11

Database Management

Development of a security alarm and an access control system for a large facility requires tremendous effort. This effort starts with a list of functional requirements that are translated into a system of alarm and access points. A solidly designed system must be developed and carefully controlled through conception to acceptance. The proper steps that must be taken to ensure an effective security system may take months to complete. The system may incorporate thousands of alarm points and hundreds of badge readers, which will affect all employees in the facility on a daily basis. To assure minimal disruption, a database containing all the alarm points, badge readers, approved access levels and badges must be accurate, well maintained and protected from corruption. This chapter will address the early decisions that affect the system and their impact on the alarm/access control database and the many aspects of protection needed to secure a reliable database.

It is important to review the concept of using and controlling badges, addressed in Chapters 1 and 2. A badge usually contains an image of the employee, employee name, company name, possibly a logo, an access technology and sometimes other detailed

information about the employee or contractor. Their access level is stored in the database. A completed badge is the same as a key to the facility and must be handled and protected like a key. If the badge is lost or stolen, it must be reported in a timely manner. It is the employee's responsibility to control the badge, properly care for it, and wear it at all times when at the facility. The actual badge stock used to manufacture the badge must be safeguarded to assure that it is not stolen or otherwise compromised. Several techniques covered in Chapter 2 will minimize the possibility of counterfeiting the badge.

There are several badge technology options available, but four are widely used in the United States. The most common is the magnetic stripe, because it is fairly reliable, inexpensive, easily programmed, and widely used outside of the security industry; however, being easily programmed can be a potential security concern. Weigand is the second widely used technology. It is immune to most environmental issues and is not field programmable. It is also reliable and very difficult to simulate or copy. The third widely used access control technology is proximity. This technology offers "hands free" access, reliability and readers that can be hidden from view. The fourth technology is actually the second type of "hands free" technology. The fourth type is the contact-less smart card. This is the up-and-coming technology, because it incorporates electronic processing and data storage. All these technologies have their advantages and disadvantages. The technology chosen will, to some extent, affect the badge numbering scheme in the database. There is no perfect technology, so the decision becomes a matter of trade-offs, discussed in more detail in Chapter 2.

Each of these technologies incorporates a protocol which is one of the critical issues to address regarding badges and the database. A protocol is simply a set of binary digits set in a pattern that allows the badge reader interface to understand the data on the badge. Protocols allow communication between electronic devices and people. As an example, English is the human protocol used in this book, and for communication to take place between two or more people, they both must understand the same language and agree to use it. In this case, a badge and the access control system must use and understand the same language or protocol. The badge protocol incorporates a predefined clumping of binary bits that

assign the critical data in the badge. For example, there are normally several bits of data to define a company, a physical site within the company, an employee credential number, and parity bits. The actual employee credential number contained on the badge is assigned to specific areas of access within the company for that given employee. A typical 37 binary bit magnetic stripe protocol uses a specific pattern. The company code might use 8 binary bits, the site code uses 6 binary bits, the employee credential number uses 21 binary bites, and parity uses 2 binary bits. This is discussed in more detail in Chapter 2. The definition of the bit patterns allows a badge reader and its interface and/or field panel to determine if a badge will grant access at a given portal. Badges that do not match the protocol are rejected. Even badges that do match the protocol may be rejected if the employee credential number in the badge protocol does not match the employee badge credential number in the security system database.

Managing and protecting the security system database is a major challenge because it deals with the human interface. Several areas of concern are:

1. Data entry
2. Alarm and badge reader definition
3. Passwords
4. Viruses and worms
5. Backups
6. System redundancy
7. Physical protection
8. Private network/wiring
9. Encryption
10. Training

DATA ENTRY

Data must be properly and correctly input into the database. There are issues with the security alarm database and the access control database. Let's look at several access control and alarm database issues. Normal credential number data entry problems are discovered in a relatively short time because the new badge does not grant the employee access into the facility or a specific area. Many more

subtle issues, however, will not be as obvious. For example, when a new badge is given to an employee because the badge has been lost or stolen, the old badge number must be removed from the database. If the old badge data is not removed, two things can happen: an unauthorized person could find the badge and use it to gain access, and the database will become clogged with useless badge numbers, which is difficult and time consuming to correct at a later date. Security alarm database inputs require accuracy and ongoing modifications. The initial data input should be based upon a standardized input form developed for the particular manufacturer's product, including detailed information as to the definition of the alarm point. For example, the zone on the field panel circuit board, number of the field panel, panel communication loop, and so on must be required data fields on the form. There must be an alarm descriptor, location and response information. If the descriptor lists response personnel, then this data must be accurate and it must be kept up to date. As personnel and phone numbers change, the data must be updated which can be a challenge, particularly if the alarmed areas include classified government projects. These areas have access lists that must be constantly updated.

The identifier used in the database to separate one John Smith from another John Smith must also be considered. In the past, unique identifiers have been Social Security numbers which are unique and easy to incorporate into the database. The main concern with this practice is that of identity theft. The database might be compromised via a network attack or theft of the server/computer on which the data resides. There are several possible safeguards. One is to encrypt the Social Security number so that it is difficult to decipher, but the level of encryption required to assure the level of protection needed is a moving target. The encryption level that was OK two years ago is no longer acceptable. (The requirement is for the encryption to be up-to-date and robust.) Another approach is to physically prevent the theft of the computer where the database resides keeping the server/computer in an area of formidable protection. One such area is a 24-hours per day, 7-days a week (24/7) Security Control Center (SCC) operation. If the database ties to the network, a robust firewall must also be incorporated. The least painful approach to solving this problem is to remove Social Security numbers all together. Social Security numbers are not the

only unique designator for employees. Most companies generate employee numbers for payroll that can be used which are much less sensitive than Social Security numbers. Contractors can still be a problem based upon the fact that they often are not given an employee-type identification number. To address this issue, another approach must be taken for contractors. One such approach might be to use a birthday plus initials or some other variation, such as a modification of their badge credential number.

ALARM AND BADGE READER DEFINITION

The definition of access and access levels is a source of many potential problems. The badge access levels are similar to the old key entry systems. For example, a key might be given to an employee to open his or her office door; the manager of the area might have a key that allows access to his or her office as well as the employee's office; the facility manager might have a key that would allow access to the above areas plus mechanical rooms, the front door and telephone closets. As the access key's use expands to more and more keyways it is referred to as a master key. This concept can grow and grow into grandmaster keys then to great grandmaster keys and even to great great grandmaster keys. Access control systems often utilize this same technique. Badge readers allow access to general areas, restricted areas, and sensitive areas. All employees are able to use readers in the general access areas and possibly some restricted or sensitive areas. In this way, the reader accepts everyone in general access and those that have special access areas, so it is inclusive. In this analogy, a badge that would gain access throughout all readers would be considered the great grandmaster badge.

The other technique used in badge control is to develop an exception list. The exceptions are the badge readers that the employee can use. For areas where only certain groups within the company have access, there are readers that exclude most badge holders. The sensitive areas that would exclude most company employees would be areas such as research labs, cashier areas, and so on. In other words, the badge for a given employee would only work at a list of exception doors and all other doors are excluded. This technique is the opposite approach of the grandmaster key concept. Whether to use the inclusive or exception approach must be

decided during system installation and must be maintained by the system administrator. (The system administrator in most security and access control systems is not what Information Technology (IT) personnel think of as a system administrator. Security uses the term to address the person who oversees and is responsible for the general operation of the systems. IT uses the term to address the person who has total control of the network/database/computer configuration and controls passwords, access to the system and any maintenance performed on the system.) Either the inclusion or exception approach requires documentation, planning and proper data entry to assure the desired operation and data integrity.

To reduce the number of possible variations with either the inclusive or exclusive approach, groups of employees that compose a variation are grouped together. For example, all employees that can only gain access to the main entry points and to the fitness center, for example, might be grouped together. A group that had access to the main entry points, the fitness center and a research lab might be combined together as another group. In this way, groups or classes of access can be changed instead of each individual in the group requiring a change. With this approach, there will still be some unique groups that may contain only one individual. Even with groups being used to define access to badge readers, the process can still become very cumbersome in a large access control system. It is not unusual for these large systems to have hundreds of groups. As readers are added, the approach is to either exclude some groups from using the readers or include groups that use the readers. Keeping the database accurate requires astute administrative controls as well as careful review of the groupings or classes.

PASSWORDS

The database should have passwords to protect it and the database should be segregated into levels of authorization. Passwords allow only certain security personnel to have access to certain areas in the computer/server software. For example, data entry must have password protection and it is best that the smallest number of individuals possible have access especially to higher levels of programming authority. It is best if only one person does the data entry, because the data will be consistent; however, due to system size,

vacation and sick time more than one individual must be utilized. Obviously some level of backup will be required, but having a small group enter the data minimizes errors and assures consistency. Standards must be developed that assure that data is entered in a consistent manner. Data entry is a critical part of protecting the database, and care should be incorporated in selecting the proper person or persons for this job. (The sensitivity of the data in the database should be taken into account when deciding whether to use an employee or contractor for data entry.) Some member or members of Security management should audit the database, audit security personnel who have access, and review data entries on a regular basis. For Security management to be effective in checking the database, it is important that they are well trained on the system. There must also be a policy and safeguards for inputting, updating, controlling and distributing passwords.

One of the major problems with limiting access and assuring security personnel that need and/or have access is obvious when reviewing the policy for temporary badges. Many locations among the company's facilities must be able to enter temporary badges into the access control system. The SCC, lobbies, and badge rooms are often capable of inputting temporary badges for employees who lose or forget their badges. This normally requires the person doing the data entry to "call up" the employee's record in the security database, input the temporary badge, and deactivate the regular badge. This temporary badge must be removed when the employee returns with the old badge. The old badge must be reactivated or, if it is not available, a new permanent replacement badge must be manufactured and loaded into the database. Keeping the database clean and uncluttered with temporary, lost, and unused badges is a major task. The badges of employees who have left the company should be removed as soon as possible after they leave. The situation is exacerbated when it includes contractors. Contractors normally come and go at a faster rate than employees. It is a good idea to limit the "life cycle" of a contractor's badge; a year is normally a reasonable time frame. After a year, the contractor might use the same badge, but the contractor must be reactivated in the database or the badge will no longer allow access. If left unchecked, the number of entries in the database will far exceed the number of employees and contractors in the company.

The password used by each data entry person must be unique and it should be difficult for someone else to guess. The length of the password is normally definable in the security system software and should ideally be at least six to eight alphanumeric characters that would include capital letters and characters (#, *, etc.). The password should be changed on a regular interval—at least once a year. (If a private security network/wiring is utilized, the interval between changing passwords does not need to be as frequent as passwords that would be used on a company's LAN/WAN, because a small number of employees are involved.) Keeping passwords up-to-date, reviewing access levels, verifying individual passwords that are being used, and reviewing the database's integrity are important tasks that should be performed regularly. Security management must take an active role in reviewing the status of the database and associated procedures. It is not what is expected, but what is inspected that counts.

VIRUSES AND WORMS

The introduction of viruses and worms into databases has become commonplace. Ten years ago, few security systems had experienced viruses, but this is no longer true. As mentioned earlier, viruses can be introduced via the company LAN/WAN as well as other physical connections to the nonsecurity world. Viruses have become so commonplace that new terminology is emerging such as "malware" (or malicious software). Instant Messaging (IM) is very popular because it provides flexibility, speed and ease of communication, but it is also very vulnerable to attacks because of its flexibility. Attacks are not limited to personal computers (PC). They now include cell phones and other processor-based electronics and will only increase and become more sophisticated. To protect the security system database from unwanted electronic intruders requires that no software be introduced into the security network without the Security management's approval. A problem that may develop is the installation of software that a data entry person or SCC operator brings into the company and loads onto the security system. The introduction of this unapproved software may not be malicious. It can be as mundane as software to play games during slow periods in the day; however, the negative impact is the same if it

contains a virus or worm. To prevent this type of unwanted software from being loaded onto the security system, the server/computer can be physically moved or the disk, PS2 and CD drives can be blocked off. Some software options provide control to the various input devices on the server/computer through the operating system software such as the different versions of Windows. There are even easier to use and more effective third-party software programs to provide this type of software protection. If the security system is connected to the company LAN/WAN, the potential of an electronic infection expands, and if connected to the Internet, viruses and worms can come from literally anywhere. Antivirus software is a must in these situations because the software searches for "signatures" that match known viruses. The problem with this solution is that antivirus software is reactive; that is, the software patches are sent out to customers after a virus attack has taken place. Another issue is that the antivirus software sometimes makes the security system software run more slowly.

BACKUP

Backing up the database is also a critical process to properly protect the security system. Backups should be performed daily on large systems because many changes are made to the database on a daily basis. The backup can reside on a disk drive or can be loaded to tape. On a weekly basis, the data should be spooled off the tape drive and stored in a physical combination safe close to or within the SCC. A month's worth of tapes should be available at any one time in the safe. The next week the newest tape should replace the oldest tape. The oldest tape should be stored offsite in a secure area. One week storage tape from each month should be stored so that backups can be made as needed to resolve corrupted data files. Backups are kept for several reasons: a computer crash, documentation, employee/contractor investigation, and file corruption. For these reasons, there must be several levels of backup available. The requirements will vary depending upon a specific application. Often, an alarm and access control history is needed for an extended period of time—possibly a year. If the company is a government contractor or the SCC is UL certified, alarm data must be kept for one year.

SYSTEM REDUNDANCY

Even with backing up the database, there is still a remaining weak link—the security system itself. Deciding which parts of the security system must be made redundant is a topic that would require a dedicated chapter. For the time being, it is important to cover a few key issues. A disaster management/business continuity plan should be in place to address various levels of system redundancy for outages. The very worst case of loss would be a total loss of the SCC, but there are lesser levels of loss that should be planned for. Cost and the development of realistic problems that could occur will drive the redundancy plan. It may be that, with minimal expense, most situations can be mitigated to an acceptable level. The level of loss that is acceptable will affect the final plan for the money needed to protect the system against such loss. The cost will also be driven by the system architecture as well as level and method of protection.

Protecting the data transmission lines, the field panels, and database is accomplished by:

1. Physical protection
2. Private network/wiring
3. Encryption

PHYSICAL PROTECTION

The purpose of physical protection is to prevent access and detect unauthorized surreptitious access. Protection can be in the form of conduit, sealed cable trays, locked rooms, and alarms that indicate potential tampering or unauthorized access. Alarms for the electronic field panels would include tamper switches on the panels themselves and motion detectors and door alarms in the protected area. The server/computer is normally located within the SCC and is protected by alarms and sometimes a badge reader. The SCC is normally occupied 24 hours a day 7 days a week. If UL certification is involved, then visitor logs and other protection are required.

PRIVATE NETWORKS/WIRING

Today, many field panels are capable of several types of transmissions. For example, a panel that uses RS485 will by definition have

dedicated wiring back to the server/computer. In contrast, a field panel that uses a LAN network and has a TCP/IP address may or may not be on a restricted private security network. It is best if the network is restricted to security applications only. The IT department typically prefers a separate network to minimize any impact on bandwidth; however, these systems are often connected to the company LAN, so security is sharing the LAN with other groups inside the company. A firewall can provide some protection from penetration initiated on the Internet, but hacking from outside the company is always a possible problem. There are still potential threats from within the company as far as gaining access to the field panels or the actual data contained in the database. Providing physical protection, as previously discussed, will add a level of protection, but internal hacking is still possible. Internal hacking is becoming more of a problem due to employee dissatisfaction and because of the difficulties of protecting against an insider threat. In addition to internal hackers gaining access or causing "denial of access" problems with the security system, there is an additional problem of viruses on the company network. This has been discussed already in this chapter. If the network or transmission system is restricted to security use only and is a closed system, viruses are more easily controlled.

ENCRYPTION

Encryption is often used in conjunction with both physical protection and private network/wiring. Encryption is critical when field panels reside on a company LAN/WAN or if there are government requirements for Department of Defense Closed Areas that must be met. Encryption is a technique that changes the data before it is transmitted and returns it to its original form just after it is received. In its simplest form, adding a random number to the transmitted data and then subtracting the same random number from the received data accomplishes encryption. There are many algorithms that are used to encrypt data. Four well known algorithms are: 1) Skipjack utilizes 80 bits 2) Data Encryption Standard uses 56 bits 3) Triple DES utilizes 168 bits 4) Advanced Encryption utilizes up to 256 bits. Encryption protects data while in transit, because it is

disguised via the addition and subtraction of a random number. This approach may not; however, protect the data in the database, central processor, or the field panel. Special software is available that encrypts data at rest in the database.

Protecting the data transmission via private security networks and encryption, as well as providing physical protection of the field, does not fully protect the database in the central server/computer processor. For instance, there will be requests for access to the database from groups inside and outside the Security department when there is an enterprise security-wide system. For example, the Human Resource (HR) department or a department manager may request pictures of employees, which reside in the database as JPEG files. If this data is provided electronically via connections to the security database, all the precautions previously discussed must be followed.

Another possible request from HR might be to use the badge as part of a time and attendance system. These system databases could be separate or they could interconnect the Security and HR workstations/computers. If they are together, the HR time and attendance computer system must physically connect to the security computer/server. This connectivity poses two potential problems: one is the physical cabling/network issue that has been discussed. The second problem is that another hacking/virus point has been provided. If electronic connections to the security database are made, then all the precautions mentioned above must be in place as well as a one-way data transfer from Security to HR.

If the databases are not physically connected, HR will want to know the badge protocol so that they can use the badge for time and attendance but remain separated electronically. Although it is generally not thought so, the badge protocol is one of the most sensitive security areas to protect and is at the very heart of what makes the access control database secure. The protocol should be a well-guarded secret. In this scenario, there are other approaches to solve the "time and attendance" problem without giving up the badge protocol to HR or the IT departments. As previously discussed, the badge contains a series of data bits, but the way the bits are grouped (protocol) is the sensitive information, so the HR/IT personnel can be provided the total number of bits including any parity information. In this way, the entire badge bit pattern can be read as a unique

credential number without providing the actual protocol. This process allows the badge to work in both systems and still keep the protocol secure. The only problem with this approach is that each badge must be loaded into the HR database individually unless a protocol converter is written and a file transfer is used.

TRAINING

Training is needed for anyone who has any level of password approval to modify the database in any way. As mentioned earlier, there are often different levels of authorization a given password will allow. A real life example is the easiest way to show the impact of poor training and how it can affect the database when the user has only minimal authorization. A large company was in the process of transitioning from one badge technology to another. The first step in the transition was to provide a multitechnology badge for employees and contractors. In this way, when everyone had received a multitechnology badge, the readers could then be replaced with the new technology readers. This required that all employees and contractors have a multitechnology badge so that either the old or new technology reader could be used until the conversion was complete. Since there were too many readers to change, it was necessary for the conversion to be completed on a building-by-building basis. The training problem was with the lobby receptionist who had a password that allowed him or her to supply employees or contractors with temporary badges if they arrived at work without a badge. There were checks and balances in place to assure that the individual requesting the badge was approved to be on site and was indeed that person. The process was for the lobby receptionist to call up the individual's record in the database and replace the badge credential number with the credential number on the temporary badge. The receptionist replaced the credential number with the first database record that was displayed on his or her workstation, not checking to see if the credential number was for the old or new technology. By replacing many of the badge holder's new technology credentials with the old technology used in the temporary badge, the new technology credential number was lost from the database. When the conversion of the actual readers was to start, it was discovered that many of the

employees and contractors could not access the building via the new technology reader because of the way temporary badges were processed in the lobbies.

In this chapter, we have considered the alarm and access control system as a complete security system to help explain the necessary precautions needed to manage the database. There are other databases in other security equipment that will apply to the issues addressed in this chapter. Some of those databases include functional security components such as video switchers, audio switchers, and digital video recorders, and LAN/WAN routers. The database used in all these systems is the heart that provides lifeblood to an electronics security system. All the databases must be properly maintained, updated and protected. Protecting a security system's databases is not a simple process. There are many aspects that must be considered. These aspects include the physical protection of field panels, transmission lines, server/computer, interconnections with nonsecurity computers and the personnel who interface with the database. The approach taken to protect the security system should consider the company culture and the complexity of the system. There will be requests to share information between groups within a company. Sharing JPEG files of employees/contractors, connecting the HR database with the access control system and sharing access control databases between sites within the company, to name a few. This makes protecting the database's integrity more important than ever before. The extent to which data is shared and the approach taken to share the data must be carefully considered. Every link to the database is a possible link to a hostile environment.