PROTECTING CONTACTLESS CARD-BASED ACCESS CONTROL SYSTEMS FROM HACKING

By Scott Lindley

Photos courtesy of Farpointe Data

SKIMMING, EAVESDROPPING AND RELAY ATTACKS CAN BE PROBLEMS. BOTH THE READER AND THE WIEGAND PROTOCOL ARE VULNERABLE. HERE'S HOW TO DEFEND THEM.

Radio Frequency Identification devices are typically used as proximity or smart card identification in tracking and access control systems. These systems operate on the assumption that the token is in close proximity to the reader because of the physical limitations of the communication channel.

However, current RFID devices are not suitable for secure identification. They can be subject to skimming, eavesdropping and relay attacks. An attacker can fool the system by simply relaying the communication between the legitimate reader and token over a greater distance than intended. As these facts become better known, there has been a drive by security directors to overcome such shortcomings.

Wiegand is the industry standard protocol commonly used to communicate credential data from a card reader to an electronic access controller. Gone are the days when Wiegand was considered inherently secure due to its obscure and non-standard nature. No one would accept usernames and passwords being sent in the clear nor should they accept vulnerable credential data. ID harvesting has become one of the most lucrative hacking activities. In these attacks, a credential's identifier is cloned, or captured, and is then retransmitted via a small electronic device to grant unauthorized access to an office or another facility.

Let's Review the Threats

First of all, when considering any security application, it is critical that you have your end user realistically assess the threat of a hack to their facilities. For example, if access control is being used merely as a convenience to the alternative of using physical keys, chances are the end user has a reduced risk of being hacked. However, if the end user is using their access system as an element of their overall security system because of a perceived or imminent threat due to the nature of what they do, produce or house at their facility, they may indeed be at higher risk and they should consider methods to mitigate the risk of a hack. Here are a few steps that may be considered in reducing that danger.

Just as we've become aware of criminal skimmers causing mischief with the ATM infrastructure, card holders should avoid presenting access control credentials to any access readers that appear to have been tampered with. Secondly these same card holders should be encouraged to quickly report to the facility's security and management teams any suspicions or access control system tampering, including instances involving either the access control readers or access credentials.

Skimming occurs when the attacker uses his reader to access information on the victim's RFID token without consent. The attacker has the ability to read stored information or to modify information by writing to the token, so he can control when and where the attack is performed. In practice the attacker's main challenge is to increase the operational range by powering and communicating with the token over a greater distance, as the owner might become suspicious of somebody in his personal space.

An eavesdropping attack occurs when an attacker can recover the data sent during a transaction between a legitimate reader and a token, which requires the attack to be set up in the vicinity of a likely target. The attacker needs to capture the transmitted signals using suitable RF equipment before recovering and storing the data of interest. The degree of success that the attacker will achieve depends on the resources available to him. An attacker with expensive, specialized RF measurement equipment will be able to eavesdrop from further away than an attacker with a cheap, home-made system. The attack is still a viable threat either way.

RFID systems are also potentially vulnerable to an attack where the attacker relays communication between the reader and a token. A successful relay attack lets an attacker temporarily possess a 'clone' of a token, thereby allowing him to gain the associated benefits. It is irrelevant whether the reader authenticates the token cryptographically, or encrypts the data, since the relay attack cannot be prevented by application layer security.

Smart card readers have several options that increase card security.

A combination keypad/card reader provides two-factor validation—something the person knows plus something the person has.

What's scary about all this is that the equipment needed to perpetrate the above attacks can be quite inexpensive and is widely available.

Boosting the Integrity of the Card-Based Access Control System

Because of such threats, single factor verification no longer provides the access security that many campus access control systems now require. Today, they want to have multi-factor verification with what they have, a card, plus what they know, a PIN. With a combination reader/keypad, access control manufacturers and their integrators can provide them with a simple, reliable solution for shoring up their system, the combination card reader/keypad.

To enter, the individual presents her proximity or smart card, gets a flash and beep, and then enters her PIN on the keypad. The electronic access control system then prompts a second beep on the reader and the individual is authorized to enter.

Another novel way of protecting card based systems is to provide a high-security handshake, or code, between the card, tag and reader to help prevent credential duplication to ensure that readers will only collect data from these specially coded credentials. In a sense, it's the electronic security equivalent of a mechanical key management system, in which this single campus is the only one that has the key they use. Such keys are only available through the integrator chosen for the job. Your integrator never provides another organization with the same key. No other organization will have the reader/card combination. Only their readers will be able to read their cards or tags and their readers will read no other cards or tags.

Smart Cards

Smart credentials go far beyond traditional identification cards. In addition to individual profile information, they can provide users with secure access to everything from their offices, parking lots and computer networks to safe methods of payment in the company cafeteria and checking out machine tools.

Let's summarize and list the various applications that the shrewd security administrator can consider for smart credential implementation:

- Physical credential administration
- Visitor management administration
- Provisioning or access privileges assigned
- De-provisioning or access privileges revoked
- Segregation of duties
- Parking permit administration
- Property pass administration
- Compliance/governance reporting and auditing
- System troubleshooting and maintenance
- Alarm correlation and response
- Emergency communication and notification
- Video analytics applications (people counting, behavior tracking, etc.)
- Identification
- Time and attendance
- Logical access
- Supplies check-out verification
- Charge privileges at various locations, including the cafeteria
- Document printing
- Biometric template storage

Let's also not forget the building management system. If the access control systems notes that someone is in a specific part of the building, the air conditioning and lighting can be activated. Once that person leaves, either the access control or video system could automatically tell the building management to turn those systems off.

If applications require multiple forms of verification, the smart card securely stores other credential types such as biometric templates, PIN codes and photos right on the card, using the enhanced storage and encryption of smart technology.

This can save money and resources, a potential green solution that would be helpful in meeting smart building requirements.

In addition to the functionality for multiple applications, smart credentials also increase the security of information kept on the card and stored in the facility. Valid ID is a new anti-tamper feature available with contactless smartcard readers, cards and tags. At manufacture, readers, cards and tags are programmed with the Valid ID algorithm, cryptographically ensuring the integrity of the sensitive access control data stored on the card or tag.

With Valid ID, readers scan through the credential's access control data searching for data discrepancies, which may occur during the counterfeiting, tampering or hacking of a contactless smartcard. Valid ID is an additional layer of protection to what is already available in smart card authentication, operating independently, in addition to, and above this standard level of security. In use, Valid ID allows a smartcard reader to effectively verify that the sensitive access control data programmed to a card or tag is not counterfeit.

If applications require multiple forms of verification, the smart card securely stores other credential types such as biometric templates, PIN codes and photos right on the smart card, using the enhanced storage and encryption of smart technology. Smart cards also provide an extra level of security at the access point, protecting the information behind closed doors or on the secure network.

Equally important, smart credentials afford security administrators more avenues to ensure safe and secure environments. The cards work in concert with access control systems, video surveillance and mass notification capabilities. With today's convergence of technologies, organizations can integrate existing systems with advanced credential reader technologies to enhance the security of their environments.

How to Help Customers Reduce Hacking Attacks

The door and window provider can be the frontline defense for protecting a security system. Understand what the customer's needs are, what the customer can do, what the customer has to work with, what hackers can do, where the hacker is most likely attack and what can be done to thwart the hacker. In other words, you need to figure out how apply the cliché "a good offense is the best defense." There are many things that can be done to reduce hacking of a card-based access control using the Wiegand system.

- Install only readers that are fully potted and that do not allow access to the reader's internal electronics from the unsecured side of the building. An immediate upgrading is recommended for readers that fail to meet this standard.

Make available credentials with an anti-playback routine, such as transmitters, instead of cards. This can be done by implementing long-range receivers installed in the locked security closet, with the electronic access control panels out of harm's way.

- Make certain the reader's mounting screws are always hidden from normal view and make use of security screws whenever possible.
- Embed contactless readers inside the wall, not simply on the outside, effectively hiding them from view. Or, if that is not possible and physical tampering remains an issue, consider upgrading the site to readers that provide both ballistic and vandal resistance.
- Make use of reader cable with a continuous overall foil shield tied to a solid earth ground in a single location. This helps block signals from being induced in the individual conductors making up the cable as well as those signals that may be gained from the reader cable.
- Deploy readers with a pigtail, not a connector. Use extended length pigtails to assure that connections are not made immediately behind the reader.
- Run reader cabling through a conduit, securing it from the outside world.
- Add a tamper feature, commonly available on many of today's access control readers.
- Use the "card present" line commonly available on many of today's access control readers. This signal line lets the access control panel know when the reader is transmitting data.
- Use access control readers with an output alternative to the industry-standard Wiegand output, provided they are supported by the electronic access control system. Alternatives can include ABA Track II, OSDP, RS485 and TCP/IP.
- Offer the customer cards that can be printed and used as photo badges, which are much less likely to be shared.

Look for These Product Options

Here are some items that you should consider to help end-users protect their access control systems:

- Offer a custom format with controls in-place to govern duplication.
- Avoid multi-technology readers as credential duplication risks increase.
- Promote a technology to limit the credentials a reader can read to a very specific population. As earlier mentioned, consider implementing a high-security handshake, or code, between the card or tag and reader to help prevent credential duplication and ensure that the customers' readers will only collect data from these specially coded credentials.
- Offer a smart card solution that employs sophisticated cryptographic security techniques. An example is MIFARE® DESFire™ EV1 cards making use of AES 128-bit encryption.
- Make available credentials with an anti-playback routine, such as transmitters, instead of cards. This can be done by implementing long range receivers installed in the locked security closet, with the electronic access control panels out of harm's way. With the receiver in the security closet, there would be no access readers installed at the door. Thus, no Wiegand data lines are ever exposed to the outside of the building. To enter the facility, the system user presses the appropriate button on the log range transmitter to gain access to any exterior entrance at a distance set by the user. The receiver, which is safely installed in the closet, will accept the signal and forward it to the access panel installed in the same closet, which will unlock the door. Meanwhile, traditional RFID access control readers could be used inside the facility.
- Offer a highly proprietary contactless smartcard technology such as Legic®.
- Provide two-factor readers, including contactless and PIN technologies. Alternatively, also offer a third factor, normally a biometric technology.

We must always stay one step in front of the bad guys. With the proper tools, any of these assaults can be defended.

SCOTT LINDLEY is a 25-year veteran of the contactless card access control provider industry. Since 2003, he has been president of Farpointe Data, a DORMA Group company. Prior, he was director of RFID products at Keri Systems and sales manager, North America, for Motorola Indala.