Feb 9, 2011, 05:58pm EST

Opening the Kaba Simplex Lock: Just How Easy Is It?

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

This article is more than 9 years old.

I have received a plethora of e-mail from concerned security officers and locksmiths throughout the world, in both commercial and government sectors, wanting to understand the magnetic attack on the Kaba Simplex series of locks that was the subject of my original article on February 1, 2011.

Kaba is one of the world's biggest lock manufacturers, and my article about the class action against it caused everyone to want to know just how simple or difficult the attack is to accomplish and whether they (or their clients) are at risk in their facilities or homes.

Because of the number of locks that may be affected throughout the world (with many in critical facilities), I view this as an extremely important security concern. So, for the past week I have been investigating three critical issues as a follow-up: just how the vulnerability was discovered by non-experts in relation to the Simplex series of locks, what is the fix that Kaba has devised to ensure the security of thousands of facilities that rely upon these devices, and is their fix effective?

Kosher Locks (without bagels) in Brooklyn

Yesterday, I interviewed one of the plaintiffs in the lawsuit. He is Jewish, Orthodox, lives in Brooklyn, deals in real estate, and until last summer, had

confidence that his Simplex push-button lock would protect his property from unauthorized entry. It seems that Kaba has found a niche in the Orthodox community, especially in New York. Everyone uses their Simplex locks. Why? Because during the Sabbath, one cannot carry keys nor do any other work that would violate religious doctrine.

Orthodox Jews in Brooklyn

Essentially, Orthodox Jews cannot drive, use the phone, utilize anything electronic, or perform functions that are normally accomplished during the week. The Sabbath is supposed to be a day of rest in all respects. However, security is still important, and locking and unlocking doors becomes a major issue for those who cannot use keys on Friday and Saturday.

The Kaba Simplex solves the problem because it is a mechanical lock that utilizes push-buttons, which, believe it or not, are allowed under Jewish law. So Kaba has, in effect, created what I will refer to as its "Kosher Locks!" According to the plaintiff that I spoke with (who wishes to remain unnamed), virtually the entire Orthodox community relies upon Kaba for their security, both in their homes and many of their businesses.

Enter the dozen or so volunteers, the Jewish Geek Squad as it were, who help the elderly of the community when they need things fixed, technical-gizmo related assistance, or to get into their houses in Brooklyn when they have forgotten the combination to their door locks. It seems that in the summer of 2009, one of these volunteers figured out that many of the Kaba locks could be opened with a relatively inexpensive magnet.

So, for the past eighteen months, they have been performing Magnetic Mitzvahs (a good deed or charitable act under Jewish law) for the residents

of Brooklyn, compliments of the deficient or defective design of the Simplex. The home and business owners thought it was a miracle: How can you wave your hand in front of my door lock and it opens? "Magic," the saviors answered. "The Lords work." They never told anyone how they were doing it. In fact, it appears they never told anyone about their secret until this fall.

And then the word leaked out and eventually ended up in the hands of lawyers, who decided that everyone was at risk and had been misled as to the security of the locks. They filed a lawsuit in November.

If you read the motion that was filed by Kaba in December in Federal Court (and is referred to in my original post), the company claims that the ability to open these locks is dependent upon many factors, and may be difficult or even impossible to accomplish. According to Kaba, there are many variables, including finding a "sweet spot" (as the defendants characterize it) in each magnet and lock which, they go on to claim, may or may not even exist. They intimate that the locks, as I read their motion, are or can be difficult to open.

Actually, I would prefer to think of the design of the lock and its specific mechanical point of failure as the Simplex G-spot, which must be found in order to exploit the mechanical vulnerability. For us, it was not very difficult to discover and it felt really good when we did!

The due diligence in the plaintiff's case started with an unnamed dad who bought a $40 magnet on-line and opened at least twenty-five locks that are "protecting" homes and businesses of his friends, relatives, and associates in Brooklyn. Then he gives his "high tech" magnet to his 13-year-old son Israel and "commands" him to open a lock. According to the father, he provides absolutely no information about the lock, where its G-spot is, or how to open it to his son. "Just do it," he challenges.

Now what thirteen year old Yeshiva student would not jump at the chance to demonstrate just how clever he really is to his father? None. So our soon-to-be covert entry expert takes only four minutes to figure out the secret and

open the lock. No prior knowledge. No training. No expertise. Nothing. All it took was just a cheap magnet and an expensive lock: the Kaba which everyone thought was secure. This was the Kaba Simplex lock that was sold to everyone who believed it would satisfy their security **and** religious needs at the same time.

In the motion that Kaba filed with the court, they clearly implied if not directly stated, that their locks could not be opened reliably with magnets. And even if some of them could, they claimed, it required a rare-earth magnet and some expertise to find that precise point that would allow it to be compromised.

I challenge this statement as misleading, which brings me to one of the critical reasons for posting this article and the decision I have arrived at for doing so.

In my earlier post, I rather sarcastically questioned whether Kaba engineers, in the 1960s, were aware of the concept of magnetism as it applies to covert entry. For years, my associates and I have known about and exploited the capability to open many locks with the proper application of a magnetic field. Covert entry experts have employed this technique quite successfully in many venues around the world, and the exploit is fairly well known in our community.

Lawyers for the defendant in this case seemed to focus their argument on the fact that rare-earth magnets were not commercially feasible until a few years ago (and evidently not available in the 1960s) when the lock was first developed. So goes their apparent logic that even if their engineers had considered the potential for a magnetic attack they dismissed it because no magnets were available, at least to the private sector, to accomplish such a bypass.

That argument may or may not be true and really begs the relevant question: Did they know about the potential for strong magnetic fields to

move ferrous metal components within their locks? If they understood that a critical piece of the lock was subject to a magnetic field, then why did they not design it differently? Or were they just not familiar with or simply ignored the concepts of magnets-metal-and-locks as they all work together to cause them to open?

I received an e-mail from a colleague at one of our National Laboratories after he read the article. He is a senior vulnerability specialist and leads a team that discovers security and design flaws in hardware. He read the article and wrote that "Their argument (Kaba's) that rare earth magnets are state-of-the-art is bizarre. I thought rare earths were commercially available in the late 1960s, with battery powered electromagnets (which can be stronger) available in the 1900s."

Exactly! Every kid who watched Mr. Wizard (myself included) learned how to make a strong magnet with some wire, a battery, and an iron rod.

The problem with this attack in relation to Kaba is the ease with which it can be carried out. Initially, we produced a video that detailed the vulnerability and why it can occur. This was distributed only to locksmiths, law enforcement and security professionals on my security website. I thought it would be ill-advised to make the video openly available to all consumers, businesses and government agencies (although many government covert entry teams were actually aware of the issue quite some time ago).

I have since decided that if a thirteen year old kid can figure this out, then everyone needs to understand their risk. Just like I made known what eleven-year old **JennaLynn** did a few years ago when she easily opened the Kwikset lock by bumping that one, and later, high security locks.

My resolve was reinforced yesterday morning when I again contacted tech support at Kaba to see if they were now warning of the security risk that is apparently inherent in many models of their locks. I was told that the locks could be used for access control and for security applications. There was

absolutely no mention of the magnet attack. That is, until I specifically inquired about Simplex and magnets. Then I was told "No comment" and referred to others in the company.

I then contacted a V.P. for Kaba, who was extremely polite but stated that it was corporate policy not to comment on pending litigation. I told him that, as a lawyer, I understood, but in fact I was not asking about the lawsuit, but about the locks and what they were going to do about it. Again I was told "No comment," which is where things stand today.

Kaba: "All locks can be bypassed, so nobody should be liable"

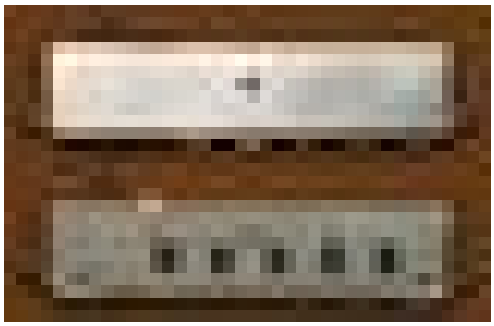
Kaba argues that "all locks can be bypassed" by locksmiths and thieves because they all have access to the same tools and information. Although this may be true, in my view it completely fails to address the core issue. They claim that the company "never advertised or warranted in any way that any of its access control products are impenetrable." No, but I would think that anyone who purchased their products had a reasonable expectation that the locks would resist a simple covert attack, at least for a few minutes. It should be noted that a close reading of their pleadings never mentions security, but only "access control." Yet their advertising, employees and dealers continue to state that their push-button locks are "just like regular locks and are designed to control access to secure areas."

So just what does "access control" really mean? In my world, **all locks are access control devices.** This is pretty obvious and basic. The real question, and one which apparently escapes Kaba, is just how **difficult** that access is to accomplish. And that premise is at the root of their problem. The simplicity of this attack is what is dangerous and what negates, in my view, any disclaimers that these locks are only for "access control." Access control means restricting access to authorized individuals. Evidently, everyone with the proper magnet is "authorized."

I don't think the owners of these locks would agree!

A Possible Fix

We obtained what appears to be the "new" enhanced version of the combination chamber from a Simplex dealer on January 28. Recall that this is the brains of the lock. It contains the ferrous part that created this nightmare for Kaba. We also purchased a complete lock in December, 2010. It contained a combination chamber that was dated November 10, 2010. It had not been modified, and the lock was easy to open.



The original (top) and modified combination chamber for the Simplex push-button lock. The only... [+]

In our initial inspection of the new chamber, it looks like the only difference between the earlier design and the "enhanced-to-be-more-secure" model is the cover. In our preliminary tests, the cover does seem to prevent our opening the lock with the same strength magnet, but we are only just beginning our analysis. We have not yet obtained a complete new lock and housing with all of the updates, which may incorporate designs to alter the magnetic field and its effects upon the combination chamber. We are waiting for a definitive word from Kaba “that they believe the problem has been remedied” before conducting further tests and drawing any definitive conclusions.

Even more interesting is the **programming sheet** that is supplied with the lock and is dated December 15, 2010, regarding the installation and code programming of the new part. This came with our January 28 combination chamber.

The notice relates to resetting an unknown combination, and warns that "Cover removal is NO longer required **and should NEVER be removed for lost code retrieval**." Nowhere in this document does it state the reason for the change in design, nor any alert to the customer as to the security threat that exists in locks that do not contain the modified chamber.

So, Kaba incorporates a changed cover design and remains silent about the reason and the underlying vulnerability. In my view, this is irresponsible and a huge mistake. More importantly, I would submit that it is placing a lot of people at risk.

Here's the icing on the cake: Kaba implied in its motion to the court that locks which were supplied after September 19, 2010 were enhanced to minimize or prevent the magnetic attack. Now it appears that the upgrade only applies to locks that were manufactured or retrofitted after December 15, 2010, according to the notice that was included with the new chamber. If I read this correctly, it means that four months elapsed before this change went into effect. I understand the delay between a new design and when it makes its way through the distribution chain to the end-user, but wouldn't it have been better to warn all dealers to stop selling any current in-stock product with the known problem until it had been resolved and upgraded?

To our knowledge, this has not occurred. The lock that we purchased with a December, 2010 date stamp does not have the new combination chamber. This would tend to confirm our belief that December 15 is the magic date. When I spoke with Kaba yesterday, they would not comment about this either.

There is no question that Kaba immediately took the threat seriously and urgently moved to fix it. So, why would they not publish a warning in the media or to their critical customers and dealers to stop selling the locks and to evaluate the potential risk in each facility?

How easy are they to open?

The reality is that the Kaba Simplex push-button lock can be opened in seconds by applying a strong magnetic field to the left side of the housing in combination with specific actions upon the lever handle or knob. This is a fact, although Kaba countered in its Motion that "any thief, even the clumsiest, can use a sledge hammer, a pry bar, or bolt cutter to bypass

essentially any lock." I have no disagreement with this statement, except that it would appear that Kaba or their counsel failed to take into account the difference between forced and covert entry.

We are not talking about forcing our way into the Simplex, which would leave visible traces, be noisy, destroy the lock, and likely leave evidence as to the perpetrator. What we are talking about is covert entry, which is the compromise of these locks without leaving a trace, with no audit trail, and with no evidence of entry. In many facilities I think this is precisely why these locks are installed: to deter covert entry into sensitive areas. That premise has been repeatedly confirmed by the emails I have received on this subject from government agencies, and Kaba advertisements which state that its locks are suitable for use as access control devices for sensitive areas.

While a clumsy thief with a sledgehammer may be able to open most locks with enough time, it may only take a couple of seconds with a strong magnet to accomplish the same result with the Simplex. It can be done silently, with little effort, and leaves no way to know whether an unauthorized person had gained access to or compromised a facility.

At the end of the day, Kaba's customers will have to judge for themselves whether the company designed a product which is or is not secure for their particular application. Although Kaba claims this is only an access control device, the real question is what was understood by their customers when they installed them, and the meaning of the illusive term "access control."

If a thirteen year old kid can open these locks, then everyone should judge for himself the threat. As a result I decided to release a slightly modified video that demonstrates just how easy the bypass is to accomplish, without showing one critical element that requires a couple of seconds to accomplish in many of these locks. We produced two different versions: one short and to the point, and the other that is quite detailed for those that need to understand the nature of the attack and the problem. If you are responsible

for the security of your facility, employees or assets, then you should view one of the segments to evaluate whether you are potentially at risk.

Watch the video and decide for yourself. Is it a state-of-the-art attack by a sophisticated thief, or a simple method of bypass which, in fact, may be executed by a stupid and clumsy one (or even a kid) who has been able to obtain a strong rare-earth magnet.

I think we all know the answer to this question. Even Kaba!

Short video that demonstrates the bypass of the Kaba Simplex lock

Detailed video that examines the bypass and the design of the Simplex lock

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**