83-05-10.1 Physical Access Control

Dan M. Bowers

Payoff

The objective of physical access control is not to restrict access but to control it. That is, the data security administrator should know who is granted access, when access is granted, and even why access is granted. In this article, physical access control options are discussed in terms of functions, effectiveness, and cost.

Problems Addressed

Access control devices and systems comprise an important part of every security system. Even the simplest single-door access control system includes at least an electric strike to automatically unlock the door, a timer to make sure that the door does not stay open all day, and a bell or light to indicate when the door is opened or that it has not reclosed properly. In a large-scale security system there may be intrusion alarms, exit alarms, closed-circuit surveillance, guards and patrols, physical barriers and turnstiles, and a variety of other devices and systems. The combined advantages of these elements constitute an effective physical security system.

Various access control systems and devices are now available whose combined advantages constitute an effective physical security system. This article discusses these systems and devices and assists the data security administrator in determining the expenditure required to address the company's level of risk.

Designing the Physical Access Control System

The functions of the physical access control system within the total security system are in the following phases of the security process

- Deterrence—The visible presence of a card reader or keypad can deter the potential penetrator who is looking for an easily picked lock.
- Prevention—The system will allow the door to be unlocked only for authorized persons.
- Detection—The system will sound an alarm if entry is forced.
- Apprehension—The system can provide a list of suspects if the perpetrator is believed to be an employee of the company.

All access control systems use three basic techniques to control entry through a door; these techniques have been described as something a person knows, something a person has, and something a person is or does. Physically, these three security methods are stored-code devices, portable-key systems, and physical attribute systems.

A stored-code device is an electronic form of combination lock, commonly manifested as a keypad access control system. It requires the person desiring entry to enter a specified sequence of numbers (something the person knows), which the electronic circuits must recognize.

Portable-key systems commonly take the form of card access, which involves the use of a plastic credit card (something the person has) on which is encoded a number that is electronically read when the key is inserted into a slot, groove, or hole. Proximity access control is a form of portable-key system using devices that need not be inserted into a reading mechanism and can be electronically read at distances of up to several hundred feet.

Physical attribute systems, sometimes misnamed biometric systems, measure some unique physical or behavioral characteristic (something the person is or does) to identify a person.

Combinations of these access control techniques can greatly increase the security provided by any one of them alone. For example, a card reader plus a keypad requires the entrant to both possess the card and know the code; therefore, a lost or stolen card or a number observed from the keypad will not grant access to a perpetrator.

A number of other features can also contribute greatly to both the security and the reliability of an access control system. They are as follows:

- Tamper alarms—If a perpetrator can gain access by smashing or opening the electronic controller, the security provided is obviously diminished. The controls must not be accessible from the unprotected side of the portal, and a sensor should be provided that will create an alarm in the event that the unit is opened or attacked.

- Power-fail protection—Units are frequently provided with internal batteries so that the access control device will continue to perform its normal function for a period of time even if the power fails or the power lines are cut.

- Code changes—A very effective, inexpensive, and lamentably little-used method of increasing the security provided by an access control system is the frequent changing of the access codes. Changing a keypad code is easily accomplished by moving some switches in the control unit. Changing the code on a card access system or other portable-key system ranges from easy to impossible and may require issuing new keys, just as would be the case if an old-style mechanical lock were changed; this should be examined when considering the purchase of a system.

- Logging—One of the most valuable attributes of an access control system is the ability to maintain a record of all activity (e.g., when each door is opened and, if individually coded keys are used to provide personal identification, who opened it). This feature can provide an excellent starting point for any post-incident investigation.

Keypad Access Control Systems

Keypad access control systems are an electronic form of the combination lock; they require that a correct sequence of numbers be depressed on a set of pushbuttons in order to open a door or other mechanism. Most keypad devices are electronically controlled, with the sequence of buttons pushed being decoded by electronic logic circuits or an internal microprocessor and the door being electrically unlocked. There are also keypad-access products that are fully mechanical, wherein the pushbuttons operate internal elements similar to the tumblers in a mechanical lock, allowing the bolt to be manually operated. Sometimes the pushbuttons are recessed or hidden behind a privacy panel to deter observation by an outsider of the entered combination; in most cases, however, the keypad hangs out in the open for all to see.

The level of security provided by any combination-lock device depends considerably on the number of code combinations that are available, since a popular method of compromising these devices—second only to watching which numbers are entered is to try all of the combinations. This may seem like an impossible task; but if there are 1000

possible combinations (a popular number, which is the number of combinations used for most remote-control garage door openers), and a different combination is tried every two seconds, the correct code is likely to be discovered within 17 minutes and is absolutely certain to be known within 34 minutes.

The number of possible combinations depends on several parameters:

- The number of keys (pushbuttons) provided.
- The number of digits that comprise the code.
- Whether a digit may be repeated in the code sequence.
- Whether multiple keys may be depressed at one time.

Most keypad access control systems use a 10-key pad and a 4-digit repeating, nonmultiple code, which provides 10,000 combinations. However, there are keypads that have from 5 to 16 keys and provide 2- to 10-digit codes, and the number of code combinations ranges from 25 to over 4 million.

The following defenses exist against those who attack a keypad access control system by trying all of the possible numerical combinations:

- Number of combinations—The greater the number of combinations, the longer it will require to try them all.
- Frequent code changes—A large number of combinations may require the perpetrator to try them over a period of days or weeks; changing the code during that period will require the attacker to begin all over again.
- Time penalty (error lockout)—This feature deactivates the system for a period after the entry of an incorrect number, so that unauthorized persons cannot quickly try a large number of combinations.
- Combination time—When this option is used, the system limits the amount of time that is allowed for entry of the combination on the principle that authorized persons can readily enter the numbers, and anyone taking excessive time is probably up to no good.
- Error alarms—When three incorrect numbers have been entered in succession, these alarms are activated to provide an alert that someone may be trying a large number of combinations. An error alarm also can completely deactivate the system for a period.

Keypad Options and Features

The standard means of keypad access control for a door consists of the keypad and its electronic controls, connected to an electric door strike. Some of these keypad access systems are self-contained and standalone and operate a single portal using a common code. Others are connected to a central control computer that can control a multiplicity of portals and may also provide other sophisticated features. The more features they have, of course, the more expensive they are.

The following features and options are available with keypad access control systems, and their availability in one form or another may be an effective method of evaluating different products and manufacturers:

- Code storage—The keypad codes must be stored within the electronic control unit by either mechanical means, such as jumper wires, rotary switches, or slide switches, or by electronic means, such as solid-state memory that is sometimes programmed from the keypad itself or sometimes by a portable programmer that is plugged into the keypad controls. The user can almost always change the codes in a few minutes. When the codes are stored electronically, there must be means provided for surviving a power outage(e.g., battery backup or static memory); otherwise all units will have to be recoded after the power has been restored.

- Master keying—With this option, individual codes are assigned to doors, and a different master code—usually in the possession of the Security and Maintenance Departments is able to open all doors.

- Individual identification—A separate code number is provided for each person who may access through the portal.

- Logging—An electronic record is kept of the time of all accesses and the identity of each person if the individual identification feature is provided.

- Visitor's call—A special button may be designated so that persons who do not know the combination may request entry.

- Housings and packaging—Weatherproof units are provided by many manufacturers, since many units must, unsurprisingly, be used outdoors and in bad weather. There are also attractive indoor units, and there are keypads that have lighted or glow-in-the-dark keys.

Costs of Keypad Systems

Keypads, like mechanical locks, will provide good protection against opportunists and amateurs. Used alone, they are vulnerable to the professional and the insider, but in combination with other devices they can be very effective. The cost of a simple, single-door keypad access control device begins in the$100 range for a mechanical or a simple electronic keypad and door strike. Good commercial-grade protection will range from $200 to $300 per door.

Portable-Key Access Control Systems

A portable-key access control system admits the possessor of a device that contains a prerecorded code; the device is inserted into a reader, and if it contains the code that the electronic controls for the reader require, the portal is unlocked. This process is no different in concept from the ordinary metal key and lock. The modern systems, however, use keys that are more difficult to duplicate; and these systems can provide complex logic, control, identification, and logging functions that a simple key does not. It should, however, be recognized that there are versions of the metal key and lock that provide at least as much security as some card access systems and at comparable cost.

The plastic, wallet-size card is the most popular credential used in portable-key access control systems; the second most popular device is a plastic key-shaped token, some versions of which are small enough to fit on an ordinary key ring. There are also standard metal keys with magnetic strips or electronic chips attached, metal cards of various shapes and sizes, and various metal and plastic tokens, pens, and even a finger ring.

The form of the device is not high on the list of factors that the user should consider when choosing an access control system. On the one side, there is merit in selecting a

Previous screen

standard form so as not to be dependent upon a single vendor's unique product. The other side of that coin, of course, is that a device that is not possessed by everyone on the street confers additional security.

Coding Methods

A wide variety of techniques and technologies are used to store the access code on or in the portable key. Early systems used the most convenient technologies then available, such as bar codes like the ones now used by the scanning machines at the grocery checkout counter and Hollerith-punched cards, which were then the backbone of all commercial computing operations. There were also cards that contained electronic circuitry and were touched to the reader mechanism to make electrical contact for reading. Modern versions of these kinds of card access systems are still available.

Most cards currently in use are magnetically encoded, and there are three basic types. The magnetic stripe card, like the bank card and credit card, has a magnetic stripe on one side. The code is recorded magnetically onto the stripe and can be read, erased, and altered using conventional magnetic tape technology. The second type of magnetic encoding uses bits or wires of magnetic material embedded into the card during its manufacture, which are read by an array of magnetic-sensing heads that determine whether there is a bit at each of the possible positions. The third type of magnetic encoding uses a sandwich construction with a sheet of magnetic material in the center of the plastic card; spots can be magnetized or not on the various positions of the sheet, thus creating coding that is read by a magnetic head.

A new access control token is becoming popular that is the size and shape of a coin and has a solid-state circuit containing the code. It can be attached to a card, key chain fob, or other device and is read electronically by touching it to a reading contact.

Another trend in card technology is the smart card, which contains a computer chip with memory that can store both the access codes and reams of additional information. Smart cards may someday be in widespread use for many purposes, including serving as a pocket data base containing medical and other records, but they are not currently popular for access control.

The number of different coding combinations possible in an electronic access control system is determined by the number of digits that can be encoded on or within the access control device. Most devices offer at least ten decimal digits, and many offer twenty to thirty, which provide from millions to millions of millions of code combinations. This large number of combinations effectively eliminates the possibility that any encoded key will work in a reader other than its own. It also provides the capability for personal identification coding, through which an access control system can regulate the access privileges of each person by portal, time, and day. In addition, it enables keeping of an access log that can provide a list of all persons who entered through a door and when, which is an important resource for an investigation after an incident has occurred. With individual identification, individuals and cards can be instantly deauthorized from the system when cards are lost or individuals are terminated or deemed to be no longer trustworthy.

Changing of the access codes, which was described previously as a procedure that can significantly improve the security of an access control system, can be problematic with portable-key systems. Users can recode their own cards or tokens with a magnetic stripe or magnetic sandwich system and even with the smart card, but the equipment required to do so will cost thousands of dollars. The other coding types cannot be changed.

A portable-key system cannot be defeated even by a professional burglar without a working key; however, once someone possesses a working key (which a pickpocket, purse snatcher, or mugger could easily steal), it can be duplicated with an ease that is largely determined by the encoding mechanism. Optical bar codes and Hollerith punches

are clearly visible, recognizable, decodable, and duplicatible by any person or organization with a little know-how. Magnetic stripes require more expertise and equipment but do not pose a problem for the professional with some equipment and resources; the specifications are published and anyone with $2000 or so can buy an encoder. Embedded materials provide a higher level of security, but analytic methods and instruments are available that can detect and duplicate any kind of code.

Reading Units

Reading units for most forms of portable-key devices require movement of the card or other device past a reading head. For key-shaped devices, this is usually accomplished by inserting the device into a hole, just as with a conventional key. The three basic types of card readers are:

- Slot readers—The card is inserted into the reader and removed, sometimes manually and sometimes using a motorized device.
- Swipe readers—The card is grasped by its top and manually moved through a slot containing the reading mechanism.
- Flat surface reader—The card is placed onto this device for reading.

Some attractive weatherproof units are available for outdoor use. The electrical power required to operate the readers must in some models be provided at the door; other manufacturers provide their own distribution from a centralized reader control panel.

Types of Systems and Costs

Like keypads, portable-key access control systems come in both standalone and centrally controlled versions. Standalone portable-key access control systems provide a self-contained unit at each portal; because of the logistical difficulties of maintaining separate lists and logs in each unit, standalone systems tend to have none or a limited number of sophisticated features such as time-and-day control and individual identification and logging. In a centrally controlled system, all files of access privileges and identification codes as well as logs of activity are stored in a central computer, and ID and access information is transmitted to and from the card reader at the portal.

Portable-key systems provide good protection against opportunists and amateurs. They also can be made difficult to defeat for all but the highest level of professional, and with logging they provide effective deterrence against the insider. The cost of a simple, single-portal, portable-key access control system, including a door strike, can be as low as $200 for a really rudimentary solution. An intelligent single-portal system with some individual ID and time-period control will be in the $500 to $1000 range plus installation. Centrally controlled systems generally run $1000 to $1500 per door plus $2000and up for the central electronics, which is frequently a PC-class computer. The plastic cards and tokens are in the $1 to $4 range.

Key-Plus-Keypad Systems

Pushbutton access control devices are simple, reliable, and relatively inexpensive, and the key to them cannot be lost or stolen. However, the key can be observed, deduced, or told to another without penalty, and there is usually no personal identification capability: all persons who know the code look alike to the code recognition unit. Card and other portable-key access control systems can have personal identification and are pickproof;

however, cards can be used by nonauthorized persons who come by them through loss, collusion, theft, or counterfeiting.

Key-plus-keypad systems combine the positive attributes of both of these simpler systems. The person requesting admittance must possess the portable key and must know the numbers to depress on the keypad. The numbers may be the same for every entrant, or each person may have a different code to remember, or the code can be derived from information encoded on the portable key or related to today's date, and so forth.

These systems can become expensive, but they provide the most effective means of electronic access control for those who are at a high level of risk. For example, the magnetic-stripe card, for which the specifications and an encoder can be bought through the mail, when combined with keypads and PINs has become the single most accepted personal identification credential for controlling access not only to physical facilities but also through Asynchronous Transfer Mode to our bank accounts.

Proximity Access Control Systems

Proximity access control systems perform the usual function of unlocking a portal using a device like the portable key but do not require any physical contact between the coded device and the reading mechanism. Some proximity systems operate like card access systems without the necessity of inserting the card into a reader; others are keypad systems without wiring between the keypad and the access control system. Some are automatically sensed when they come into the vicinity of a reader; and some require a deliberate action, such as pressing a button, by the person possessing them.

In the usual card or keypad system, communication of a code from the user to a reading and code-recognition mechanism takes place electrically or magnetically. In a proximity system, it is accomplished through electromagnetic (which includes RF and radio), optical, sonic, or other wireless transmissions.

The most familiar form of proximity access is in a garage door opener: The user carries a token into which has been set a code of his or her own choosing, and on command (by pushing a button on the token) the code is transmitted by radio to a controller within the garage into which the same code has been set. Upon recognizing the correct code, the controller turns on a motor that cranks the garage door open or closed; similar devices are available for ordinary doors.

Types of Systems

There are two basic types of proximity systems:

- User activated—The user initiates transmission of the code to the system (such as with the garage door opener) using a portable device that incorporates a battery power source. The two types of user-activated systems are as follows:
  - Wireless keypads—The user depresses a sequence of keys on a keypad, and the coded representation of each key is transmitted to the system; a TV remote control works in this way.
  - Preset code—The code is fixed in the device by means of internal jumpers or switches, and the user depresses a single button to cause the code to be transmitted. Some systems have more than one button and can transmit more than one code. The garage door opener is a present-code system.
- System sensing—The system senses the presence of a coded device without the user having to perform any action at all. These types of proximity access control systems

operate over a wide range. Some require power from an internal battery, and some absorb power from the RF field of the interrogating system. The several types of system-sensing systems are as follows:

- Passive devices—These devices contain no battery; they sense an electromagnetic field that is continuously transmitted by the reader and reradiate at different frequencies using a number of tuned circuits on the portable device.

- Field-powered devices—These devices contain an active electronic circuit, complete with code storage electronics, a digital sequencer, and an RF transmitter, along with a power supply circuit that extracts electrical power from the field transmitted by the reader.

- Transponders—These portable devices are two-way radio sets containing a radio receiver and transmitter, code storage, control logic, and a battery that powers it all. The reader transmits an interrogating signal that when received by the device causes it to transmit the access code.

System Applications

Proximity cards and tokens have widespread use in business and industry. Coded tags are attached for noncontact identification of articles moving through a manufacturing process or stored in inventory. Animal identification both for wildlife conservation purposes and for domestic accounting purposes is also an important application. In addition, automated, noncontact recognition of vehicles is being used for access into garages and for automated toll collection. Proximity ID cards are becoming one of the most popular forms of card access control for people in business and industry. The simplest form of system-sensed passive proximity token is a garment tag that sounds an alarm if an attempt is made to the garment.

Features and Functions

The features and functions that are important when evaluating proximity access control systems are the same as those that are important in card access, with a few additions because of the noncontact nature of proximity. Some of the parameters to be considered are as follows:

- Code capability—Top-end systems provide millions of different codes, but some systems have considerably fewer.

- Individual identification—All commercial proximity access systems provide individual identification for tens of thousands of people. Some simpler systems and residential-class products offer the capability of identifying only a few dozen people; and many others, such as the garage door opener and the panic token, have no multicode personal identification capability.

- Battery requirements—Batteries will last for at least a year, but just as with a wristwatch, calculator, and TV remote control, they will periodically need replacement.

- Sensing distance—The distance at which a proximity system can be triggered varies from one inch to hundreds of feet. Those systems without batteries generally have sensing distances of three feet or less.

Previous screen

- Form and size of device—Some proximity access control products are like credit cards, some are the size of a cigarette pack, and some fit on a key ring.

- Code changes—Passive cards and most field-powered devices have codes that are embedded and cannot be changed. Some of the other devices allow changing of the code through internal switches or jumpers or through use of a separate programming unit.

- Concealment—The readers for proximity systems can be installed so that their presence is not obvious, since there is no need for accessible and visible readers. This, however, affects only amateur adversaries; the professionals will readily deduce or detect the presence of the system.

- Physical protection—Since RF waves pass readily through sturdy materials such as cement, wood, brick, and glass, a proximity access control system can easily be protected from assault and vandalism by placing the reader behind such a barrier.

- Costs—The cost of proximity access control systems with personal identification and other upscale features are similar to those for the high-end card access systems, that is, in the range of $1500 per portal plus a central control unit. Costs of the portable tokens vary widely: The passive field-powered cards (which require the expensive readers) are in the$5 to $8 range; battery-powered devices run from $20 to $50.

Access Control Systems Based on Physical Attributes

The ultimate access control system would uniquely identify a person and admit that person and only that person independent of whether the person possessed a particular coded card or token and/or knew a particular code. This ultimate identification system would be based on one or more physical characteristics. Nonautomated physical attribute identification systems have long been the primary method of verifying the identity of a person: the signature (as used on personal checks and credit card slips); the fingerprint (as used by the FBI); pictures (as used on ID badges, passports, driver's licenses, which have become the preferred form of identification for banking and credit transactions);and, to a limited extent in some criminal proceedings, the voiceprint. Digital Network Architecture may be next.

Types of Systems

The equipment that is now available for access control in some cases measures the physical attributes that are well-known and of accepted legitimacy, and in others relies on attributes that the manufacturers themselves have represented as being unique. A discussion of the current offerings follows; other techniques will doubtless come and go.

Facial Recognition.

There has never been a fully automated system using the face as a physical attribute, although for twenty years semiautomated systems have been available that store a person's picture on microfilm, videotape, videodisk, or digital memory. Such systems are a sort of nonportable picture badge, with the image retrieved by an automated identification means such as a card or a PIN. Another simple and economic form of face-based nonautomated access control that has become popular is the video intercom, which was originally developed for entry lobbies in apartment buildings. This device allows the occupant to both speak with and see the face of a visitor before opening the door (usually electronically).

Previous screen

Signature Comparison.

The signature is the basis for personal identification in hundreds of millions of financial transactions every day. There are machine-assisted methods for presentation of a stored signature image to the bank teller, but these are not used for access control.

There has never been a fully automated system for signature comparison, although for twenty years there have been fully automated systems that are based on the manner in which the person writes the signature (e.g., pressure, acceleration, speed), rather than on the appearance of the finished signature.

Fingerprint Comparison.

Fully automated fingerprint access control systems have been marketed for 25 years by a continually changing series of unsuccessful vendors originally driven by work for the FBI and the Air Force. The technology is similar to that used in the FBI fingerprint search operation, which makes 15,000 searches a day through a file of 25 million prints.

Fingerprint-based access control can be installed for a price that is little more than that for a top-end card access or proximity system.

Hand Geometry.

Hand geometry as a unique physical attribute stems from a 1971 study by Stanford Research Institute on the efficiency of manufacturing and inventorying gloves for Air Force pilots. An access control system based on this physical attribute was introduced in 1972. It was successfully sold and widely used under the aegis of several companies, but was abandoned by a major player in the security electronics field in 1988 as a business area not worth pursuing. New systems are on the market today, at prices that are competitive with those for card access systems.

Voice Recognition.

Voice recognition was the subject of extensive research activities in the early 1970s, but no serious voice-based products were marketed until the late 1980s. Voice input has a natural cost advantage over other physical attribute-based access control systems in that the data-entry mechanism is an inexpensive telephone handset and the workings are all electronic. However, it has suffered from suspicions of unreliability and fear of being easily outwitted by recording and playback devices, and from government reports openly stating these concerns. There have been a number of products on the market from time to time, at prices competitive with those for card access systems. One rudimentary form of voice-access control is the telephone entry system, which is actually a machine-assisted voice-plus-keypad system. Like the video intercom, it is intended for multi-unit residences and requires that the person on the inside recognize the voice of the prospective admittee.

Blood Vessel Patterns

Other systems analyze the patterns of blood vessels on various portions of the human anatomy. One system that was introduced in 1983 is based on the conclusion of a 1935 medical paper that the pattern of the blood vessels on the retina of the eye is unique. Another uses the blood vessels on the wrist.

A question is legitimately raised about whether any one physical attribute provides a more dependable basis for identification than the others. Fingerprints certainly have the most solid legal precedent and endorsement through long-term use, and there is only one chance in a billion that two randomly selected fingerprints will match. Signatures are also well accepted as identification for financial transactions. Voiceprints have acquired some legitimacy in the courts. Faces have never been measured in an automated identification

system. The uniqueness of the other attributes is validated only by the claims of the companies that sell the equipment. In practice, however, all of the products have accuracy rates in the one-in-a-thousand category because of the problems in measuring the attribute, and no attribute has been demonstrated to be superior.

An Assessment of Physical Attribute Access Control

Automated systems using physical attributes to identify persons have been offered for 25 years by dozens of companies that along with their products have come and gone, and scores of new products are on the market today. A major problem with these systems has been cost: $15,000 per portal in the 1970s was not uncommon, and costs below $5000 per portal have only recently become realistic. A second problem has been the unavoidability of errors, because even though the physical attribute itself may be unique to the person, the measurement of it is imprecise and will differ from one trial to the next. The error rates have improved from 1% to 0.1% and better over the past twenty years.

The kinds of things that can cause errors are easy to understand. Fingerprints can become difficult to read in extremes of temperature and humidity, when worn down from laying bricks, or when scratched from pulling thorny weeds. Voiceprints can be affected by sinus or throat conditions and mental stress. Some individuals have difficulty with certain kinds of systems; for example, some elderly persons have virtually no fingerprints. There is also legitimate concern that attributes can be counterfeited by such means as a plastic mold of the finger, a voice tape player, and forgery of signatures.

The error rate of a physical attribute system can be much improved by combining it with an identifying card or PIN , because the system is then required to determine only that the fingerprint does or does not match the single fingerprint(or face, hand, voice, eye, signature, etc.) that is on file for that person rather than whether or not this fingerprint exists among a (possibly huge)file of acceptable persons. This system thus created is a combination system either attribute plus card or attribute plus keypad; and as discussed previously, combinations of access control systems always provide greatly increased security over either of the single systems alone.

Another major problem with physical attribute access control systems involves the long-term viability of the vendors (i.e., will they be around to fix it when it breaks). These systems have a consistent 25-year history of commercial failure, a history that is not limited to the two-guys-in-a-garage operations but includes prominent billion-dollar computer and electronics companies. The company that sold the product today may not be in the business next year.

The future of automated access control systems based on physical attributes is easy to predict: They will ultimately be the predominant means of identification, but this will almost certainly occur in the next century.

Electrical Locks

Regardless of the sophistication of the access control technology, a number of seemingly mundane devices exist that can have a great effect on the security of the system if they are properly designed. Electric locks are devices that keep a door locked or allow it to be opened under the control of an electrical signal. They are an essential ingredient of an access control system. The door is held secure until an authorized identification means (e.g., card, fingerprint, keypad) is validated by the system, and the door is then released for an amount of time sufficient for a person to enter.

Methods of Electric Locking

A discussion of several of the methods by which electric locking of standard hinged doors is accomplished follows.

An Electric Strike.

An electric strike mounts on or in the door frame and operates by an electric solenoid that releases a movable striker plate so that it may rotate out of the way of the bolt, thus allowing the door to be opened without retracting the bolt. The door can also be opened from the inside at any time by turning the knob, which retracts the bolt while the striker plate remains in place. A standard-duty electric strike can be purchased for $30 to $50, but the heavy-duty, commercial-grade versions, some available in stainless steel, will run $175to $350. To this must be added the cost of the special power supplies that are required.

An Electric Deadbolt.

An electric deadbolt operates in reverse to the electric strike. The door strike in or on the frame remains fixed in place, and the bolt is electrically moved in and out of the strike using a solenoid or in some cases a motor to unlock the door. On some units, the bolt can also be moved using a doorknob or lever; in others, this is not possible. Prices begin around $80 for the mortise models, $120 for the surface mounts, the $260 range for heavy-duty models, and $500 for a heavy-duty double bolt, plus the cost of the power supply. Another consideration is that since the bolts are mounted on or within the door itself, power must be run onto the door from the hinge side, using transfer hinges or door cords. These locks are more resistant to attack than are electric strikes.

An Electric Latch.

An electric latch electrically releases an antishim device similar to that on mechanical dead-latch locks; it operates entirely within the strike cutout on the door frame, thus requiring no messy wiring on the hinge side or through the door. They run a couple of hundred dollars each.

An Electromagnetic Lock.

An electromagnetic lock employs an electromagnet that is attached to the top of the door frame and a metal plate that is mounted onto the door opposite the magnet. When the electromagnet is energized, the door is held closed with a force that varies from 500 to 1500 pounds, depending upon the model. Prices range from $250 for a 500-pound version to $360 for 1500 pounds. Control and power units and fancy options will add several hundred dollars more, and installation costs in the region of of $800 per door are not uncommon.

Selection and Installation

Selection and installation of an electric lock is reasonably straightforward, but there are two situations that present special problems:

- Glass doors—Since glass doors (including the double sliding versions that are popular in homes) have no cutout, no place to put a bolt, and no striker plate, frequently the only method of locking them is to use an electromagnetic lock with the metal plate bolted onto the glass or the frame that surrounds it.

- Double doors—Wooden or metal double doors are locked at their center point. A center stile requires two locking mechanisms, with wiring running through it if electric strikes are used or through both door leaves to the hinge side if electric deadbolts are used. Usually the stile is made removable to accommodate the movement of large items through the portal, and this will require wiring that can be temporarily disconnected. Double doors with no center stile present special problems because pressure at the center will easily lever the doors open; electromagnetic locks or vertical-pin locking mechanisms are the only secure method of locking these doors. The most economical means of securing double doors is to pin one leaf with vertical locking pins that can be manually opened when needed, and use only the other leaf for everyday access.

Power and Operation

The different kinds of locks present different requirements for wiring and supporting hardware. The electric strike and the electromagnetic lock are entirely wired within the door frame, since their active components are mounted therein. Nearly all models of electric bolts operate within the door itself, and wires therefore must be brought onto the door using an electric transfer hinge or flexible door cord and transferred to the other edge of the door using a hole bored crossways through the door. This procedure, which is called “coring,” is not a trivial task. Commercial door manufacturers can supply a cored door.

Electric locks are usually powered by voltages of 12V or 24V and are available in either Alternating Current or Direct Current. They require holding current in the vicinity of 200 to 300 mA, less than 10 watts, although some go up to nearly 1 ampere; however, the initial surge current required to operate some models can go up to 20 amperes. The cost of a transformer or rectifier capable of providing power to a single lock is $20 or so. AC power is generally cheaper to provide than Direct Current. However, if the security requirements are sufficiently high that the electric locks must be kept in operation even if the AC power has failed (i.e., through the use of a backup battery), then DC powering is essential because there are no Alternating Current batteries.

Installation of electric locks may be in either the fail-open or fail-locked(a.k.a. fail-secure) configuration, which refers to the condition open or locked that the lock is in when power is absent. In the fail-locked configuration, the door cannot be opened from the outside if the power fails. In the fail-open configuration, anyone can get into the facility by cutting the power lines. Installation of backup batteries, though it adds cost, can remove both of these problems.

Emergency Egress

An essential requirement when selecting and installing the locking mechanisms that will form a company's first line of security is that there must be straightforward and unimpeded egress under emergency conditions, such as when the building is on fire. Electric locks present some unique considerations with respect to emergency egress. The electric strike, which is the most popular, is no problem, since retracting the bolt opens the door. The good electric bolts and latches are engineered so that turning the knob or lever will open them. Some motor-driven locks, including the garage door opener, cannot be unlocked without power. Electromagnetic locks are opened by means of a simple switch that cuts off power to the lock, but finding and operating the switch in the dark may be a problem.

Fire and life safety code requirements vary from state to state and from city to city, and the security system designer must integrate those local requirements into the total security system. Accommodation can and must always be made between security requirements and safety considerations.

Previous screen

The Door Protection System

Most break-in attempts are attacks on the surroundings of the lock, rather than on the access control system or the lock itself. All links in the protective chain must be of equal strength, and an understanding of the equipment that, in addition to the lock and the high-technology card or keypad system, makes up the complete door protection system is therefore necessary. This ancillary equipment is commonly classified collectively as “door hardware.”

The center of the system, of course, is the door itself. Most good commercial doors can be penetrated by a moderately equipped burglar in under 30 seconds. Hardening of doors with steel plate and fiberglass fill results in products that claim, for example, to require 1.5 minutes to penetrate using explosives and to repel small arms fire up to .357 magnum and 7.62 NATO rounds. Penetration protection of up to thirty minutes can be obtained with a grid of I-beams on or within the door. These Herculean and unattractive measures are seldom appropriate.

Door hardware includes certain equipment that is always present (e.g., hinges, strikes, and knobs) as well as equipment that is used only under special circumstances or in commercial and industrial buildings:

- Hinges—This element of the door hardware is essential to operating the door. Hinges are best mounted in the interior, but since fire codes will require that all emergency doors open out, this is not always possible. Exterior hinges must be protected from attack using continuous piano hinge or knurled-over ends or spot-welded blocking plates that protect the pins.

- Strikes—These are the plates or cavities that keep the door locked by capturing the bolt. They are usually part of the mechanical lock set.

- Door contacts—These are sensors that provide electrical indication as to whether the door is open or closed. They can be integrated into the hinge or separately installed in or on the frame. Door contacts are essential elements of an alarm and intrusion detection system.

- Bolt sensors—these provide electrical indication that the bolt is in the secure position. Bolt sensors are supplied by the lock manufacturer as part of the lock-bolt-strike system, because these three components must all be mechanically integrated.

- Wire-through hinges—Also known as power-transfer hinges, wire-through hinges are used when electrical connection to the door is required(e.g., to drive an electric bolt or sense the switch in an exit pushbar).

- Door cords—These are another means of providing electrical connection to the door. A length of wire, sometimes looped, sometimes coiled, is provided at the hinge side, recessed into the frame, and hidden and inaccessible when the door is closed. The speaker in a car door is connected to the stereo unit using a door cord.

- Automated openers—These are common in supermarkets and other retail stores as well as in entrances that are used by physically disabled people. They are usually triggered by pressure mats or PIR detectors, but a key-operated switch, remote-control unit, or electronic access means may be used. Openers commonly include the complete capability to open doors and hold them open and then close them, and thus are sometimes called door operators.

- Holders—This equipment, which holds doors in the open position, is available in three varieties mechanical, magnetic, and remote controlled. Mechanical and magnetic holders require the door to be manually opened and closed. With remote-controlled electric holders, the door must be manually opened but can be released electrically.

- Closers—This equipment eases the door firmly shut to make certain the bolt latches behind the strike.

- Coordinators—These function as closers for double doors and make certain that the inner leaf closes first.

- Panic hardware—This hardware encompasses the entire class of equipment that allows and controls emergency egress and includes such items as paddle-type exit bars with battery-powered sonic alarms and big red warning signs and attractive burnished-aluminum pushbars with and without control switches within.

Recommended Course of Action

In choosing an access control system, the user must decide what expenditure is warranted to protect against the level of risk, since the access control system will be only one component of the total security and life safety system.

The keypad access control system is simply a combination lock that is quicker to operate, is more difficult to defeat, and has more features and options than the version sold at the corner hardware store. Pushbutton systems should not be used alone in situations in which there is a large risk of collusion, since the code combination can be told to unauthorized persons without penalty. They should not be used in remote or unattended locations, such as vacation cottages, where unauthorized persons may carry out an extended program of trying all of the codes. Keypad-only access control is generally used in low-security applications; yet given a regular program of changing code combinations, error alarms and remote indication, and perhaps a surveillance camera, a relatively high degree of security can be provided. Keypad systems cost from two to ten times more than a common lock, and the increased security and extra features will in many cases be justified.

The card-only (or other form of portable-key) access control system is equivalent to a conventional lock and key, yet it is more difficult to duplicate and can have many additional features. When equipped with personal identification, individual control by time and space, and logging of accesses and attempts, this system is undefeatable by an amateur and by many professionals as well. Card-only systems can cost twenty times as much as a common lock but will provide sufficient additional security to justify that expenditure when the threat requires it.

Card-plus-keypad systems eliminate the loss and theft loopholes in the card-only systems and the collusion loophole in the keypad systems. They cost a little more than card-only systems, but they provide substantially increased security. Further, the increased security afforded by adding a keypad to a card reader in some cases allows the use of simple, standalone single-portal systems rather than an expensive centrally controlled system and the expensive wiring required to wire it to every portal. In these cases, single-portal card-plus-keypad systems can be less expensive than centrally controlled card-only systems.

Proximity-access systems are a very convenient form of portable-key access and are fast becoming the preferred form of access control in new commercial installations. They should be given serious consideration.

Physical attribute systems are a viable top-of-the-line means of access control at costs that are no longer out of reach. However, continuing concerns exist regarding the viability of the vendors at any given time. Used in combination with a keypad or a card reader, these

Previous screen

systems will continue to be used in some special situations for the remainder of this century.

Without adequate attention to the simpler devices such as electric locks and door hardware, the most sophisticated access control system will be only a minor annoyance to the potential penetrator. In addition, the physical structure itself should not be neglected; too many times, doors equipped with $3000worth of access control equipment are set into a flimsy sheet rock wall.

Author Biographies

Dan M. Bowers
Dan Bowers is a consultant for Bowers Engineering in Randallstown MD.