Specifications that will Help Stop Access Control Systems Hacking

By Scott Lindley

Beware: *The Federal Trade Commission Is Now Insisting on Cyber Security Protection*

Hacking has become a threat far bigger than most think. Indeed, the greatest threat to national security these days comes from not from aircraft carriers or infantry divisions, but a computer with a simple Internet connection located anywhere in the world. The U.S. federal government suffered a staggering 61,000 cyber-security breaches, that it knows of, last year alone. Protecting users from professional hackers is imperative for specifiers.

Odds are that most of us do not work for organizations as large as the U.S. government or as big of target as a major corporation. That should not give you rest. Many hackers are just teenage boys in basements just trying to get into any system that they can. It's referred to as "opportunistic hacking." And, when they get in, they like to change code that will create mayhem. Think *Ferris Bueller's Day Off*. Providing anti-hack card-based access control systems eliminates one of the more popular opportunities that Junior likes to leverage.

To give businesses an incentive to meet these cybersecurity threats, the Federal Trade Commission (FTC) has decided that it will hold the business community responsible for failing to implement good cybersecurity practices and is now filing lawsuits against those that don't. An appeals court backed its lawsuit against the hotel chain operator Wyndham Worldwide for not protecting consumers' information and, just recently, the FTC

Photo courtesy of Farpointe Data

filed a lawsuit against D-Link and its U.S. subsidiary, alleging that it used inadequate safeguards on its wireless routers and IP cameras that left them vulnerable to hackers.

The FTC is recognizing a problem that some security practitioners do not appreciate. To get into Information Technology (IT) and critical infrastructure Operational Technology (OT) systems, hackers are looking for the easiest path in, leveraging many different physical assets, including those within the enterprise security system itself. They typically start with hardware which will give them access to specific computers. Then, those computers will give them access to both the target's external and internal Internet.

Why do we mention both IT and OT systems? It's because most everyone understands what IT is; very few relate to OT. IT security lives in the context of networks, servers, storage, apps and data. IT involves a system where hosts are talking to lots of other hosts and where there are frequent patch cycles – in weeks or sometimes days – in response to expected and known cyber threats. IT security basically protects data (information).

Nonetheless, an attack on the IT system can create very big problems from stealing personal information such as Social Security numbers, HIPPA protected files and other privacy/ID data to transferring funds. If this isn't bad enough, however, the new trend of attacking the OT system can be even worse.

Out back, beyond the white collar offices and data centers and, often, miles away are the industrial control systems (ICS) that run organizations' operations. In industries as diverse as oil and gas, power generation and distribution, healthcare (i.e. MRI's), transportation systems, manufacturing and many others, ICSs, by connecting sensors, machines and instruments, create automated solutions that increase productivity. They control local operations such as opening and closing valves and breakers, collecting data from sensor systems to turn up the heat of furnaces and monitoring the local environment for alarm conditions. When hacked by sophisticated government backed entities, havoc can run rampant.

For instance, a little over a year ago, around 1.4 million homes in western Ukraine lost their electricity for several hours. This was a very sophisticated attack. Once the hackers had access, they manually opened the breakers. They then employed theBlackEnergy virus to hinder efforts to locate and restore the opened breakers. There was also a simultaneous Distributed Denial of Service (DDOS) on the utilities' call centers to slow down customer reports of outages.

Closer to home it was learned that breaches of the operating system at a dam outside of New York had been attributed to hackers working for companies that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps. Here the perpetrators successfully obtained unauthorized access to the Supervisory Control and Data Acquisition (SCADA) systems of the dam. Fortunately, in this case the Federal Bureau of Investigations(FBI) found those behind the cyber intrusion and the Justice Department held them accountable.

Often, Security Professionals Themselves Can Be at Fault

Interestingly, some security people don’t seem to secure their own security equipment. Over the past year, as noted already by the FTC, users are learning that today’s IP-enabled contactless card readers and wireless cameras have become favorite targets of hackers. Unsecured, they provide irresistible backdoors. Thus, new specifications are needed for electronic access control projects.

Let's begin with understanding one of the easiest problems to correct with security equipment. Were you aware that by simply putting the default installer code in a disarmed state, it can be used to view the user codes, including the master code or to change or create a new code? Therefore, if a potential unauthorized person gains access to a panel in the unarmed state, using the installer code gives that person access to all installed hardware. This will even allow creation of a new user code or change of a current user code, which then trumps the master/ other user codes.

So, if the installer does not change the default code, the user might as well be giving a user code to everyone. Less than 30 seconds is all it takes to view the master, all other user codes, or even create a new one. Yes, but what if the installer says they don't have the default installer code? Unfortunately, too often, these codes can be found online by anyone that knows how to do a simple Google search. Of course, once inside the system, the hacker can also get access to the rest of the computer system.

Sometimes the problem is within the software itself. The default code is embedded in the app to provide a mechanism to let the device still be managed, even if the administrator's custom pass code is lost. However, it is a poor developer practice to embed passwords into an app's shipped code, especially unencrypted.

Adding to the problem is that Wiegand, the industry standard over-the-air protocol commonly used to communicate credential data from a contactless access credential to an electronic access reader, is no longer inherently secure due to its original obscure and non-standard nature. Today, 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, one or more of a credential's identifiers are cloned, or captured, and are then retransmitted via a small electronic device.

For this reason, options are now available that can be added to the readers. The first is MAXSecure, which provides a higher-security handshake, or code, between the proximity or smart card, tag and reader to help ensure that readers will only accept information from specially coded credentials. The second is Valid ID, a relatively new anti-tamper feature available with contactless smartcard readers, cards and tags. Embedded, it can add an additional layer of authentication assurance to NXP's MIFARE DESFire EV1 smartcard platform, operating independently, in addition to, and above the significant standard level of security that DESFire EV1 delivers. Valid ID lets a smartcard reader effectively help verify that the sensitive access control data programmed to a card or tag is indeed genuine and not counterfeit.

Role of the Access Control Provider

First of all, when considering any security application, it is critical that the access control provider needs to realistically assess the threat of a hack to a facility. 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 to 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 the danger of hacking into a Wiegand-based system:

- Install only readers that are fully potted. Potting is a hard epoxy seal that does 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 certain the reader's mounting screws are always hidden from normal view. 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 onto the individual conductors making up the cable, as well as those signals that may be gained from the reader cable.
- Deploy readers with a pig tail, not a connector. Use extended length pig tails to assure that connections are not made immediately behind the reader.
- Run reader cabling through a metal conduit, securing it from the outside world. Make certain the metal conduit is tied to an earth ground.
- Add a tamper feature, such as Valid ID, commonly available on many leading 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.
- Provide credentials other than those formatted in the open, industry standard 26-bit Wiegand. Not only is the 26-bit Wiegand format available for open use, but many of the codes have been duplicated multiple times. 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.
- Employ a custom format with controls in-place to govern duplication.
- Offer a smart card solution that employs sophisticated cryptographic security techniques, such as AES 128-bit.
- Make available non-traditional credentials with an anti-playback routine, such as transmitters instead of standard cards and tags. Long range transmitters offer the additional benefit of not requiring a reader be installed on the unsecure side of the door. Instead they can be installed in a secure location, such as the security closet, perhaps up to 200 feet away.
- Offer a cutting edge, highly proprietary contactless smartcard technology such as Legic® advant.
- Provide 2-factor readers including contactless and PIN technologies. Suggest users roll PINs on a regular basis. If required, offer a third factor, normally a biometric technology (face, fingerprint, voice, vein, hand, etc.).
- Assure additional security system components are available. Such systems can also play a significant role in reducing the likelihood of an attack as well as mitigating the impact of a hack attack should it occur.
- *Intrusion:* Should the access control system be hacked and grant entry to a wrong individual, have a burglar alarm system in place to detect and annunciate the intrusion.
- *Video:* If the access control system is hacked, granting entry to an unauthorized individual, have a video system in place to detect, record and annunciate the intrusion.
- *Guards:* If the system is hacked and intruders are let in, make sure that guards in the control room as well as those performing a regular tour receive an alert notifying them that someone has physically tampered with the access control system.

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

Adding Encryption into an Access Control System

One aspect of securing a card’s information is to make the internal numbers unusable; they must be encrypted. To read them, the system needs access to a secret key or password that provides decryption.

Here is how it works. The number is encrypted using an encryption algorithm and an encryption key. This generates cipher text that can only be viewed in its original form if decrypted with the correct key. Today's encryption algorithms are divided into two categories: symmetric and asymmetric.

Symmetric-key ciphers use the same key, or secret, for encrypting and decrypting a message or file. The most widely used symmetric-key cipher is AES (Advanced Encryption Standard), which is used by the government to protect classified information. Another common symmetric cipher, noted for its high speed of transaction, is the TEA (tiny encryption algorithm); it was originally designed at the Cambridge Computer Laboratory.

Asymmetric cryptography uses two different, but mathematically linked, keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. RSA (named after Misters Rivest, Shamir and Adleman) is the most widely used asymmetric algorithm.

Today,13.56 MHz smart cards are used to provide increased security compared to 125 KHz proximity cards. One of the first terms you will discover in learning about smart cards is "MIFARE," a technology from NXP Semiconductors. MIFARE enables 2-way communications between the card and the reader.

MIFARE Classic was an original version of the MIFARE standard used in contactless cards. It stores the card number on one of its sectors, then encrypts the communication between the card and reader to theoretically make it impossible or, at least, very difficult to clone a card. Unfortunately, a security flaw was discovered in the MIFARE Classic standard which meant that, with the right knowledge and hardware, a card could still be cloned or another card in the series created.

Modern encryption algorithms play a vital role in assuring data security:

> **Authentication:** the origin of a message.

> **Integrity:** contents of a message have not been changed.

> **Non-repudiation:** the message sender cannot deny sending the message.

The newest of the MIFARE standards, DESFire EV1, includes a cryptographic module on the card itself to add an additional layer of encryption to the card/reader transaction. This is amongst the highest standard of card security currently available. MIFARE DESFire EV1 protection is therefore ideal for sales to providers wanting to use secure multi-application smart cards in access management, public transportation schemes or closed-loop e-payment applications. They are fully compliable with the requirements for fast and highly secure data transmission, flexible memory organization and provide interoperability with existing infrastructures.

Additional encryption on the card, transaction counters and other methods known in cryptography are then employed to make cloned cards useless or enable the back office to detect a fraudulent card and put it on a blacklist. Systems that work with online readers only (i.e., readers with a permanent link to the back office) are easier to protect than systems that have offline readers, since real-time checks are not possible and blacklists cannot be updated as frequently with offline systems.

Don't Let Them Hack via the Access System You Specify

Protecting your customers' organization(s) from hackers is imperative. The threats have grown to include sophisticated government-backed entities and teenage mischief makers. In either case, these bad actors are targeting both IT and OT systems, often with the result of imperiling our national security. With knowledge of what hackers seek and the remedies available to thwart them, anti-hacking specifications are now mandatory. If, for no other reason, the FTC is now providing new motivations.

SCOTT LINDLEY is a 25-year-plus veteran of the contactless card access control industry. He is president of Farpointe Data.