KIM ZETTER BUSINESS AUG 2, 2010 8:03 AM

'Gross insecurity' of high-tech locks exposed

SAVE

IT WOULDN'T BE DefCon without a noted lock hacking team demonstrating the gross insecurity of some of the latest security locks, such as a biometric lock that could be easily cracked with a paper clip.

This year the three-member team of lock hackers, Marc Weber Tobias, Toby Bluzmanis and Matt Fiddler who have been cracking locks at DefCon for several years, also defeated an electro-mechanical lock, two deadbolts, and an electronic safe. The researchers gave Wired.com a sneak peek at their cracks and provided videos, which you can see below.

The lock that would seem to have thwarted them the most was actually one of the easiest to crack. The Biolock Model 333 is a sleek £126 ($200) lock that combines a mechanical cylinder and fingerprint reader.

The Biolock fingerprint reader illuminates a blue LED when a fingerprint is authenticated. If the reader fails, a key can be inserted in a key port hidden behind a flip door in the handle.

“It’s a very neatly designed container,” says Tobias. “But the problem with this lock design is so elementary, frankly it defies belief.”

The lock can be programmed with one or more “master” fingerprints, which can be used to authorise other users. To open the lock, a user touches the fingerprint pad, and a blue LED light illuminates to indicate the person is authorised, allowing the door handle to turn. The lock can also be unlocked with a remote-control.

If the fingerprint reader fails, a mechanical key can be used instead. The key entry is concealed beneath a flip door on the lever handle. And therein lies the security problem, Tobias says.

A paperclip inserted in the Biolock's key chamber (hidden behind a flip door) is used to push an internal pin and unlock the door, making the fingerprint reader superfluous.

The mechanical lock, which uses a bypass cylinder, can be easily thwarted with a paperclip inserted in the keyway to depress a pin that engages the latch. In two seconds, the researchers were able to open the lock.

“This is an absolute perfect example of insecurity engineering,” Tobias says.

Biolock did not respond to a request for comment.

The researchers also tackled a smartkey deadbolt from Kwikset, which makes some of the most widely used locks in the US The smartkey technology allows someone to easily programme the lock with a reset tool to accept specific keys, making it popular with apartment building owners who can re-programme the lock when a tenant moves out.
The lock’s packaging touts it as certified at grade-one security level -- the highest for residential locks. The researchers, however, were able to crack the lock with only a key blank cut to a specific depth and a screw driver.

They put the blank into the lock, inserted a screw driver to push the blank into the chamber, then used a small vice grip to turn the screw driver and open the lock.

They would need to remove the blank using a wire to make the lock operational for other keys. Major Manufacturers also makes a £57 ($90) locksmith tool that consists of a T-rod with a blank attached to the end to replace the screwdriver and blank.

“The entire security of this system rests on tiny little sliders that are being warped in this process,” says Tobias, noting that the crack doesn’t take any expertise to conduct. Ironically,

Kwikset's packaging for the lock includes a statement that says, "All you need is a screw driver." The slogan refers to installing the lock, but "either way," says Tobias, "it is essentially a very true statement."

Kwikset spokesman Brent Flaharty said in an email statement that the company couldn't respond to the researcher's claims without seeing a video of the hack. He added that Kwikset's locks have "passed the most stringent lock-picking standard."

But Tobias says that the standards are part of the problem, since they don't test for many real-world lock-cracking techniques.

"You read the packaging and yes they are certified as grade-one. But they ought to be putting on the package that there are tools and techniques that can open these locks in 30 seconds or less," he says. "Obviously they won't do that, because no one will buy their locks."

Next, the researchers cracked the AMSEC electronic safe Model es1014. The safe is not high security, but is marketed for home and small businesses and sells for about £57 ($90).

A piece of metal from a hanging file folder is slipped into the AMSEC safe to access a reset button inside the safe.

It has a digital keypad that can be programmed with up to eight numbers. Inside the safe, is a reset button on the back of the door to change the combination. Little thought apparently went into the position of the button, however, because the researchers found they could reach it with a flat metal piece used for hanging file folders. Bluzmanis slipped the metal into the narrow space between the closed door and frame, flipped it around and pressed the reset button, allowing him to reprogram the combination to anything he wanted and open the door. AMSEC did not respond to a request for comment.

The most impressive lock they examined, the iLoq C10S, is an electro-mechanical lock that combines electronic key authentication and audit trail with a mechanical lock. The researchers were able to disable the electronic portion, allowing unauthorised users to gain entry without being tracked. The attack requires modification of an authenticated key supplied either from an insider or through borrowing or theft.

The iLoq has a unique award-winning design that differs from other electro-mechanical locks: it has no battery, either in the lock or in the key. Instead, the processor for authenticating keys is powered by a mechanical motor inside the lock. Unfortunately, the clever design works against the lock's security, Tobias says.

The lock operates in four stages. As a key is inserted, the motor wakes the processor to authenticate the key. Then the motor turns a gear to start the mechanical system. As the key travels through the keyway, it lifts a nylon pin that lifts a second metal pin, allowing the lock chamber to turn. The lock resets when the key is removed.

The hack involves filing off a tiny hook at the tip of an authenticated key, which would take less than a minute to do, Tobias says.

The iLock key has a small hook on the end that catches another hook inside the lock to reset the lock. When the hook is filed off the key, the lock can't reset, and the electronic part of the key is disabled, allowing even simulated keys to open the lock.

When the key is inserted, it's authenticated by the processor, and the pins lift to open the door. But absent the hook on the end of the key, it's unable to catch a second hook inside the lock to reset the mechanical portion that generates energy for the processor. With the processor dead, any simulated key, non-authenticated key or even a screw driver can be inserted to lift the nylon pin that lifts the metal pin and opens the lock. The modified key would be in the audit trail, so investigators would be able to identify who owned that key, but not necessarily who modified it.

A second attack involves using a little Dremel tool that costs about £38 ($60). In this attack, the researchers insert the tool to shave off the hook inside the lock. The result is the same as the previous hack, with one caveat. The first key inserted after the hook is shaved must be an authenticated key; if an unauthenticated key, the lock will be disabled for any authenticated key thereafter.
An iLock spokesman said the hacks were unrealistic.

"Cutting off a part of an iLOQ key with the purpose of enabling the next key inserted to open the lock successfully, even [while] having no access rights, is a very complicated and stupid way to give access to a criminal companion," said spokesman Michael Szücs in an email. "Much easier it would be to leave a window open."

The last lock they tackled was the KABA InSync deadbolt, a battery-operated electronic lock combined with an RFID key. To crack this one, the researchers simply inserted a small wire into the communication port at the bottom of the lock, and pushed a locking bar inside, allowing them to open the door.

KABA did not respond to requests for comment.

Here are some videos of the locks being hacked:

<object width="404" height="436"
data="http://c.brightcove.com/services/viewer/federated_f9/1813626064?isVid=1"
type="application/x-shockwave-flash" id="flashObj">

<param name="bgcolor" value="#FFFFFF" />

<param name="flashVars"
value="videoId=2753671710O1&playerID=1813626064&domain=embed&dynamicStreaming=true"
/>

<param name="base" value="http://admin.brightcove.com" />

<param name="seamlesstabbing" value="false" />

<param name="allowFullScreen" value="true" />

<param name="swLiveConnect" value="true" />

<param name="allowScriptAccess" value="always" />

<param name="src" value="http://c.brightcove.com/services/viewer/federated_f9/1813626064?
isVid=1" />

<param name="name" value="flashObj" />

<param name="flashvars"
value="videoId=2753671710O1&playerID=1813626064&domain=embed&dynamicStreaming=true"
/>

<param name="allowfullscreen" value="true" />

</object>

<object width="404" height="436"
data="http://c.brightcove.com/services/viewer/federated_f9/1813626064?isVid=1"
type="application/x-shockwave-flash" id="flashObj">

<param name="bgcolor" value="#FFFFFF" />

<param name="flashVars"
value="videoId=2753671710O1&playerID=1813626064&domain=embed&dynamicStreaming=true"
/>

<param

<param name="seamlesstabbing" value="false" />

<param name="allowFullScreen" value="true" />

<param name="swLiveConnect" value="true" />

<param name="allowScriptAccess" value="always" />

<param name="src" value="http://c.brightcove.com/services/viewer/federated_f9/1813626064?isVid=1" />

<param name="name" value="flashObj" />

<param name="flashvars" value="videoId=275367171001&playerID=1813626064&domain=embed&dynamicStreaming=true" />

<param name="allowfullscreen" value="true" />

</object>

<object width="404" height="436" data="http://c.brightcove.com/services/viewer/federated_f9/1813626064?isVid=1" type="application/x-shockwave-flash" id="flashObj">

<param name="bgcolor" value="#FFFFFF" />

<param name="flashVars" value="videoId=275360734001&playerID=1813626064&domain=embed&dynamicStreaming=true" />

<param name="base" value="http://admin.brightcove.com" />

<param name="seamlesstabbing" value="false" />

<param name="allowFullScreen" value="true" />

<param name="swLiveConnect" value="true" />

<param name="allowScriptAccess" value="always" />

<param name="src" value="http://c.brightcove.com/services/viewer/federated_f9/1813626064?isVid=1" />

<param name="name" value="flashObj" />

<param name="flashvars"
value="videoId=275360734001&playerID=1813626064&domain=embed&dynamicStreaming=true"
/>

<param name="allowfullscreen" value="true" />

</object>

<object width="404" height="436"
data="http://c.brightcove.com/services/viewer/federated_f9/1813626064?isVid=1"
type="application/x-shockwave-flash" id="flashObj">

<param name="bgcolor" value="#FFFFFF" />

<param name="flashVars"
value="videoId=275376235001&playerID=1813626064&domain=embed&dynamicStreaming=true"
/>

<param name="base" value="http://admin.brightcove.com" />

<param name="seamlesstabbing" value="false" />

<param name="allowFullScreen" value="true" />

<param name="swLiveConnect" value="true" />

<param name="allowScriptAccess" value="always" />

<param name="src" value="http://c.brightcove.com/services/viewer/federated_f9/1813626064?
isVid=1" />

<param name="name" value="flashObj" />

<param name="flashvars"
value="videoId=275376235001&playerID=1813626064&domain=embed&dynamicStreaming=true"
/>

<param name="allowfullscreen" value="true" />

</object>

This article was originally published by WIRED UK

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.

TOPICS TECHNOLOGY HACKING

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