Michel Lauzon
Director of Client Services
SMS Security

Fob Cloning in Condominiums

In recent years condominiums have been facing a significant new threat; the cloning of access control credentials, also known as key fobs and fobs. Numerous websites and storefronts have sprung up offering to clone access control credentials at ever-decreasing prices. These individuals operate without oversight and will even offer to come to your condo unit to clone your fob for as low as $20/$30 per fob.

How Fob Technology Works

An RFID (radio-frequency identification) key tag, commonly known as a fob or key fob, is a handheld device that allows many condo owners to access their condominium entrances, amenities and in some cases, their elevators. These fobs contain a microchip that houses the fob's identification number along with an antenna and coiled wire. The majority of these fobs are low-frequency passive credentials and operate on frequencies between 30 kHz to 300 kHz, with most manufacturers using 125 kHz. These credentials use no power source and are powered by the energy transmitted from the RFID reader, commonly known as card readers.

Most fobs have two sets of identification numbers, a facility code and a card number. Different facility codes allow the same card numbers to be used multiple times and reduces the likelihood of a client receiving duplicate fobs. These fobs have no encryption and continuously transmit the same facility code and card number.

When a credential is placed within 10cm of the card reader, the reader powers up the fob, which then transmits its unique identification number to the Access Control Unit (ACU) Panel (also known as door controllers) through the cable connecting the card reader and panel. The ACU panel checks the number, confirms it is in the database with the correct access level, and then sends a signal to the door strike to disengage, allowing the individual to open the door.

Credential manufacturers purchase a certain amount of blank credentials and then program them to a series of numbers for use at multiple buildings/clients. Multiple facility codes are included to reduce the likelihood of

duplication. Once the manufacturer programs the credential, the number cannot be changed. A proprietary system of "burning" the coil makes it no longer re-programmable.

Cloning a Fob

Individuals and businesses take advantage of fobs and fob cloning devices widely available for sale online at exceptionally low prices (often for as little as $10.00). As these fobs have not undergone the proprietary "burning" process, they arrive blank and can be programmed and reprogrammed to any facility code or card number. Given that the communication between the card and access control system is not encrypted, cloners need only match the card number for the fob cloned.

Fob duplicators work by scanning a valid fob and programming its number onto a blank fob. Now there are two credentials with the same number. Both will have the same access level at your property and will open doors with identical transactions on the access control software.

Numerous credentials with the same card numbers can be reproduced and given to friends, family or left in lockboxes for use by short-term rental tenants. Depending on the lockbox material, fobs left inside may also be subject to cloning, allowing a nearby fence to become a security risk.

New Technologies – Smart-Fobs

To prevent cloning, low-frequency fobs should be replaced with high-frequency, smart credentials. These smart-fobs run on 13.56 MHz and use two-way encrypted communication, which uses similar technology to your debit/credit cards, passports, hotel keys, etc. Mobile credentials, fob numbers tied to cell phones via applications made and managed by the access control manufacturers also use NFC (near field communication) or Bluetooth for two-way encrypted communication.

When the smart-fob enters into a smart-reader's range, it begins a secure communication session using Shared Encryption Key Codes. Once this is established, the card number is transmitted, and the communication session is closed off.

This means that instead of one-way communication, there is two-way communication between the smart-fob and the smart-reader. In addition, the access control system will also program the smart-fob and smart-reader with specific encryption key codes, which a cloning device cannot copy without going into the access control system software.

One drawback of smart-credentials is that they will not have the same read range as the old fobs and require the smart-fob to be placed closer to the smart-reader and slightly longer.

> *When the fobs are more widely available and more cost-effective through the corporation, residents will respond appropriately, allowing the corporation to maintain better control.*

In order to use these high-frequency smart-fobs or mobile credentials, all fobs and card readers require replacement. Older legacy software often must be upgraded, which necessitates the replacement of one or more access control panels. Depending on the property size, the number of doors and other components tied into the access control system, such as in-suite alarms, suite smoke detectors, intercoms, etc., can cause these upgrades to exceed most budgets.

How to Discourage Cloning

While your corporation reviews the pros and cons of such an upgrade, there are many ways to discourage owners and tenants from cloning fobs.

Corporations should be mindful of the price they sell their fobs to residents. While the corporation's cost per fob is usually around $10.00, many corporations sell fobs for $25-$50 and, in some cases, upwards of $75 to $100. Prior to the proliferation of fob cloners, corporations wanted to keep greater control on the number of fobs issued to residents, often capping the number of fobs to the number of bedrooms. Corporations have also historically overpriced the fobs to ensure that residents take good care of their credentials and take extra steps not to lose them. This has pushed residents towards fob cloners.

Many duplication websites list the addresses of frequently cloned fobs to try to attract additional clients. Corporations should review these websites periodically, contact them to have their property removed from the list and speak to their corporation's legal counsel regarding the possibility of drafting rules & regulations banning the practice of fob cloning.

To deter cloning, corporations should make purchasing a new credential as easy and as pain-free as possible, allowing residents to buy them online via condo management software, at all times via the concierge desk and during office hours through the management office. When the fobs are more widely available and more cost-effective through the corporation, residents will respond appropriately, allowing the corporation to maintain better control.

In addition, corporations should perform frequent fob audits to ensure that unused fobs are deactivated until needed again. Any lost/unused credentials should be deactivated instead of entirely removed from the system. This allows the information to stay on the system (suite #, names, phone numbers, etc.) while ensuring the fob no longer has access to the property. The concierge and security staff should be trained to recognize possible cloned fobs, for example, the same card used at multiple areas, different people using the same fob, frequent tailgating/trespassers related to the same card, etc.

The access control cloning threat has shown no slowing down nor coming to an end. With any legislation concerning fob cloning highly unlikely, corporations need to act to ensure the safety and security of their community. ■

Michel Lauzon, Director of Client Services for SMS Security, has over 12 years of experience in the security industry, progressing from Security Guard to Director within the Golden Horseshoe Residential Security Market. He is a member in good standing with ACMO as well as with the American Society for Industrial Security International (ASIS). smssecurity.ca