Securing Fob Access Systems Against Casual Fob Duplication

DEALERS - Updated June 2018

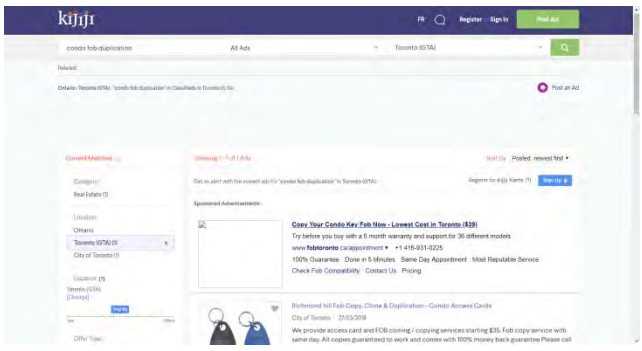
A question often asked is what can be done to prevent unauthorized access control fob duplication.

In a condo community, there are typically 2 to 4 fobs issued per suite. These are usually provided to the residents in exchange for a deposit of $50 or more. If a fob is lost or stolen it can be easily removed from the system and the resident can be provided with a new fob with a different ID number.

Sometimes a resident will want to save the cost of the fob deposit, or otherwise keep private that they wish another fob for their building. This may be for guests, children of the resident, a maid or pet care provider, etc. In these cases, non-residents acquire an unauthorized duplicate fob. When they use this, the access control system registers the actual resident entering the property, rather than someone that should rightfully be checking into the building with security or pre-cleared by security/management for fob entry with restrictions such as 'no use of common facilities'. The problem is especially prevalent with the most widely used fobs, the Low Frequency ('LF') radio fobs commonly called '125khz' credentials.

The resident in this case is circumventing the security protocols for the rest of the residents of the community. This is similar to having a "Do Not Dup" Master Key that a resident makes an unauthorized and secret copy of anyway, distributing it to unknown 3rd parties.

Duplicating most fobs is pretty easy nowadays. A quick Kijiji search yields multiple, local services offering "5 minute fob duplication", some even specifically targeted to the Condo market:



Beware Generic Fobs

There are many generic fobs available to dealers. These are from a multitude of overseas manufacturers that are making them typically in low-security (i.e. very easy to copy) formats such as “125-khz SIA 26-bit”. They can be ordered from eBay or Alibaba websites, with any ID range and ‘site/facility code’ with no particular checking for duplicates by these overseas companies. Even Amazon has listings for very inexpensive 26-bit cards/fobs for sale! They can be inexpensively copied in just a couple of minutes using the services mentioned above. They are often made of cheap plastic in various colours or the popular grey, with only the ID number etched on them, sometimes with the dealer’s name screen-printed on them.

These are common examples:

Doing a search on overseas supplier sites such as Alibaba.com for “125 khz fob” returns 286 companies that are happy to supply these generic, easy to copy fobs.

The Problem with standard ’26-bit’ Fobs

A huge portion of existing fob access systems use a format called “SIA 26-bit” format. SIA is the Security Industry Association, which the last revision to this standard was way back in 1996.

The Standard 26-bit Format is an Open Format. An Open Format means that anyone can buy HID cards in a specific format and that specific format description is publicly available. Almost all access control systems accept the standard 26-bit format.

‘SIA 26-bit’ has 255 possible facility codes from 1 to 255. There can be up to 65,535 card ID numbers, from 1 to 65,535 per facility code, giving about 16,700,000 possible unique fobs. There are no restrictions on the use of this format.

The problem is that many sites reuse the same ID ranges, such as numbering fobs from “1 to 1000” or “1000 to 1999” for their communities. It’s rare to see a community use some more random set such as “38750 to 39749” for their fob ID numbers. This results in a large number of “accidental duplicates” between many communities, since the Facility Code is what it overly relied upon for uniqueness, with only 255 possible different Facility.

This shortcoming of 26-bit fobs can be corrected by using a MAXSecure-style fob technology which eliminates this high risk of ‘accidental duplicate’ fobs from another site working at yours. This is covered in more detail later in this paper.

What can be done? (4 different options)

The problem is prevalent with Low Frequency ('LF') radio fobs, commonly called '125khz' credentials. There are several common solutions but not all equally good for use in a condominium community:

Solution 'as-is' - Just leave things as-is ("I gave a fob to my friend so they could use the pool")

If your fobs are currently 125-khz they may continue to be copied and any number of unauthorized/unknown non-residents may have access to your community and its facilities.

Solution 'A' - Use a mixed-technology reader with PIN # (not recommended for condos)

This solution uses fob readers with a PIN number pad on them.

These are not at all convenient for residential use. The resident needs to present ("wave") their fob at the reader then enter a 4-digit PIN. While this is effective in preventing criminal copying of a fob, since duplicating a fob without the owner knowing will still not provide the PIN number to use it, it DOES NOT prevent a resident from duplicating their fob then telling the unauthorized user their personal PIN to use with it.

Solution 'B' - Use Paired readers & fobs with encryption technology (Very Good Solution)

This is a much better solution, particularly for a condominium community where it is important to have high security for all but not make residents feel burdened entering their homes or using the shared facilities of their community. This solution provides new readers throughout the condo using 'ISM-band' communication technology (a style of fob usually called 'Mifare') with encryption and MAXSecure-style technology. MAXSecure adds a security verification code, between credential and reader. Readers secured this way will not react to fobs that do not have their paired code.

Solution 'C' - Use encryption technology paired readers & fobs mixed with Smartphone 'fobs' (BEST SOLUTION for Condo Communities)

This is most often the very best solution. This offers "conventional", high-security access fobs to those residents that wish them, using the secured, encrypted technology of Solution 'B' above, with the addition of readers that will **also** react to specially registered smartphones. The advantage of this is covered in detail in the following section.

The Solution in Detail:

High-security Encrypted Formats and MAXSecure

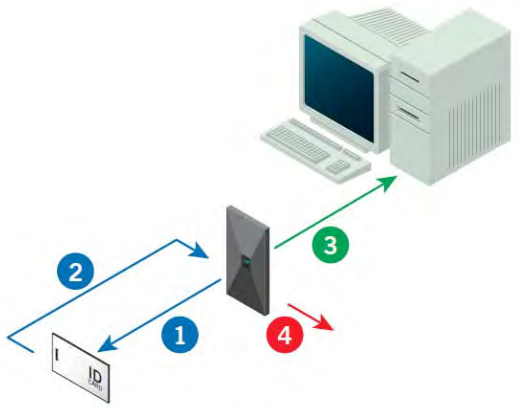
Encryption technology paired readers & fobs with the addition of a MAXSecure-style feature, offers a number of tangible security benefits. For example, MAXSecure ensures that a user's credentials are truly unique, with no duplicates, even when implementing the industry standard (and relatively low security) 26-Bit format. Further, a MAXSecure-enabled reader will only read credentials with the matching MAXSecure code.

1) Reader powers access control credential.

2) Card/fob transmits MAXSecure code and access data to reader.

3) If reader authenticates card's MAXSecure code, then reader transmits access data (facility code, ID number, etc.) to access controller.

4) If reader does not authenticate card's MAXSecure code, then the reader transmits nothing to the access controller.



Casual duplication of these credentials is prevented when protected by high security encryption between the uniquely coded readers of the community and the fobs. There is no way for casual third party duplication companies to read and duplicate this unique code; it is not part of the normal credential data stream from the reader to the access panel.

This means that a duplication service could only possibly duplicate the fob "usual data" by cloning the ID and site code printed on the fob, but that this unique site-coded identification data is not present in the duplicate fob, therefore the MAXSecure enabled reader in your community would simply ignore the duplicate fob.

MAXSecure also completely eliminates the potential 'accidental duplicate' between other communities, as discussed above in "The Problem with standard '26-bit' Fobs".

This is an excellent solution for a condo community. It only requires that, at a minimum, the readers be upgraded to encrypted technology readers with MAXSecure-style verification. Thereafter, all NEW fobs would be ordered with the encryption and MAXSecure lock/code in them and would be safe from casual & accidental duplication. This solution is inexpensive to implement initially, although the community remains less secure over the time it takes to slowly retire the existing fobs for new, secure ones.

Recommended Solution – Implementation and Cost

The recommended solution for a community would be to reach into their Reserve Fund to upgrade not just the readers but also all of the existing fobs, particularly older & less secure "125-khz 26-bit" fobs to one of the modern +35-bit formats. New readers and fobs would implement encryption technology and be paired with MAXSecure-style verification. This would immediately end the problem of casually duplicated fobs. The costs are not excessively high at all.

This upgrade would take a day to implement the hardware. Once done, residents would have to simply pass by the office or concierge/security desk to swap their old fob for a new, secure one – or the new fobs could be distributed a week or two ahead of time with a particular day for them to be 'turned on' and everyone starts using them on that day.

This is also an **excellent** time to update your database or implement a new one 'from scratch'. Many older condos have access systems that are not up to date and many fob numbers assigned that are no longer properly tracked to the owner. While implementing these new technologies, all newly issued fobs can be properly recorded into the database. If the old access system does not support modern database functions and tracking, it may be an excellent time to look at replacing the access control panels and install modern, secure Windows-PC software also, as part of the overall upgrade. Indeed, many older access control systems are still in the field that are running on an obsolete 'PC-DOS' platform or Linux!

Recommended Solution – with an eye toward the future (Bluetooth)

Adding Security by Eliminating Fobs

A fast-growing option is to eliminate fobs completely and implement access using people's ubiquitous smartphones. With the revolution of highly secure technology such as Google Pay, Apple Pay, Samsung Pay and a multitude of other similar applications, more and more people are using their smartphones to order taxis and pay for lattes.

In communities that want to be able to provide this very modern entry method, residents using their smartphone as their 'fob', it is necessary to implement "Conekt Mobile-Ready" readers that support Bluetooth Low Energy (BLE) technology to communicate. These are duel-tech readers that will also read the encrypted, secured fobs discussed throughout this paper, allowing residents the option to use a standard fob **or** their phone.

When activated within the Conekt Wallet App or similar, mobile credentials allow users to identify themselves at designated access points—doors, gates, parking facilities, and more—with the existing standard electronic access control system.

The advantage of Conekt Technology is that each 'fob ID', which are identical to a standard, physical fob to the access control system and database, are locked to the unchangeable, built-in serial number of the phone they are assigned to. They cannot be 'given out' – once used, that 'fob id' is locked to that phone, for unique identification without the possibility of unauthorized duplication. Of course, if a resident moves out, removing the ID from the system is the exact same easy procedure as if they had a physical fob.

If you have any questions about the above, please feel free to contact me directly for a prompt reply.

Jeff Mullen, President

CONDO SECURE

Direct: 416.879.7514 www.CondoSecure.com jmullen@condosecure.com

CondoSecure Systems is a Toronto area manufacturer and provider of advanced security products, access control and Insuite Keypad systems, focused on the condominium markets in the GTA & worldwide.

Role of Bluetooth - *As seen in Professional Security Magazine*

16TH MAY 2018

As you join in the trend to use smart phones for mobile access control, select the right communications protocol, writes Scott Lindley, General Manager, Farpointe Data.

Using smartphones in access control systems is the new buzz in discussing readers and credentials. Electronic access control manufacturers are promoting the various ways that mobile technology, soft or virtual credentials, can be used to replace cards. It's not surprising that all are trying to get on board.

According to Gartner Research, 95-plus percent of all adults aged 18 to 44 own smart phones. That's not all – 69 percent of the entire population already uses smart phones. That's babies through seniors. Gartner suggests that, by 2020, 20 per cent of organizations will use mobile credentials for physical access in place of traditional ID cards. Let's rephrase that last sentence. In less than 18 months, one-fifth of all organizations will use the smart phone as the focal point of their electronic access control systems. Not proximity. Not smart cards. Phones!

Besides the fact that just about everyone has one, what are other reasons? To arrive at that answer, let's review the basics of access control. Access control authenticates you by following three things:

- Recognizes something you have (RFID tag/card/key),
- Recognizes something you know (PIN) or
- Recognizes something you are (biometrics).

Your smartphone has all three authentication parameters. This soft credential, by definition, is already a multi-factor solution. Your mobile credentials remain protected behind a smart phone's security parameters, such as biometrics and PINs. Once a biometric, PIN or password is entered to access the phone, the user automatically has set up two-factor access control verification – what you know and what you have or what you have and a second form of what you have.

To emphasize, one cannot have access to the credential without having access to the phone. If the phone doesn't work, the credential doesn't work. The credential works just like any other app on the phone. The phone must be "on and unlocked."

These two factors – availability and built-in multi-factor verification – are why organizations want to use smart phones in their upcoming access control implementations.

Why Bluetooth

Bluetooth and Near Field Communications (NFC) are the most popular short-range radio wave communication standards used in smartphone credential systems. When implementing mobile access, there are a few things to consider before deciding on the type of reader to invest in. The installed base of mobile devices can affect the technology choice as iPhones 5s and earlier do not support NFC. In organizations with a large base of iPhones and Androids, Bluetooth is the only option.

Bluetooth technology is quite popular and, if you have ever tried to sync smart phones, computers and/or headphones, you have probably used it. Bluetooth readers are less expensive because almost every smart phone already has Bluetooth. Not even 50 percent of all smart phones yet have NFC.
In most instances, NFC (Near Field Communications) uses less power. As a result, this means that the smart phone needs to come into much closer nearness to the reader, like a proximity card versus a longer-range transmitter. The good news is that such closer proximity prevents interference for other devices communicating from farther away. The negative is that the reader can seem more finicky.

There are other advantages to a closer read range. NFC eliminates any chances of having the smart phone unknowingly getting read such as can happen with a longer read range. There are also those applications where multiple access readers are installed very near to one-another due to many doors being close to one another. One reader could open multiple doors simultaneously. The shorter read range or tap of an NFC enabled device would stop such problems. However, with this said in defense of NFC, it must also be understood that Bluetooth enabled readers can provide various read ranges of no longer than a tap, as well.

And, this leads to a major advantage for Bluetooth. Read range can be from an inch to over 15 feet. Installers can provide adjustable read ranges and differ them for various applications. For instance, they could choose a reader requiring presentation at the computer server room. Three feet may be the preferred range at the front door. When entering the facility gate, a still longer read range, perhaps six feet, can be provided so users don't have to open their car window to reach the reader. At 15 feet, the reader can open parking garage doors or gates that allow entrance to the facility, such as at gated communities. There is yet another advantage to a longer reader range. Since NFC readers have such a short and limited read range, they must be mounted on the unsecure side of the door and encounter all the problems such exposure can breed. Bluetooth readers mount on the secure sides of doors and can be kept protected out of sight.

The Bluetooth technology used in access control is called Bluetooth Low Energy (BLE). It is very efficient; a single cell battery could operate for months on end. For those technically inclined, it operates with a maximum speed of 1Mbps with actual throughput of 10 ~ 35 Kbps. Thus, access control using Bluetooth BLE technology with today's smartphone offers the promise of lowering the cost of hardware.

To make the system work, there needs to be a direct connection between the Bluetooth enabled device [the Smartphone] and the Internet. This is done very simply through the cellular data network or a secure WIFI connection. To install a mobile credential, a user needs to first have the Wallet App installed on a supported smart phone. Next, you launch the App and select the "+" button, indicating that you would like to load a new credential. A Registration Key Certificate is provided for each credential ordered. Now, enter the unique 16-character Key from the Certificate and tap "Submit."

Once successfully registered, the new mobile credential will appear in the Wallet App ready for use. From that point on, the user simply presents their smart phone to the BLE-enabled reader. Forget having to enter a PIN or password to authenticate your identity (as you do with a card). Henceforward, your smart phone is your identity. Once the phone is operational, so too is your credential!

Caveats

As when implementing any new technology, become familiar with it. Where can you find the benefits? Where are the potential pitfalls? Make sure your manufacturer not only understands Bluetooth but knows how to coach you through your initial installations. Don't forget about your cybersecurity responsibilities. For instance, some older Bluetooth enabled systems force the user to register themselves and their integrators for every application. Door access – register. Parking access – register again. Data access – register again. Et cetera.

Newer solutions provide an easier way to distribute credentials with features that allow the user to register only once and need no other portal accounts or activation features. By removing these additional information disclosures, vendors have eliminated privacy concerns that have been slowing down acceptance of mobile access systems.

Also, you don't want hackers listening to your Bluetooth transmissions, replaying them and getting into your building. Make very sure that the system is immunized against such replays. That's simple to do. Your manufacturer will show you which system will be best for each application. Research shows that Bluetooth enabled smart phones are continuing to expand in use to the point where those not having them are already the exceptions. They are unquestionably going to be a major component in physical and logical access control. If they are going to constitute 20 percent of all card-based access control within the next 18 months, you can expect the numbers to be much higher by the end of 2020.