KIM ZETTER SECURITY AUG 9, 2007 2:00 AM

Medeco Readies Assembly-Line Fix for DefCon Lock Hack

High-security lock manufacturer Medeco is countering a security attack uncovered at the Defcon hacking conference with design changes to safeguard its claim to "bump proof" deadbolt locks.

Researchers were able to bypass the lock inside a Medeco M3 high-security deadbolt to open the deadbolt lock. They say the attack works on any deadbolt, not just those made by Medeco.Dave Bullock

SAVE

HIGH-SECURITY LOCK MANUFACTURER Medeco says it's planning a design change to counter one of two attacks against its products that were described at the DefCon hacking conference over the weekend, boosting security on a line of locks found at the White House, the Pentagon, embassies and other critical locations.

On Sunday, three researchers led by lock-picking expert Marc Weber Tobias showed how they could easily "bump" and pick Biaxial and high-security M3 locks made by Medeco Security Locks, a Virginia-based company that claimed last year that its locks were "bump-proof."

The only tools the researchers needed to bump the Biaxial lock was a special bump key and a hammer. The M3 lock, which comes with an added slider feature, required an additional tool – a paper clip.

Matt Blaze, a professor of computer and information science at the University of Pennsylvania who has written about master-key locks, says the researchers' work is impressive and concerning.

"Medeco locks are marketed to people who want to use them for high-security applications," Blaze says. "They're widely trusted to be very, very secure and are regarded as effectively pick-proof in practice. So any time there is an attack against this kind of lock, particularly a non-destructive kind of attack (that doesn't show evidence of an attack), that's very surprising."

Picking a Medeco M3 lock proved to be as easy for the researchers as picking other locks.

Photo: Dave BullockPrivately, the researchers also showed Wired News a new type of attack on deadbolt locks that requires only a modified $2 screwdriver and a wire shim device. Wired News agreed not to publish the details of the technique, but the researchers say it exploits a flaw present in single-cylinder deadbolts – those that have a single-sided key entry with a flip switch on other side. It does not work on deadbolts that require a key on both sides of the lock.

The researchers demonstrated this technique on Medeco's M3, though they say it works on some other brands of single-cylinder deadbolts they've tested.

"The interface for deadbolts is defective," says Tobias, an investigative lawyer and the author. "I don't want to create a panic, but this needs to get fixed."
Clyde Roberson, director of technical services at Medeco, acknowledged that the researchers might be right about the deadbolt problem. This week the company rapidly developed what he hopes is a hardware solution to the vulnerability, and Roberson is scheduled to fly to Florida on Thursday to meet privately with one of Tobias' researchers to see their attack on the lock and try out the fix.

Medeco hopes to roll out the solution on its factory floor this Friday if tests show the solution works.

But Roberson is more skeptical about the bumping demonstration. He told Wired News he thinks the researchers' claims are untrue and Medeco locks are still bump proof.

"We stand behind our locks," Roberson said. "We don't believe you can use a bump key on Biaxial or M3 (locks) at all, whether it's with a paper clip or not. We believe that this information is factually incorrect."

Bumping uses kinetic energy to open a lock with a specially cut key. The attacker inserts a bump key into a lock, and then raps it with a small hammer. The energy created by the impact travels through the key and causes the locking pins inside the lock cylinder to separate, allowing the cylinder to turn and unlock the device.

The attack is considered a serious threat because, like lock-picking, it's a covert technique for breaking into a locked door that leaves no obvious telltale evidence behind (though forensic examiners who scrutinize the inside of the lock might find little marks on the internal pins).

Although locksmiths and covert-entry specialists have known about and practiced bumping for years, the general public became aware of it only in the last two years after researchers disclosed the industry secret, and videos showing how to bump locks appeared on the internet.

It's been widely believed that Medeco's high-security locks were impervious to the technique. In a conventional pin-tumbler lock, each cut in the user's key lifts the corresponding pin in the lock to the exact height needed to turn the cylinder. But Medeco's patented pin tumbler locks also require the key to rotate the pin to one of three orientations – left, right or center. The feature has made its Biaxial high-security locks a favorite for years with customers who sought extra protection. When bumping received national media attention last year, the company even issued a press release boasting that its locks are "bump proof."

Tobias and his colleagues began testing that claim a year ago last April through a combination of computational analysis and mechanical tests. Using computers, they analyzed and crunched Medeco's published non-master-key codes to determine how many bump keys they would need to make to encompass all of the possible

key-code combinations. (Lock companies publish such codes so that locksmiths can create keys for the locks.)

Medeco's keys have a special feature in that the bidding on them (the peaks and valleys) is cut at different angles and different offsets (spacing). These angles and offsets can be combined in more than a million variations to create keys that are unique to each lock. Using a computer, however, and taking advantage of engineering tolerances in the lock, the researchers crunched the codes and synthesized the combinations to create fewer than a dozen keys (they've asked us not to disclose the exact number) that will fit into numerous Medeco Biaxial and M3 locks.

Blaze says the approach is impressive.

"It's interesting to see how this combination of mechanical and computer analytical methods can be used to attack these things," he says. "If you're just looking at these things in mechanical terms or you're just looking at these things in computational terms, you won't be able to attack them successfully. The combination of the two, I think, is fairly unique and pretty clever."

Even then, the researcher's technique should have failed against Medeco's newest lock, the high-security M3 introduced in 2005. An improvement on the old Biaxial, the M3 cylinders feature a slider inside. A patented bar on the side of the key has to push in the slider in order for the key to enter.

But the researchers, among them computer security researcher Matt Fiddler and a professional locksmith who asked not to be named, found a way to bypass the slider on the M3 locks as well. They simply use a modified paper clip to push back the slider and then bump the lock as if it were a previous-generation Biaxial lock.

To demonstrate their bumping technique against 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 hit it several times with a bump hammer and turned the key.

Tobias says that last year his group provided Medeco with full documentation of their techniques as well as video showing them cracking the locks. But Medeco's

Roberson dismissed their claims after Tobias visited him last October to show him the technique. Although Tobias was able to open locks he'd brought with him, he was unable to bump open locks that Roberson pulled directly from the factory line. Tobias says this is because his team was still perfecting the bump keys at the time, and that he was able to open those same locks later after the design of the bump keys was tweaked and the keys were re-cut.

The failed demonstration is what left Medeco's Roberson initially unconvinced of Tobias's claims. Roberson adds that since then Medeco researchers have not been able to replicate the bumping claims, he thinks the researchers simply designed one bump key to open one lock used in their demonstration, which wouldn't open other locks.

"A bump key is something that works on any cylinder that you walk up to," Roberson says. "They couldn't walk up to a random lock on a door and open it."

Tobias says that contrary to Roberson's statement, their bump key has worked on more than one lock.

"We've opened many, many locks with the bump keys," he says. "Theoretically, we can open all of the M3 locks, but we don't know for sure. What if we can open just 50 percent of them? The question is ... what percentage becomes a threat?"

Tobias has posted a security alert about the M3 deadbolts to a restricted industry site for professional locksmiths and next month he'll meet with representatives of the Underwriters Laboratories – the lab that tests and creates standards for manufacturers' products – to discuss improving the standard for such locks. Currently the standards don't test for bumping.

Two other companies that manufacture deadbolt locks – Schlage and Abloy – did not respond to calls by press time.

Blaze says that Tobias' claims shouldn't be dismissed.

"We can all be excused for not having realized this was possible before somebody pointed it out to us, but I think the big question is, now that somebody has figured it

out, how is Medeco going to react? Hopefully Medeco will acknowledge the problem and look for ways to correct it," he says.

Roberson will be discussing the bumping attacks again during his Thursday meeting with Tobias' research partner, and says Medeco is conducting additional tests of the bumping attack with independent testers. He says if he's satisfied that the researchers' claims are true, the company will address the issue.

"There's always a possibility that we're wrong," he says.

Kim Zetter writes about cybersecurity and national security and is the author of Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.

READ MORE

The Best Mattresses You Can Buy Online

I've spent years testing dozens of bed-in-a-box hybrid, foam, and certified organic mattresses.

MARTIN CIZMAR

13 White Elephant Gifts Worth Fighting Over

Bring the gift everyone will want to win from this year's holiday party, from a desk organizer shaped like a pear to magnets they'll wish they could eat.

NENA FARRELL

Breathe Easy—We Found the Best Air Purifiers

WIRED tested and reviewed dozens of air purifiers to find which are the most effective against dust, smoke, allergens, and more. Here are our top picks.

LISA WOOD SHAPIRO

The Best Nintendo Switch Games for Every Kind of Player

From *Super Mario Party Jamboree* to *The Legend of Zelda: Echoes of Wisdom*, these are our absolute favorite escapes for the best portable console.

GEAR TEAM

The Best Android Phones, Tested and Reviewed

Shopping for a phone can be an ordeal. That's why we've tested almost every Android phone, from the smartest to the cheapest—even phones that fold—to find those worth your money.

JULIAN CHOKKATTU

The Best Cozy Games for Long, Cold Nights

Forget stressful leaderboards and time-sensitive missions. These games let you play at your own pace.

LOURYN STRAMPE

The Best Computer Speakers for Jamming Out in Your Home Office

These WIRED-tested computer speakers, from stereo speakers to surround sound, will suit any budget.

SIMON HILL

The Best Folding Phones

Ready to move on from the traditional glass slab? Introduce a hinge into your life with our favorite folding smartphones.

JULIAN CHOKKATTU

The Best MagSafe Accessories for Your New iPhone

The weird, wonderful world of MagSafe accessories can make your smartphone feel modular. These are our favorites.

JULIAN CHOKKATTU

The Best Umbrellas to Help You Ride Out the Rain

These are the best umbrellas we've tested. They'll protect you from showers and heavy rain and will hold up for the long haul.

JULIAN CHOKKATTU

The Best Kindles to Take Your Library Anywhere

Here's how Amazon's ebook readers stack up—and which one might be right for you.

BRENDA STOLYAR

The 11 Best TVs We've Tested (and Helpful Buying Tips)

From QLEDs to fancy OLED models, these are our favorite televisions at every price.

RYAN WANIATA