VIZpin Security Overview

VIZpin was developed to improve the security, convenience and affordability of accountable access control. Traditional access control systems have several vulnerabilities that compromise security. This paper describes how VIZpin addresses these.

Physical Security

In order to interact with a user interface device (UID) such as a card-reader or keypad, traditional access control systems require the UID to be mounted on the unsecure side of the door. A UID mounted on the unsecure side of the door that directly controls a door mechanism like a door strike or mag lock, can be easily opened up and ***hot-wired*** to unlock the door which is a serious security risk. (see https://www.youtube.com/embed/lQtBgl2Slqg).

If the UID is a Wiegand output device, the card data is transmitted in an unencrypted format and can be hacked simply by monitoring the data lines. More info can be found at http://blog.opensecurityresearch.com/2012/12/hacking-wiegand-serial-protocol.html.

If the UID is an IP device, for instance Power-over-Ethernet (PoE), the device can be removed from the wall and the hacker would have direct access to that network. If the UID is Wi-Fi enabled, a hacker can also access the network using that access point.

Once a hacker has the Wiegand ID, they can use a ***replay attack*** or an inexpensive, off-the-shelf card programmer to program a new card with the same Wiegand ID.

VIZpin reader-controllers use long-range Bluetooth and can be mounted on the secure side of the door or device you are trying to protect. This prevents hackers from physically accessing the device, eliminating "hot-wiring," skimming and Wiegand replay attacks .In addition, VIZpin reader-controllers have no hardwired, PoE or Wi-Fi network connection, preventing hackers from accessing the IP network through our device.

Personal Compliance

Low to medium security environments rarely have full-time personnel for monitoring all employee activity and instead, rely heavily on compliance to ensure security, safety and accountability. Familiar examples of policies to ensure compliance are "Keep your card on you at all times" and "Don't share your keypad PIN# with anyone." Unfortunately, in many instances convenience outweighs security compliance; the classic example is a visitor who has to use the restroom that is outside the secured office. If the access control system uses keypads or card-readers, most hosts would simply point the person in the right direction and say "here, use my card" or "the code to get back in is 1234." Now there is no record of who actually came and went. Another challenge with card-reader systems is that many people leave their cards or fobs on their desks, especially if they are on a keychain. A card left unattended can be picked up easily by a nefarious individual and scanned in seconds without the user even knowing their corporate security identity had been compromised.

People tend to be much more careful with their Smartphone than their cards and fobs, and are highly unlikely to loan their phone to anyone to "get back in." Many businesses also mandate that Smartphones with corporate access have passcodes or utilize Smartphone biometrics such as fingerprint recognition in order to use the phone. The VIZpin SMART app can be configured to require a passcode each time you open an access point; a feature known as multi-factor authentication.

Bluetooth Security

Many Bluetooth devices transmit unencrypted data in order to simplify the pairing process which raises concerns when using Bluetooth in a security application…and it should. Bluetooth is a long-range technology (30'/10M) with published protocol and unencrypted data can be read easily by hackers using a ***man-in-the-middle attack***.

If you are using a VIZpin SMART (LE) device, VIZpin keys use double encryption including AES128 bit plus; a proprietary, patented VIZpin algorithm and every time a VIZpin key is used it uses unique data. To further improve security, VIZpin keys can be configured to rollover as frequently as every 15 minutes. If you are using a Bluetooth Classic device, the VIZpin keys are device specific and can roll over at such a high frequency that even a small number of repeated pairing attempts to discover the key cannot be completed before the key rolls over.