White House High-Security Locks Broken: Bumped and Picked at DefCon

From: InfoSec News <alerts () infosecnews org>
Date: Thu, 9 Aug 2007 02:07:21 -0500 (CDT)

http://blog.wired.com/27bstroke6/2007/08/jennalynn-a-12-.html

By Kim Zetter
August 05, 2007

A group of researchers has cracked the security features in what are supposed to be some of the world's most secure locks -- locks that are used at the White House, the Pentagon, embassies and other critical locations.

The researchers presented their findings for the first time at the DefCon hacker conference this weekend and showed how they could easily bump and pick the newest high-security M3 locks made by Medeco, a company that owns an estimated 70 percent of the lock market.

In addition to bumping and picking Medeco's M3 cylinder locks, the researchers also succeeded in the last few weeks to crack a Medeco M3 deadbolt lock -- considered to be one of the highest security locks in the world. They showed Wired News how to open the deadbolt in less than a minute using nothing more than a modified $2 screwdriver and a wire shim. They asked, however, that we not publish the details.

"Medeco invented the pin tumbler lock that lifts and twists the pins," says Marc Weber Tobias, one of the researchers and an investigative lawyer and author. "It's a brilliant idea and basically these are unpickable locks. But we can pick them. Everybody in my profession has been trying to break these for 30-35 years. And frankly, I can't believe that we've come up with this and nobody else has."

He says the deadbolt crack is especially concerning.

"The deadbolt is really a serious security problem," he says. "I don't want to create a panic, but this needs to get fixed."

The M3 is a new high-security lock that Medeco launched in 2005 to improve upon its previous Biaxial locks. The key for unlocking Medeco's M3 lock has a patented bar on the side of it that has to make contact with a slider inside the lock. The feature is intended to heighten the lock's security. But Tobias and his group found a way to simply bypass

the slider with a paper clip and proceed to open the lock as if it were a previous-generation Biaxial lock.

"We wanted to (take) a picture of a sign outside the White House or the Pentagon that says 'Security Warning: No cameras, no cell phones, no paper clips," Tobias says. "This is so ludicrous."

Tobias and his two colleagues, among them computer security researcher Matt Fiddler and a professional locksmith who asked not to be named, made headlines last year when they published techniques for bumping Kwikset locks -- the standard brand of lock that is used in most homes. After a small media storm ensued, Medeco responded to the news that Kwikset's locks could be bumped by saying that its own locks were bump-proof.

So Tobias and his colleagues decided to test this claim last April. They conducted extensive analysis of Medeco's published key codes and within three months had made their first breakthrough toward cracking the security of the locks. They then spent the next 12 months perfecting their techniques and creating and testing a special set of keys derived from the published key codes for non-master key locks. They've since filed several provisional patents for their cracking techniques.

To demonstrate their crack of Medeco's M3 lock for Wired News, Tobias took a lock and inserted one of the keys that he and his researchers designed from Medeco's codes. Then he hit it several times with a bump hammer and turned the key.

The deadbolt was opened just as quickly with an even simpler technique using the wire shim and screwdriver. Tobias pointed out, however, that this cracking technique works only on deadbolts that have a single-sided key entry with a flip switch on one side, not on deadbolts that require a key on both sides of the lock.

Tobias says that his group provided Medeco with full documentation of their techniques as well as video showing them cracking the locks. He says that rather than comment on whether their techniques were plausible, Medeco said the researchers didn't know what they were talking about and insisted its locks were still bump- and pick-proof. Tobias says he told Medeco that he was willing to sponsor a worldwide validity test to demonstrate his group's ability to crack the locks, but Medeco hasn't responded to his offer.

Tobias thinks there are a couple of possible reasons why Medeco hasn't commented on the techniques they used to crack the locks.

"Either Medeco has known about this (problem) for a long time and just won't comment on it, or the government has known about it for a long time and hasn't told Medeco. Or (Medeco testers) just can't replicate this (cracking technique) and don't understand what we're talking about. But the bottom line is that we're opening the locks."

Medeco was unavailable for comment, but a call to the company's main number produced a voicemail message addressing the bumping controversy and directing callers to this page on the company's web site.

Tobias says he initially didn't intend to release this information about the M3 locks at DefCon. He planned to simply write about it in the next edition of his book. But Medeco's continued insistence that the locks are secure has prompted him to discuss the issue more publicly. He posted information about the lock cracking techniques on his blog and, three days ago, posted a security alert specifically about the M3 deadbolts to a restricted industry site for professional locksmiths. He also met with a representative of the Underwriters Laboratory and intends to speak in September at a meeting of the lab's standards

technical panel for UL 437 to discuss improving the standard for such locks. Currently the standards don't test for bumping, Tobias says.

[This weekend at DefCon Tobias ran into Jennalynn, a 12-year-old girl who appeared in a YouTube video last year bumping a Kwikset lock. (Jennalynn's mother declined to give her daughter's last name because she preferred not to have it published.) Tobias asked her to try bumping Medeco's Biaxial lock, a more secure lock. She did it three times. Below [1] is a video showing her bumping the lock, with Tobias next to her.

[1] http://www.youtube.com/watch?v=D1LH7lrftKA

⬅ By Date ➡ ⬅ By Thread ➡

Current thread:

White House High-Security Locks Broken: Bumped and Picked at DefCon *InfoSec News (Aug 09)*