VULNERABILITY CHECKLIST
STOP HACKING OF YOUR ACCESS CONTROL READERS & CARDS

Beware: The Federal Trade Commission Now Insists You Provide Cybersecurity Protection

"When manufacturers tell consumers that their equipment is secure, it's critical that they take the necessary steps to make sure that's true."

Jessica Rich, former Director of the Federal Trade Commission's Bureau of Consumer Protection

Source: http://time.com/money/4625703/federal-trade-commission-dlink/

Protecting your organization(s) from hackers is imperative. The threats have grown to include sophisticated government backed entities and teenage mischief makers. Hackers look 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.

With knowledge of what hackers seek and the remedies available to thwart them, anti-hacking specifications for the access control system are now mandatory. If, for no other reason, the Federal Trade Commission (FTC) is now providing new motivations, deciding 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.

VULNERABILITY CHECKLIST
STOP HACKING OF YOUR ACCESS CONTROL READERS & CARDS

Two-factor readers provide an additional layer of protection over single-factor readers.

Add these common sense solutions to protect your electronic card access control system from being a gateway to hackers, just as it was for the Romantik Seehotel Jägerwirt in Austria, in which guests were locked out of their rooms, as reported by Dan Bilefsky in the New York Times[1].

Default Codes

- Do not leave the default installer code in an unarmed state. It can be used to view the user codes including the master code or to change or create a new code.
- If your installer says that they don't have the default installer code, have them find it. Too often, these codes can be found online by anyone that knows how to conduct a simple Google search.
- Sometimes the problem is within the software. The default code can be 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 very poor developer practice to embed passwords into an app's shipped code, especially unencrypted.

Wiegand Raises Red Flags

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.

- 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 custom Wiegand formats, ABA Track II magnetic stripe emulations, as well as serial options such as OSDP, RS485 and TCP/IP.
- 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 MAXSecure™, which provides a higher-security handshake, or code, between the proximity card, smart card or tag and reader to help ensure that readers will accept information from similarly specially coded credentials.
- Deploy credentials making use of ValidID™, a relatively new anti-tamper feature available with contactless smartcard readers, cards and tags. Embedded, it can add an additional layer of authentication assurance. It 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.
- 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.).

[1]Bilefsky, Dan, "Hackers Use New Tactic at Austrian Hotel: Locking the Doors", New York Times, January 30, 2017.

VULNERABILITY CHECKLIST
STOP HACKING OF YOUR ACCESS CONTROL READERS & CARDS

Employ These Simple Reader Implementation Techniques

Many installation techniques are simply common sense. For instance—

- Install only readers that are fully potted. Potting is a hard epoxy seal that does not allow access to the reader's sensitive 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.

Rugged Readers provide protection in extreme conditions that could damage conventional readers.

- 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.

Credentials that support MIFARE® DESFire® EV1 provide higher-level protection for security-sensitive applications.

Card Protection Solutions

- Today, 13.56-MHz contactless smart cards are used to provide increased security compared to 125-KHz proximity cards.
- Offer a contactless smart card solution that employs sophisticated cryptographic security techniques, such as AES 128-bit encryption.
- Offer a cutting edge, highly proprietary contactless smartcard technology such as Legic® advant.
- Consider NXP Semiconductor's MIFARE DESFire® EV1, which includes a 128-bit cryptographic engine on the smart card itself to add an additional layer of encryption to the card/reader transaction. Both Legic advent and MIFARE DESFire EV1 are amongst the highest standard of card security currently available.

Leverage Long Range Reading Systems

- Use 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 unsecured side of the door. Instead, they can be installed in a secure location, such as the security closet, up to 200 feet (61 m) away.

Long-range transmitters with a range of up to 200 feet allow a receiver to be placed in a secure location—out of sight and out of harm's way.

VULNERABILITY CHECKLIST
STOP HACKING OF YOUR ACCESS CONTROL READERS & CARDS

Assure Anti-Hacking Compatibility Throughout the System

The Open Supervised Device Protocol (OSDP) is a communication standard adopted by the Security Industry Association (SIA) that lets security equipment, such as card and biometric readers from one company interface easily with control panels and equipment from another manufacturer.

- A two-way channel paves the way for forward-looking security applications such as the handling of advanced smartcard technology, transparent operations, PKI and mobile device access. Not only does it provide a concise set of commonly used commands and responses, it eliminates guesswork, since encryption and authentication is predefined.
- The specification handles smartcards by constantly monitoring wiring to protect against attack threats and serves as a solution for high-end encryption such as required in federal applications.

Leverage Additional Security System Components to Stop Hacks Used to Gain Entry

These systems can 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.

There Is No Excuse… the FTC Says So

Always stay one step in front of the bad guys. With the proper tools, any of these assaults can be defended. All of the solutions described above are easily implemented by using Farpointe Data access control cards, fobs, tags and readers.

P/N: 01001-001 · Rev. 06.17

Farpointe Data, Inc.
1376 Borregas Avenue
Sunnyvale, CA 94089-1004 USA
Office: +1-408-731-8700
Fax: +1-408-731-8705
support@farpointedata.com

www.farpointedata.com