Aug 22, 2011, 06:25pm EDT

A Medeco Knockoff Lock You Can Open With a $3 Screwdriver

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

This article is more than 8 years old.

Earlier this month at Defcon 19 in Las Vegas, we presented an analysis of the Kaba E-Plex series of electronic access control devices as reported by Forbes' Andy Greenberg.

The lock below, produced by Medeco, is a high security deadbolt that has a security rating and... [+]

Examining what we perceived as failures in security engineering, these design flaws in Kaba locks would allow us to open this series of locks within seconds. We used common items that are available to anyone, and more importantly, they are available to any thief or inside attacker within a high-security environment. The Kaba locks are used in commercial buildings and their latest model is intended for use in federal and other government facilities for secure access control. The E-Plex 5800 was specifically designed as the first lock to comply with the new requirements for the

acceptance of secure, verifiable, and reliable identification for all federal employees and contractors, pursuant to the FIPS 201 standard.

Kaba is the third largest lock manufacturer in the world but is by no means the only company that struggles with the conflict that often occurs between mechanical and security engineering issues. Virtually every lock maker has, at one time or another, produced products, from simple to sophisticated functionality and options that are seriously flawed with regard to their security. Most engineers clearly understand how to make things work properly, based upon sound mechanical designs, but have little or no clue about "breaking them."

The failure to understand the techniques that we employ to compromise security systems (and particularly mechanical and electronic locks) can be deadly in terms of the product performing as specified in security standards and in protecting assets, facilities, and personnel as specified and required by the end-user.

Two ends of the "security spectrum" have repeatedly demonstrated this problem. In my article about Hewlett Packard and their defective laptop lock, we demonstrated the ability to rap open this $40 device in seconds by using a plastic-handled screwdriver. While HP represents that they manufacture this lock, in reality it is produced in Taiwan by a third-party supplier. It is one of a host of security products that illustrate what I perceive as illustrative of junk security engineering.

I would consider these locks as the low end of the "security spectrum." The Kaba Simplex 1000 push button lock that I wrote about earlier this year was another perfect example of this, only the price tag for that was several hundred dollars. The lock, now fixed by Kaba, could be opened in seconds with a strong rare-earth magnet.

At the other end of the "security spectrum" are high security locks. These usually carry ratings by standards organizations like UL and BHMA. In 2007, as an example, we attacked the design of the Medeco Maxum deadbolt as seriously flawed, and demonstrated how to open that lock in under thirty seconds with implements costing a few cents, and a two dollar screwdriver. The Maxum was one of the most widely respected high security deadbolts in the U.S. Medeco, to their credit, urgently addressed the problem after we presented our findings at DefCon. They developed a patented fix which would prevents the lock from being attacked in the manner we originally described.

There is a vast difference between a lock manufacturer that expends significant resources for research and development and one that simply copies or mimics other successful products and capitalizes on their reputation. It is akin to knocking off trademarked designs of popular watches, handbags, and the unlimited number of expensive items that are cheap copies, designed to either fool the consumer or blur the distinction between quality components and engineering, versus inferior designs and in our case, a false sense of security.

Enter the CX5 Security Corporation in Quebec, Canada. This company, which sells its locks in Canada and to a more limited extent in the United States, advertises a "high security deadbolt lock" for about $240.00. It looks secure and when I called the manufacturer was told that in fact it was, and would be difficult to compromise without a lot of effort.

Evidently neither management nor the design engineers at CX5 read the news media coverage of our attack on the Medeco product four years ago. Unfortunately, like so many others, they took some shortcuts in the development of their deadbolt lock and according to representatives of CX5 "copied the design of the Medeco lock."

Watch the video we produced that documents one of the critical design flaws that we found in this expensive lock and decide whether you would rely

expensive high security-rated locks, or low-end like so many of us rely upon to protect our laptops, they all should accomplish the same fundamental purpose: to provide the measure of security that we paid for and expected to receive.

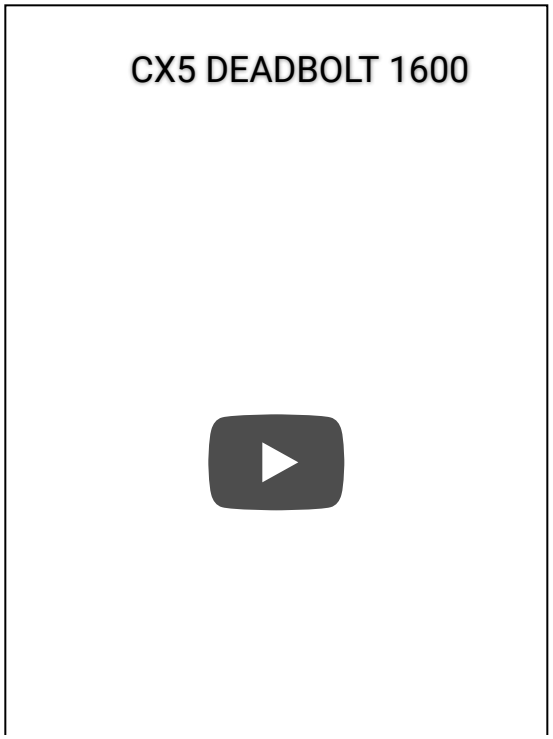
Stay tuned for many more examples of what you thought you were paying for in security, but did not receive, especially those devices that protect your personal computer. You may be surprised at how many manufacturers are producing locks that can be easily defeated.

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**

upon its security.



This is not an inexpensive product. It has a UL437 security rating which primarily relates to the pick resistance of the lock. It has absolutely nothing to do with the method by which we totally compromise the security of this lock. UL 437 is a commercial standard, not high security. The CX5 deadbolt looks very secure, which is precisely the problem. It is not, and neither the company nor the unsuspecting consumer knows the difference. When I tried to discuss this issue with the management of CX5, they refused to return my four phone calls, saying they were busy in meetings.

No lock company is immune from the problem of insecurity engineering, whether the largest or smallest, as we have repeatedly shown. The end-user is the loser in terms of getting what they paid for and more importantly, in a failure of security.

Can CX5 fix the problem? Probably, just like many of the other locks that we have examined. But that really is not the point. The real issue is why they have to do so in the first place. Locks have a unique role in every society; they protect people, their assets, and information. Whether they are