KIM ZETTER 08.08.08 11:19 AM

Researchers Crack Medeco High-Security Locks With Plastic Keys

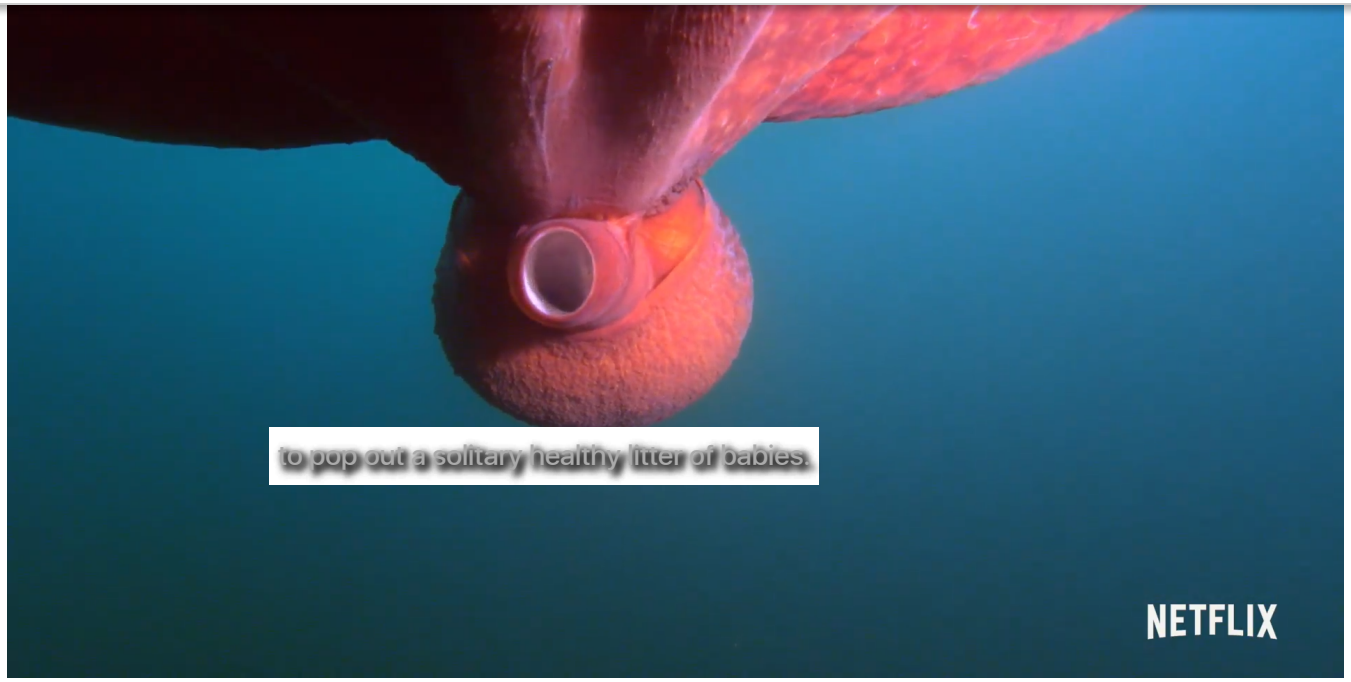
Marc Weber Tobias and two colleagues discovered that they could create plastic keys to open Medeco's M3 high-security locks, despite key control measures designed to thwart key duplication.

conference Friday in Las Vegas, Medeco high-security locks take Visa, too. As well as MasterCard, American Express and Discover cards.

To be more precise, the researchers say that plastic used in all of these credit cards can be easily fashioned into simulated keys that open three kinds of M3 high-security locks made by the Virginia-based Medeco Security Locks company – locks that are used to secure sensitive facilities in places such as the White House, the Pentagon, embassies and other buildings.

"Virtually all conventional pin-tumbler locks are vulnerable to this method of attack, and frankly nobody has really considered it or looked at it before," says Marc Weber Tobias, one of the researchers.

The researchers showed Threat Level how they could create the simulated keys from plastic simply by scanning or photographing a Medeco key, printing the image onto a label and placing the label onto a credit card or other plastic to cut out the key with an X-Acto blade or scissors and then use the key to open a lock covertly.



SCIENCE

Absurd Planet: WIRED's Absurd Creatures Series Gets New Life on Netflix

Any credit card plastic will do to create a simulated key, as will Shrinky Dinks plastic, which comes in sheets that can be run through a printer. For the digital picture of the original key to work, the image has to be to scale.

Images of a Medeco key printed on a sheet of adhesive labels.
*Photo: Dave Bullock (eecue)/Wired.com*The researchers can make plastic keys, despite the

Tobias, an investigative lawyer who will be demonstrating the hack with Matt Fiddler, a computer-security researcher, and Tobias Bluzmanis, a Florida locksmith. "Key control is supposed to make this impossible to happen. That's what you're paying for."

High-security locks – which can cost two to four times the price of a common Kwikset lock used in most homes – have millions of possible key combinations, as opposed to just thousands in low-security locks. High-security locks also use patented key-control systems to prevent just anyone from duplicating the keys.

What this means is that only specific locksmiths who are authorized by the lock maker are given key blanks, key codes and equipment to make the keys. To ensure that no keys are made before a lock is sold, the locks are also shipped to the locksmith without pins in them – the bars inside a lock cylinder that engage with the grooves on a key to open the lock. The pins are added by the seller after a customer purchases the lock, using proprietary key codes doled out to locksmiths by the lock manufacturer.

If a buyer wants additional keys made for the lock later on, he has to return to the same seller to have him make the keys or find another locksmith who is authorized to use that particular key code. Keys used in places like the White House would likely use an even higher level of key control, whereby only the manufacturer – Medeco – would be able to make duplicate keys.

At least in theory.

"Basically, we've destroyed Medeco's key control, because we can make (plastic keys) for any of their M3 locks and a lot of their Biaxial locks, which is their last generation of locks," says Tobias, who authored the book *Open in Thirty Seconds*, with Bluzmanis.

The researchers demonstrated the technique using a Medeco mortise cylinder that Threat Level purchased in California before leaving for Las Vegas. After buying the lock, Threat

seconds to open the lock using a plastic key.

"It's keys by e-mail," says Tobias. "It's key-mail."

Locksmith Tobias Bluzmanis cuts out a key printed on Shrinky Dinks plastic.
*Locksmith Tobias Bluzmanis cuts out a key printed on Shrinky Dinks plastic.*The attack requires brief access to a high-security key long enough to take a picture of it with a camera phone or scan it, so it will likely have to involve an insider or someone else with access to keys – such as a valet parking attendant.

"You're an employee and you loan it to somebody or your kid takes it off your key ring and makes a copy and tells his friends to break into the facility – I can give you a lot of scenarios," Tobias says. "Insiders are always the biggest threat."

Medeco urges companies to implement internal key-control measures to track who has keys and make sure employees are vigilant about handling them. But Tobias says that because people think Medeco M3 high-security keys cannot be easily duplicated, they're not as careful as they should be.

"If you're a security manager for the Federal Reserve or Citibank, you have a belief that what the company is telling you is true, that unless it's authorized, nobody can reproduce your keys," Tobias says. "So if you give a key to an employee you don't have to worry about

rim and interchangeable cylinder locks.

The method doesn't work with other high-security locks, such as those made by Assa, Abloy, Schlage, Mul-T-Lock, and Kaba.

A plastic key inside an opened Medeco mortise cylinder.
*Photo: Dave Bullock (eecue)/Wired.com*Medeco's keys have a special feature in that the bitting on them (the peaks and valleys) is cut at different angles and different offsets (spacing). The patented, integrated design works so that the bitting performs two functions, lifting the pins and rotating them.

The fact that both functions are integrated into one feature makes it easy, Tobias says, to create a simulated key. By contrast, other high-security locks require extra features on their keys to open the lock – for example, Schlage's Primus lock has side-bit milling, which can't be reproduced on a plastic key.

The Medeco M3 key does have an extra feature to secure the lock – a step protrusion on the side of the key that's designed to move a slider inside the lock. But last year at DefCon, Tobias and his colleagues showed how they could simply insert the end of a bent paper clip into a Medeco high-security lock to push back the slider, rendering the slider ineffective as a security layer. Once that is done, they're then able to insert the plastic key in this new

which makes inserting a plastic key and paper clip easy. Once the plastic key is inside the cylinder and lifts the pins, it's not actually strong enough to turn the cylinder, so the researchers insert a small turning wrench to turn the cylinder and open the lock.

The researchers say they were able to open Threat Level's lock with covert methods because they were able to determine the angles of the bitting from the scanned picture of the key. Had the picture been poorer quality, they still could have created a key to lift the pins, but they would have had to use a forced-entry technique to break the cylinder and open the lock.

A Medeco mortise cylinder with a bent paper clip and plastic key.
*Photo: Dave Bullock (eecue)/Wired.com*The researchers say the issue of the plastic keys is more serious than what they revealed last year at DefCon, when they demonstrated how they could bump and pick Medeco's patented M3 Biaxial and deadbolt locks – locks that Medeco claimed were bump- and pick-proof. They were able to create bump keys for the locks after spending months analyzing Medeco's published key codes.

But by using plastic keys, the researchers can now crack the M3 locks in a way that doesn't require knowledge of key codes or any significant skills or equipment, although it does require brief access to a key to copy it.

rethink everything he once believed about Medeco locks.

"Basically if someone came to me (before) and said they could pick a Medeco lock, I'd say, 'You're crazy; you don't know what you're talking about.' If they told me they could open it with plastic, the same thing. I'd say, 'You're crazy.'

"Locksmiths don't have a clue what is going on. Your locksmith will tell you this is impossible."

See also:

- White House High-Security Locks Broken: Bumped and Picked at DefCon
- Medeco Readies Assembly-Line Fix for DefCon Lock Hack

#DEFCON #HACKS

More Stories

DEALS

30 Best Memorial Day Deals on Tech, Gaming, Home, and More

LAUREN STRAMBO AND WIRED STAFF

MISINFORMATION

The DHS Prepares for Attacks Fueled by 5G Conspiracy Theories

JON BRODKIN, ARS TECHNICA

BUYING GUIDE

The 7 Best Portable Grills You Can Buy

SCOTT GILBERTSON

WHILE YOU WERE OFFLINE

The Willis Tower Looks Creepy With the Lights Off

GRAEME MCMILLAN

ROUGH RIDE

Informal Transit Is Crucial for Some. Can It Weather Covid?

FLAVIE HALAIS

CLEVER TWIST

A Grad Student Solved the Epic Conway Knot Problem—in a Week

ERICA KLARREICH