Feb 16, 2011, 12:53pm EST

The Kaba Simplex lock is only for "access control": Is that what FDNY Engine Company 65 thought?

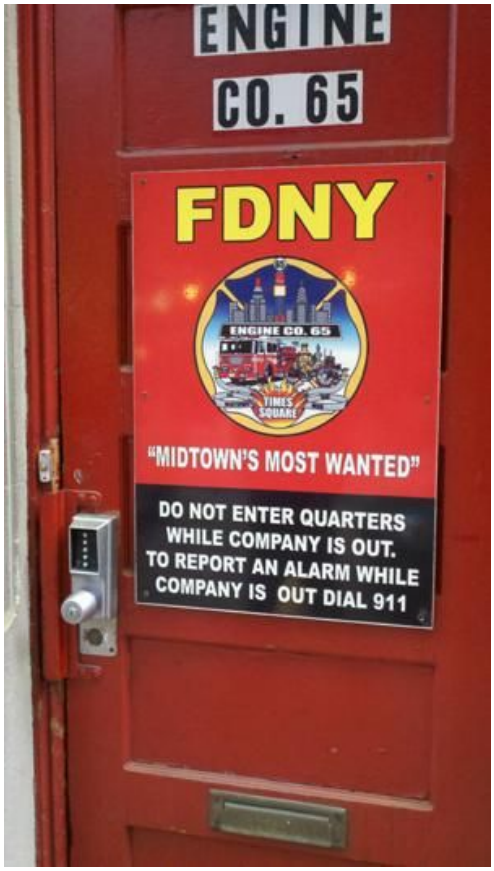
Marc Weber Tobias Contributor
Cybersecurity
I am an investigative attorney and physical security specialist.

This article is more than 9 years old.

A picture is worth a thousand words, and this one, in my view, says it all. The company that made the push-button lock that is shown on the FDNY door was sued in late November in a class action lawsuit which I wrote about in two previous articles. It is a serious security issue and in my view, everyone that owned these locks prior to December, 2010 could be in jeopardy and should know about it.

I happened to be walking near Times Square on Monday when I came across New York Fire Department Engine Company 65. The door was locked and the fire trucks were gone. I would be interested to know just who thinks that the Kaba Simplex lock on the door was strictly for "access control" rather than for security. Kaba has repeatedly told the world that these locks will limit access to secure or sensitive areas, but are not for security. I

would absolutely agree with that statement in theory, but not in reality. The real question is whether the fireman in this particular firehouse thought that this lock would also protect their equipment, personal property, valuables and everything else that is stored in their facility, from unauthorized access?



A Kaba Simplex lock protects an FDNY firehouse in Manhattan. Many of these locks can be opened in... [+]

Unlike the game of jeopardy that Bruce Upbin played against an IBM computer that he described in his **article** earlier this week, (where the stakes were only trying to see if he could outwit a specially programmed super computer), this game that Kaba has been playing over the last few months that involves some models of their Simplex can have real and serious consequences for the people that rely on these locks.

Today In: Tech

It is beyond my comprehension as to why the company, once they were made aware of this issue did not immediately notify everyone, stop selling the vulnerable locks, and fix them. As I note later in this article, it appears they figured out an extremely simple, cost effective and secure fix. It may not be perfect, but it does solve the immediate security concern, once implemented.

The game that Bruce played last week only showed that he clearly was not as smart as the mega-computer. And by the way, he lost in about five milliseconds! In real life, people rely on locks to protect them. They do not understand subtle distinctions between “access control” and “security.” They

do not want to play the game of jeopardy against criminals, vandals, and other threats.

To most consumers, businesses, and government agencies, locks are locks. While they may have several purposes and levels of security, they are all designed for one thing: to limit access. And in my view, just about every single location where these defective locks are installed is placing people at risk. Venues include firehouses, airports, computer server rooms, banks, clinics, hospitals, businesses and homes.

Even bathrooms in commercial buildings can pose dangers. Just think if you are a female employee and need a code to enter in order to use the toilet? You feel secure because you know that nobody but authorized employees with the right code can enter, right? Would you feel secure, knowing that some “psycho with a magnet” could gain access to what you believed to be a “secure area?” Of course not. End of story.

If I understand properly, the company claims that its Simplex locks are only for “access control’ and not for security. It is, in my view, a distinction without a difference. All locks are about access control. I bet the members of Engine Company 65 thought that the Kaba Simplex lock on their door would protect their firehouse when they were away fighting fires. So, should they be concerned that a thirteen-year old kid figured out how to open these locks with a fifty dollar magnet in about four minutes? I think so.

The Fix

We have analyzed the apparent fix that Kaba has implemented in their combination chamber (the brains of the lock) to stop it from being opened by a strong magnet. I say "apparent' because I have not seen any word from Kaba to confirm this, and there is nothing in the **programming sheet** that comes with the updated combination chamber to indicate any security problem.

The fix works, it is simple, and in our view makes the lock mechanically secure. It can be retrofitted to older chambers in the field, although I think it would be smarter and more preferable to replace the entire chamber. Locksmiths should do the upgrade, not the consumer, for a variety of reasons.

How much does the new cover cost to make? I do not know, but if it costs the company a dollar that would probably be a stretch. Of course, the cost for the replacement part is only the beginning of the story. Someone has to install it.

The real question is how Kaba intends on fixing the thousands, if not millions of locks that are out there and at risk of an attack. I am quite certain that every fire station in New York that uses these locks for “access control’ would like an answer to that question, and sooner than later. Kaba has been aware of this vulnerability at least since August of 2010. My information is that it might have been earlier if you believe some of the posts on locksmith blogs.

The bypass of locks by magnets is not a secret and has been around for quite a while. If Kaba did not know about this method of attack, they should have. I remember attending locksmith and security conferences a few years ago when different locks and electric strikes were easily defeated by strong magnets. While I do not specifically remember if the Simplex was shown, I can attest that others were opened easily.

Kaba usually has a large booth at these events and I cannot imagine that their sales or engineering people would not have walked around and witnessed some of these demonstrations. Maybe they just did not connect the dots. Or maybe, like many lock manufactures, they simply “knew” that their locks could never be opened in this manner. Just like what I was told by tech support at Kaba when I was researching this matter in order to write a security alert and analysis. I was advised essentially that “there would be

no internal component that would be affected by a magnetic field and which would allow the lock to be opened."

Well, in my career, I can say that almost every manufacturer that has made such a statement has or may be proven wrong sometime in the future. For a lock manufacturer it requires staying current with bypass techniques and understanding how locks work, and what really unlocks the mechanism. It requires a basic understanding of threats and how to guard against them. I would argue that current lock products that are being sold should periodically be tested against known attacks.

Believe it or not, it is not the correct credential (the key or the code) that **actually** unlocks a lock! These "credentials" control the **mechanism** that allows the lock to be opened or closed. If you can directly access that control mechanism, then you open the lock. In the case of the Kaba Simplex, the magnetic field is able to move a critical component and allow the lock to be opened without the proper code.

In my world, it is "security engineering 101." Every design engineer should understand basic bypass methods, and using magnets is one of them.

While the cover of the internal brains of the lock has been fixed so the Simplex cannot be opened with a magnet, we may not be quite done with this story. I would stay tuned because there may be some unintended ramifications to this fix which will require added "enhancements" to ultimately get it absolutely right.

Finally, if you are wondering if I know if the lock on the FDNY was vulnerable, the answer is no, because I did not try to open it. Perhaps Engine Company 65 could weigh in on this and ask Kaba.

Marc Weber Tobias

Follow

I wear two hats in my world: I am both an investigative attorney and physical security/communications expert. For the past forty years, I have worked investigations, ... **Read More**