KERI SYSTEMS INCORPORATED

2305 Bering Dr, San Jose, CA 95131
Phone (800) 260-5265 / (408) 435-8400 / Fax (408) 577-1792

Solutions White Paper – Wiegand Interface Readers Have 4 Core Problems

Problem

While extremely common, Wiegand interface readers are based on a hardware protocol that is almost 50 years old and poses a number of security and life safety risks in the modern world, as well as some significant installation limitations.

Details

1) Wiegand readers are unsupervised devices, meaning that they can be compromised without the customer knowing it, ironically creating a weak point in what are supposed to be secure systems. The instructions on how to do it are readily available on the Internet. Two web sites that describe exactly how it can be done are:
   http://www.wired.com/threatlevel/2007/08/open-sesame-acc/
   http://www.securityinfowatch.com/Access+Control/hacking-wiegand-card-reader

2) They can also be vandalized, become defective, or even stolen with no notification to the system administrator. A system interfacing to a Wiegand output reader never knows if the reader goes off line or is removed, creating at best an inconvenience and at worst, a life safety issue. Vandalized or destroyed readers can leave someone stranded outside in an non-secure area, without the ability to enter a building, which can create a serious life safety issue, not to mention a significant liability exposure.

3) The most commonly formatted card or fob used on a normal Wiegand interface reader has had the same exact ID number issued tens or even hundreds of times, creating the opportunity for a duplicate credential to gain access where it should be restricted.

4) Readers with a Wiegand interface are limited to a 500’ (150m) maximum distance from the controller using #18 AWG (1.2mm) 6 or 7 conductor cable. The distance is half of that if #22 AWG cable (0.6mm) is used.

Solution

Due to its popularity, Keri supports the Wiegand interface on all of its products. However, Keri’s NXT reader and controller communication uses a secure RS-485 interface and the readers are fully supervised and monitored by the system while a Wiegand interface solution is not. If a Keri reader is compromised or the cable is cut, the system operator is immediately notified with a message. Additional alerts can be set up within the software to include email or text message notification creating, a far more reliable and secure solution.

Keri’s NXT cards and fobs are all uniquely coded with billions of possible ID so there is never a duplicate ID issued, eliminating the chance of a purposeful or inadvertent granting of access to a duplicate card ID. They also have an encrypted card number making them virtually impossible to predict internal patterns to duplicate cards.

Because the NXT readers communicate via RS-485, the cable distance is double that of Wiegand interface readers, and the 4 conductor cable used (including shielded CAT5) is 35%-50% less expensive than the shielded 7 conductor cable required for Wiegand output readers.

Summary

Wiegand technology readers create gaping holes in a security system, which by its nature is designed to provide security, not compromise it. This pervasive a problem will only be overcome when the industry begins to embrace more secure reader technologies that provide greater levels of security for the facilities and people they are supposed to protect. The NXT system provides that secure technology.

Needed Equipment

1) NXT Controllers and NXT Readers as needed for Installation
2) NXT Cards or Tags
3) Keri - Doors.NET - Access Control Software