powered CM locks typically operate for more than a year on standard commercial batteries.

In the Field

At the *Clackamas High School* in North Clackamas, Oregon, computerization and electronic credentials are used where needed, but simpler solutions also are applied whenever they will deliver the desired results. Every exterior exit is wired so it can be “dogged down” (retracted) electrically from one of two central office locations. If an emergency lockdown situation occurs, all doors can be locked at once to protect the perimeter, while the exit devices still allow safe egress for those inside. Interior classroom doors are equipped with a lock cylinder on the inside so the door can be locked down without the teacher having to go into the corridor, which could be unsafe. The combination of central unlocking control for perimeter doors with individual inside locking for interior doors provides the security needed without excess cost or complication.

All building entrances at Clackamas High School are equipped with proximity card readers that allow authorized individuals to enter. Cards can be issued to allow access only to the gym, auditorium or cafeteria for scheduled community activities. The cards activate exit devices with electric latch retraction or electric strikes to allow entry during specified times. Some keys are issued for access to the building, but only to those with an ongoing need. To prevent unauthorized duplication, the school uses the Schlage Primus high security key system, primarily on exterior doors and high-security interior doors such as computer labs.

To help the *West Islip, New York K-12 district* determine the exact type and condition of existing hardware on each door and establish a priority for its replacement, the Metro New York office of Ingersoll Rand Security Technologies conducted a Security and Safety Needs Assessment at the district’s six elementary schools, two middle schools, and the West Islip high school. To regain key control, the district standardized on the Schlage Primus patented keyway system, with key blanks only available through the manufacturer.

At the high school, because of its size and more complex access control requirements, Locknetics CM standalone electronic locks were installed on some exterior doors. The locks accept either i-Button or magnetic card credentials, and PIN numbers can be added as well. The locks also can control or restrict access during specific hours and provide an audit trail of who used or attempted to use the lock. If an i-Button is lost or a teacher forgets to turn it in when leaving the district, it can simply be deleted from the database. This avoids the cost of rekeying and maintains the desired level of security.

Some K-12 schools are moving into biometrics for certain applications. *Robert C. Byrd High School*, in Clarksburg, West Virginia, has installed a HandReader to control access to its critical mechanical room, the heart of the school’s physical plant. Custodians and other authorized school personnel now must swipe their identification badge and scan their hand to enter the room.

Biometrics Ensure Identity

Incorporating biometric devices into the system is the only certain way of ensuring that the person being allowed entry is actually the authorized person and is permitted to have access during that time. Nothing else ties a person specifically to a credential. However, a biometric device is only as good as its reliability. Ideally, it should allow a person holding a credential to enter 100%

of the time during authorized hours, and it should reject unauthorized requests with the same certainty. In practice, a false reject can be just as much of a problem as a false acceptance, and some biometric methods are more reliable than others.

Hand geometry systems use the size and shape of the hand and fingers to verify identity. Length, width, thickness and surface area of the fingers and hand are measured, analyzed, and the unique features are stored in a template, which is used for subsequent verification.

According to Frost & Sullivan's World Biometric Report 2002, hand geometry continues to be the dominant biometric technology for access control and time-and-attendance applications. It is especially well-suited for handling large volumes of transactions where a high degree of reliability is required.

Fingerprint readers use the unique pattern created by the ridges and valleys of the fingerprint characteristics for identification much as law enforcement agencies have for decades, but they automate the process and integrate fingerprint capture and associated algorithms for template creation into their terminals. Fingerprint recognition works best when applied to smaller populations.

Although biometrics may deliver more security than most educational facilities need, remember that card access systems, PIN numbers, keys or other credentials still allow anyone who possesses them to gain entry. They can't provide total control because they can be lost, stolen, borrowed, copied or otherwise compromised. Also, research shows that people who pose a security threat typically will follow the path of least resistance and choose the easiest targets. By installing an access control system geared to your security needs, you can deter such occurrences up front and reduce the possibility of security breaches, along with their associated problems and costs.

If your budget will not accommodate the full access control system you want or need, a system with modular capabilities will make it easier to increase a facility's level of security and move it up the security pyramid. If the products available in a proposed system allow it to be upgraded without replacing the existing equipment, cost savings will accrue in hardware, installation, troubleshooting and possibly maintenance.

Identify the Weakest Link

No matter how sophisticated your access control system, it is no better than its weakest link. The higher the level of security required for an area or a school, the more important it is to have the strong support of the levels beneath it. All the electronics in the world won't stop an intruder if the lock on a door doesn't latch properly.

Better security can start with a security and safety needs assessment by a qualified security consulting firm. This should be the first step in taking a proactive approach, rather than one that is reactive. This type of assessment, performed by an outside party, focuses on the school's door openings, key controls, credentials, links with time-and-attendance and personnel scheduling, and other risks inherent with the overall access control system.

Throughout the search for security, it is important to remember that the final choices must comply with local building codes, fire codes and Americans with Disabilities Act guidelines. These factors may add to the complexity but must be considered as part of the solution. A professional

security consultant can be a big help in achieving the highest level of security while also ensuring that the facility is code-compliant and ADA-compliant.