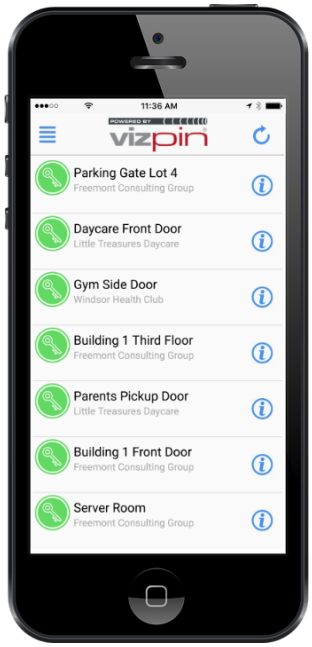
VIZpin Smartphone Access Control System
SECURITY OVERVIEW

The VIZpin Smartphone Access Control System was developed to improve the security, convenience and affordability of managed 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 flaw. [More information can be found here: Hot-Wiring Keypads]



If the UID is a Wiegand output device, the card data is transmitted in a well-known and unencrypted format and can be recorded by simply monitoring the data lines. [More information can be found here: Hacking Wiegand]

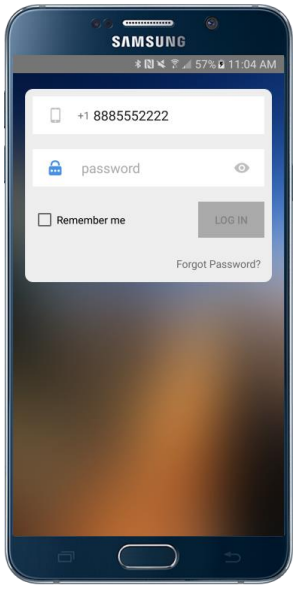
VIZpin controllers have built in Bluetooth readers. These readers work up to 30' (10M) away so the controllers can be mounted on the secure side of the door you are trying to protect. This prevents hackers from physically accessing the device, eliminating "hot-wiring," skimming and Wiegand replay attacks.

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

A hacker can now see all unencrypted Wiegand IDs being sent across the network, and can later use a ***replay attack*** or an inexpensive card programmer to program a new card with the same Wiegand ID.

VIZpin controllers have no hardwired, PoE or Wi-Fi network connection, which prevents hackers from accessing your network through our device. Additionally, our controllers require absolutely no network connection for operation; everything is performed using only Bluetooth and the user's phone. This means that we don't create any new holes in your network infrastructure or require you to run a parallel network to isolate any potential security risks. It also removes any costs associated with secure network access for the UIDs because our controllers require none.

Personal Compliance



Many locations cannot afford full-time staff to monitor end user activity so they rely on compliance to ensure security, safety and accountability. Stated policies like "Keep your card on you at all times" and "Don't share your keypad PIN# with anyone" are difficult to enforce. Convenience often outweighs security compliance and employees share their cards and PIN#s. Most of us have been at a meeting and had to step outside. Most hosts won't escort you, they are more likely to loan you their card or give you the keypad code. Now there is no record of who actually came and went.

In a traditional card reader system, many people leave their cards or fobs unattended. Those cards and fobs can be picked up easily and scanned in seconds without the actual user even knowing their security identity had been compromised. They are also small and easily to slip into your pocket to be used later.

People are much more careful with their Smartphone than their cards and fobs, and are very unlikely to loan their phone to anyone to "get back in." Many businesses also mandate smartphones with corporate access have passcodes or utilize smartphone biometrics such as fingerprint recognition in order to unlock the phone. The VIZpin SMART app can be configured to require the user to login in order to access their keys adding another security layer in addition to that of the smartphone. This also prevents a hacker from gaining access to an unlocked phone and using any of that user's keys.

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 a published protocol and unencrypted data can be read easily by hackers using a ***man-in-the-middle attack*** *(MITM)*.

If you are using a VIZpin SMART (Bluetooth low energy, 4.0) device, VIZpin keys use double encryption including AES128 bit plus a proprietary, patented VIZpin algorithm. Every time a VIZpin key is used to connect to our controllers, it uses unique data that prevents replay and MITM attacks. To further improve security, VIZpin keys can be configured to expire as frequently as every 15 minutes, requiring the user to revalidate their keys against the server before being able to use existing keys for unlocking.

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.