

ACCESS CONTROL INDUSTRY BEST PRACTICES

Introduction

Recent questions have been raised about the vulnerabilities of physical access control systems. Unfortunately, some critics, with limited familiarity of the security industry, have oversimplified the tradeoffs between convenience versus security of access control systems. Some have actually sensationalized these accounts and even worse, some have not presented the facts in an accurate manner.

One positive benefit of this is to increase the awareness of the need for a set of “Best Practices” to mitigate the risks of some of these “theoretical” attacks. This article will focus on the best practices that should be followed when choosing and installing access control readers. The audience for this article includes system integrators, consultants, architects and engineers and the end-users of access control systems.

The most important concept to embrace in adopting best practices is that an effective security system uses “layered security.” Simply put, this involves using additional safeguards to make sure that a security failure at one point will be detected at a successive point. For example, a home protected by a burglar alarm might use both glass break detectors and motion detectors to detect when an intruder gains illicit entry through a window instead of a door.

Choosing the Right Reader

There are a wide variety of reader technologies being offered by today’s manufacturers and it is important to make sure that the correct technology is chosen to match the desired level of security. Using a good, better, best grading system will help make the correct choice easier.

Prox technology is a viable choice, especially for sites where there are existing Prox cards in use. Contactless smart cards represent the next generation Prox technology and offer increased security, as well as additional benefits such as multiple applications, read/write and increased memory. But some manufacturers, in an attempt to sell a “universal” reader capable of reading almost any contactless smart card technology, actually disable all of the security mechanisms in order to achieve their goal. These readers, referred to as “CSN readers,” only read the card’s serial number, which, as per ISO standards, must NOT be protected by any read security since they are needed by the reader to be able to detect when more than one card is presented to a reader at the same time. This process, referred to as “anticollision,” takes place before the card and reader mutually authenticate each other. Because the ISO specifications are a publicly available document, details of how this anticollision process works can be used by a perpetrator to build a device to clone (simulate) the serial number of a contactless smart card.

Ranking these three types of readers from the lowest to the highest level of security provided would be CSN readers, Prox readers, and contactless smart card readers using mutual authentication.

Communications Protocol

A reader typically reads a card and sends the card data to another “upstream” device which makes the decision as to whether or not the door should be unlocked (upstream devices include panels, as well as host computers running the access control management software). When the communication takes place using wires, there are many different methods to choose from. The most popular and de facto industry standard is the Wiegand Protocol. This protocol became very popular because it is almost universally supported by almost all reader and panel manufacturers. Although more modern protocols such as RS485, F/2F, and TCP/IP offer more security in the communications, there is less interoperability between different manufacturers of readers and panels.

The best practices described below will increase the security of any communication protocol used by the reader to

communicate with an upstream device. Since often times the reader manufacturer is different than the panel manufacturer, some features of readers described may not be supported by all panel manufacturers.

Protect the Wiring

Installing the security systems wiring in conduits would make it more difficult to compromise without being noticed due to the difficulty of identifying the correct conduit, as well as the additional time required to compromise the wiring in the conduit. Even if the entire wire run is not fully enclosed in conduit, just using conduit for the most vulnerable areas is desirable. Additionally, bundling several wire runs together (ideally in conduit) so that identifying the correct set of wires is more difficult, is also desirable (follow the manufacturer's recommended installations, some wiring such as power may not be recommended to be in the same conduit as data communications wires). Particularly important is to protect the wiring from outside readers that are located at the entrance to a premise.

Avoid the use of readers with built-in connectors that make it easier to swap out a reader and avoid the use of wire-nut connectors to connect the reader wire pigtails to the panel wiring. Instead, connect the wires in a more secure and permanent fashion, such as soldering with shrink-wrap tubing to cover the connections.

Use Security Screws

Always utilize security screws that require special tools to remove a reader and other security components. If the correct tool is not available, then it makes it nearly impossible to remove the reader without causing damage to the screws, which may be noticed – especially if policy dictates that readers be examined on a periodic basis. It also has the effect of making the removal process more difficult and slowing down the removal increases the possibility that the malicious attack will be noticed.

Prevention using Anti-Passback

Another best practice is to program the access control host software to refuse granting access to a cardholder that is already “inside” the facility. This mechanism, sometimes referred to as “anti-passback” is already available in many access control systems. Note that this feature requires two readers at the door – an “in” reader and an “out” reader. One side benefit of using anti-passback is that it prevents a user from using his/her card and others following through the open door, which is referred to as “tailgating”.

Detection -The Second Line of Defense

Buy readers with a tamper detect mechanism that provides a signal when the reader has been removed from the wall. Almost every panel manufacturer provides the ability to monitor this alarm signal and report when a reader is tampered with. If possible, use the correct electrical polarity so that a tamper signal will be generated when the wires are cut. Another method that can be used by installers is to include an additional pair of wires that are connected together through a resistor at the reader. This loop can be monitored by the panel using a technique called supervision, which can detect when the wires are cut, shorted, or other electrical characteristics of the wires are changed.

Immediately investigate tamper alarms even if they are momentary and return to normal. You might actually detect the perpetrator in action or find that a “foreign” device has been installed to intercept and monitor the communications between a reader and the upstream device. If the reader is controlling a sensitive location, such as a perimeter door, have it and the door monitored by CCTV. Some access control systems can automatically switch the viewing monitor to the door with the tamper alarm, as well as tag the video history log with the event for later review.

Many reader manufacturers, such as HID Global, also have the capability of sending “health” messages (sometimes called “I’m Alive” messages) on a periodic basis to the upstream device. This can also be used to detect when the wires are cut and does not require any additional wires to get this protection. If these periodic messages are set to occur faster than it would take to install a rogue device, then the panel would notice the interruption. Ideally they would be set to occur as fast as every second. Monitoring health messages also provides additional benefits since it will detect reader malfunctions. It is better to know when a reader is not working before somebody complains (usually in the middle of the night when they cannot get in the door).

For converged physical access control systems and logical access control systems, “geographic” monitoring is available. If a person has just come in through a door at a site in Buffalo, but is trying to log into his computer in Denver, then obviously there is a problem. Another benefit in converged systems is to not allow a person to log onto his computer if he hasn’t used his card at a perimeter reader. This simple concept will get people to change their behavior and not tailgate when they are denied access during the computer log-on process.

Use Additional Factor Authentication

The use of card readers with built-in keypads means that lost cards cannot be picked up and simply used to enter a facility. It also eliminates the threat of card cloning. Make sure that the password is changed periodically, or if a common password is utilized, change it every day to increase the effectiveness.

The use of biometric readers to ensure that the person presenting the card is actually the same person that was issued the card can be used at doors where a higher level of security is required. A similar solution is to use hand-held biometric fobs that only emit RFID card data after a biometric authentication has occurred. These types of devices, available from companies like Privaris, actually help to increase privacy and cannot be surreptitiously read without the user’s permission since the access control credential cannot be read until the biometric authentication process has taken place.

Mind the Cards

A perpetrator may use surreptitiously obtained cards for nefarious purposes. One way to do this is to claim that a card was lost when it really wasn’t. Make sure the old card is voided immediately. Another way for a perpetrator to fraudulently obtain cards is through “gray” market sources such as eBay® or even legitimate card resellers. There are several best practices to prevent this. First, make sure that only issued cards are valid; don’t have “spare” cards pre-validated and ready to hand out. Some access control systems can also generate a different message than “just denied” for cards number ranges that haven’t been entered in the system. When an illegally obtained card is used, if the message generated by the access control system was “Card out of range” instead of simply “Denied,” it should signal more urgency to be investigated. Similarly, cards using a different data format that are reported as “Unrecognized,” as well as cards with the wrong facility code, are also indications that illegally obtained cards are being used. Therefore, any messages reported by the host access control system with wrong formats, wrong site codes, or out of the range should be immediately investigated.

Another best practice is to use a proprietary format offered by an OEM or one that is exclusive to a particular site, such as HID’s Corporate 1000. Cards with these formats are virtually impossible to illegally obtain, as compared to the industry-standard open-format 26-bit Wiegand format. Some manufacturer’s readers can even be set to ignore “foreign” cards completely, which will also present an obstacle to using cards obtained on the “open market.”

As described earlier, never use contactless smart card readers that solely rely on the card serial number such as CSN readers. Some companies advocate these types of readers because they do not require implementation of security mechanisms, which may not be available to be licensed by that reader manufacturer and add cost.

Conclusion

There are many additional best practices that we have not discussed, such as the use of security mechanisms on the card (like holograms) and other tamper evident technologies, instructing employees not to wear their badges in prominent view when outside the premises, the use of RFID shield devices, and much more.

Following as many of these best practices as feasible, with attention to appropriate levels of security, will result in a system that better fulfills its intended function with less possibility of being compromised.