Schneier on Security

Locksmiths Hate Computer Geeks who Learn Lockpicking

They do:

> Hobby groups throughout North America have cracked supposedly unbeatable locks. Mr. Nekrep, who maintains a personal collection of more than 300 locks, has demonstrated online how to open a Kensington laptop lock using Scotch tape and a Post-it note. Another Lockpicking101.com member discovered the well-publicized method of opening Kryptonite bike locks with a ball-point pen, a revelation that prompted Kryptonite to replace all of its compromised locks.
>
> Other lock manufacturers haven't admitted their flaws so readily. Marc Tobias, a lawyer and security expert, recently shook up the lock-picking community by publishing a detailed analysis of how to crack the uncrackable: Medeco locks.
>
> "We've figured out how to break them in as little as 30 seconds," he said. "[Medeco] won't admit it, though. They still believe in security through obscurity. But by not fixing the problems we identify, lock-makers are putting the public at risk. They have a duty to disclose vulnerabilities. If they don't, we will."

Tags: disclosure, locks, physical security, vulnerabilities

Posted on July 17, 2008 at 1:30 PM • 46 Comments

Comments

Anonymous • July 17, 2008 1:41 PM

practiced some of these tricks back in 1972 when skill was still in the fingers and the mind.

Chris • July 17, 2008 2:07 PM

The lock industry needs to modernize and have experts extensively test their products, just like everybody else. Welcome to the new world, lockmakers.

---

sooth sayer • July 17, 2008 2:17 PM

Locks are for honest people to feel good; I don't think there ever was an unbreakable lock.

twofish .. that's another (fishy) story altogether.

---

bob • July 17, 2008 2:24 PM

Yeah; if hobbyists dont talk about it, criminals will NEVER find out.

I first started learning how locks worked when someone stole my locked-up bicycle in 6th grade (and for icing on the cake, they left the lock laying there locked where the bike had been).

For key locks, Ive always preferred my pocket screwdriver and a (heavy) paperclip, although a leatherman is handy to bend the paperclip with. Several times I have had to let people into their own desks. One time I needed to get at locked-up letterhead to print a contract on when a secretary was out sick.

Roy • July 17, 2008 2:26 PM

Bump keys were 'outed' about five years ago, yet the key manufacturers don't seem worried about the problem. If your locks get bumped, and you complain, they'll just say to get the lock rekeyed. Ka-ching, another sale, it's money in the bank.

Urox • July 17, 2008 2:33 PM

Actually, the first problem I encountered with the kryptonite U-lock was that it had a *plastic mechanism* inside the lock. Crowbar beats plastic.

Nomen Publicus • July 17, 2008 2:36 PM

Many "locks" are little more than security theatre as you can find out from reading "Surely you're joking, Mr. Feynman!" by Richard Feynman.

The fun Richard would have had with our pathetic attempts to prevent anything bad happening to anybody, ever.

RockDoggy • July 17, 2008 2:54 PM

Scotch tape and a post-it note? MacGyver would be proud!

Lockguy • July 17, 2008 2:55 PM

Marc Tobias has not published "a detailed analysis" of how to defeat the Medeco lock. His position is the antithesis of ethical hacking - he published a seriously incomplete video (with the crucial steps cut out), no details of how it was done and to date no one has been able to replicate what he claims he did, including Medeco. Medeco has no way to respond to this. Tobias does not deserve to be mentioned on Schneier.com.

FDHY • July 17, 2008 3:20 PM

No Tech Hacking is much easier :)

Rapier57 • July 17, 2008 3:31 PM

The Kryptonite locks we happily opened with the old plastic Bic (TM) pens back in my high school days were actually replaced with locks that are very easy to pick, even today. Simple picking tools and little skill required. The old Kyptonite barrel locks at least required some skills. An associate demonstrates this in a physical security presentation.

---

brasscount • July 17, 2008 3:46 PM

So, did Medeco pay out on their million dollar challenge?

---

aph • July 17, 2008 3:47 PM

Even with the best, unbreakable lock, it will only prevent undetectable unauthorized entry, and make brute force entry only slightly harder. Even the Medeco locks can't stop someone from kicking your door down or breaking a window. While either of those are noisier and more likely to draw attention to the perpetrators, it's still not going to stop the "smash and grab."

If someone wants in to your house, a lock isn't much of a deterant. They only stop the casual thief.

The CameraMan • July 17, 2008 4:03 PM

Just two hours after this was posted, Wired.com posts "How to bump a lock" (http://howto.wired.com/wiki/Bump_a_Lock unlinked because my mad html skillz are sadly lacking). Coincidence?

And to aph: "only" stopping a casual thief is a valuable contribution. Most thieves are what you term "casual" thieves. Assuming you aren't a big juicy target, stopping casual thieves may be good enough. It's certainly better than nothing.

The CameraMan • July 17, 2008 4:04 PM

Oh, I spoke too soon: it linked itself automatically. i love the interwebs.

---

alan • July 17, 2008 4:08 PM

Liquid nitrogen and a hammer beats most locks.

A "true-temper lockpick" (a 20# sledgehammer) also works wonders.

With physical locks sometimes security theater is helpful. My current bike lock has a cable on it the thickness of a Red Bull can. Bite thieves don't even look twice. They just figure it is too hard and move on to an easier target. (Then again, most bike thieves seem to be rather unsophisticated and just cut the chain.)

In the world of crime (as in anything else) the only two groups you really worry about are the skilled professionals or the obsessed hobbyists.

The CameraMan • **July 17, 2008 4:16 PM**

Actually, the obsessed hobbyists aren't out to cause harm, so you really only have to fear the skilled professionals...

---

golux • **July 17, 2008 4:16 PM**

Actually with some duct tape and a tig welder electrode, breaking a window can be very silent. All you need is access to the latch on the back side, not complete glass removal. Dual pane windows would be a little more tricky.

---

ntokb3 • **July 17, 2008 4:33 PM**

A wise man once said that "locks are there to keep honest people honest..." Thanks dad.

Timm Murray • **July 17, 2008 4:53 PM**

@sooth sayer:

"Locks are for honest people to feel good; I don't think there ever was an unbreakable lock."

Not entirely true. The modern safe lock can be made invulnerable to everything short of brute forcing the combination with minimal additional design features. See:

http://www.crypto.com/papers/safelocks.pdf

Other ways of getting in (e.g. drilling/tunneling your way through the side of the vault) can be protected against with reasonable levels of additional design combined with good overall procedures.

So why aren't all locks made invulnerable? The design flaws are left deliberately in place in the event of someone forgetting the combination. In computer security, we might tend to frown on deliberate design faults, but it is a real problem that would be foolish to ignore.

FDHY • **July 17, 2008 4:59 PM**

@Timm Murray
"The modern safe lock can be made invulnerable to everything short of brute forcing the combination with minimal additional design features."

It still possibly wouldn't stop social engineering or other no tech attacks.

---

there are better locks • **July 17, 2008 5:27 PM**

Even the classic Abloy isn't the easiest one to pick http://www.youtube.com/watch?v=wyB7DFtVRBk (invented in 1907). Newer models are more advanced.

---

clvrmnky • July 17, 2008 6:03 PM

"Even with the best, unbreakable lock, it will only prevent undetectable unauthorized entry, and make brute force entry only slightly harder."

The problem with some techniques, such as lock-bumping, is that there is no evidence that the lock has ever been compromised. It looks just like some left the lock open (if you are lucky). Good luck with that insurance claim.

So, yes, a lock is only as good as the door/wall/window it is protecting. But, as some have pointed out, it is also a good way of forcing someone to deal with the lock, or try something else more risky. The idea is to turn away or make more difficult so-called casual crime.

A common housebreaker simply tries doors and windows as he or she goes down the street at night.

As with encryption, it is not necessary to have or demand the best, unbreakable lock. The idea is to protect within reasonable limits what you you need to protect. Security is not a go/no go binary decision.

As far as I am concerned, hobbyists are simply keeping the lock companies honest by forcing them to define the parameters of what "good enough" means to /them/.

Example: if any old lock is good enough to lock up your beater bicycle, then I'd rather know that a specific brand will at least challenge a thief long enough that my ride is still there a few hours later. So, there is a difference between a decent lock which may take a little expertise, time or brute force to compromise, and one of the barrel combination locks that anyone can pick with their bare hands in 10 seconds.

Some locks are just more good enough than others.

---

alan • July 17, 2008 6:19 PM

I live in a city where bike thefts are a BIG problem. Most of it is blamed on meth users, though there are rings of bike thieves here as well.

The meth heads will take *anything*. (I once left a bike on my porch that had a broken frame and they stole it. It was almost unridable. I snapped the center post weld next to the crank.)

The bike thief rings usually just cut the cable on the lock. Picking takes to long. You want physical strength of the chain/cable. The lock is pretty much ignored unless it has a well-known flaw or can be cut easy. They want to cut whatever, throw it on the truck and get out of there.

The only lock compromises I have heard about locally are where people have shimmed locks. I have not heard of anyone having a lock picked locally that was not a Kryptonite ball point pen hack.

---

godel_56 • July 17, 2008 6:28 PM

BTW, tinted plastic films applied to the inside of a window will dramatically increase the strength of the glass. Although there are special purpose tough security films that are specially made for the job, even the ordinary light control films will give a burglar a nasty surprise, and a lot more work than they were expecting!

Anonymous • July 17, 2008 6:49 PM

Guard dogs hate computer geeks who pick locks. Picture some geek being chased after defeating a lock, thinking he was thinking.

---

xyzzy • July 17, 2008 7:31 PM

For a while, bike thieves would cut the frame of the bike, slide the lock's shank or chain or cable through the slot, toss the bike in a pickup, then weld the frame back together in the chop shop. Maybe they still do that.

The other one around here was theft of forklifts and skiploaders. The thieves would then use it to rip up an entire ATM, put in the truck, then leave the skiploader or whatever at the scene. It turns out it wasn't that hard to drive off the construction site with the equipment, and since they were only using it for a couple of hours, not much chance of them getting caught for it.

Other lock guy • July 17, 2008 9:43 PM

@Lockguy - There's much more to it than that video. Marc has just published an entire book on the Medeco:
http://www.security.org/
The video was just a teaser.

Don't go smearing people's names like that when you obviously aren't following the issue closely.

---

jesus burns in hell where my soul shall dwell burning for us burning for the lies of his god • July 18, 2008 12:14 AM

stop the press:::::

Schneier, UW Team Show Flaw In TrueCrypt Deniability
http://yro.slashdot.org/article.pl?no_d2=1&sid=08/07/17/2043248

"An anonymous reader writes
"Bruce Schneier and colleagues from the University of Washington have figured out a way to break the deniability of TrueCrypt 5.1a's hidden files. What about the spanking-new TrueCrypt 6? Schneier says that 'The new version will definitely close some of the leakages, but it's unlikely that it closed all of them.' Meanwhile, PC World is reporting that the problems Schneier and colleagues found are bigger than just TrueCrypt. Among their discoveries: Word auto-saves the contents of encrypted files to the unencrypted

portions of your disk, and this problem should apply to all non-full disk encryption software. Their research paper will appear at Usenix HotSec '08.""

http://www.darkreading.com/document.asp?doc_id=159192
http://it.slashdot.org/article.pl?sid=08/07/08/027220&tid=93
http://www.pcworld.com/businesscenter/article/148513/data_can_leak_from_partially_encrypted_disks.html
http://www.schneier.com/paper-truecrypt-dfs.pdf
http://www.usenix.org/events/hotsec08/cfp/

Dirk • July 18, 2008 2:19 AM

I'ts not a problem that any criminal subject can open a lock by force. Nobody believes even the "unbreakable" locks can resist enough force. But if one opens a lock with a sledgehammer, after that anyone can see that someone did. If you pick a lock with skill, it shows no obvious marks. You can't simply tell anyone broke in.
Locks are used to prevent simple access. You want to have it obvious when they fail.

To the locksmiths: another example that security by obscurity never works for long.
Shure there is a lot of money on the line and a lot of trust because your whole business is based on trust. But, by outlawing people who show you the faults you won't earn any trust back.

---

there are better locks • July 18, 2008 2:25 AM

Virtually pick proof lock. The video is commercial, but explains pretty well the mechanics of the lock.
http://www.abloy.com.au/videos/Abloy_Protec.wmv

---

there are better locks • July 18, 2008 2:50 AM

Forgot to mention this pdf from Toool: http://www.toool.nl/abloypart3.pdf

---

Sparky • July 18, 2008 3:04 AM

Is there any kind of consensus for responsible disclosure for flaws in locks?

Locks usually can't be "patched" in the field, and most of the time, the lock manufacturers don't even know who bought their locks. Responsible disclosure would probably mean wait until the manufacturer has recalled most of the locks, or a number of years so that most of them have been replaced because of old age.

What surprises me, is the simplicity of most of these breaks. That, combined with the fact that nearly all of them are class-breaks, and there is only one severity level (full break, as opposed to fishing/XSS/privilege escalation/remote code execution/DoS attacks), makes this a rather difficult situation.

Nostromo • July 18, 2008 4:59 AM

"If someone wants in to your house, a lock isn't much of a deterant. They only stop the casual thief."

All thieves who break into normal houses are casual thieves. You can't make $100k/year by burglary. What's the resale value of the stuff in your house?

The only people with significant resources who are likely to break into your house are law enforcement, and nowadays they don't bother with locks, they just smash your front door down.

Raimundo • July 18, 2008 7:40 AM

www.lockpickernetwork.wikidot.com

youtube search medeco picking lockpicking medeco
also multilock pick
disc detainer pick

the truth is out there

Patrick Austin • July 18, 2008 8:31 AM

I read the police blotter every day, and there are a lot of break ins, but I don't know as I've ever read about a lock being picked. It's always either a door left unlocked or a screen cut out or whatnot. Guys breaking and entering while you're at work are probably not the types who read the lock picking forums and have the cash to buy 300 locks to practice on. :)

Oshik Amiga • July 18, 2008 12:43 PM

Very Nice ...

Thankyou

http://www.greenlocksmith.com/

Skorj • July 18, 2008 4:10 PM

" I don't know as I've ever read about a lock being picked. It's always either a door left unlocked or a screen cut out or whatnot. "

Lock bumping cannot be distinguished from a "door left unlocked" after the fact. While most breakins are smash-and-grab, lock bumping is as easy as throwing a brick through a window, and requires only slightly more complicated tools.

OTOH, living on the second floor is a huge deterrent against smash-and-grab: never underesimate the laziness of casual thieves.

Jaakko Fagerlund • **July 18, 2008 4:55 PM**

I have done a responsible discovery in the realms of locksport and it was so small flaw and only an attack method that would be used by the true professional or obsessed hobbyist, so after discovery I went public after a six month period during which the manufacturer (ABUS) made a change to their product line.

If anyone wants to see the what kind of problem it was, here is a PDF:
http://koti.mbnet.fi/einstein/lp101/ObtainingAbusPlusKeyCode.pdf

Also at the same time my friend Jonathan King made a success and a responsible discovery story on Medeco locks and this was also a great step in getting locksport enthusiast involved with the industry.

Scote • July 19, 2008 6:38 PM

"OTOH, living on the second floor is a huge deterrent against smash-and-grab: never underesimate the laziness of casual thieves."

Actually, thieves often **love** the smugness of people with second story windows and doors. A second story entrance is often concealed from street view which makes for unobserved ingress and egress and people often leave second story windows and balcony doors unlocked.

Never underestimate that thieves already know how to take advantage of what you smugly think is an advantage.

Michael E. Gruen • **July 20, 2008 3:09 PM**

Funny story about Marc Tobias--

Few years ago, I attended DefCon and watched Tobias talk about security and knowing your adversary and so forth. Finding the talk rather fluffy, I walked out and into a lounge area where one hacking group projected a Wall of Sheep-- that is, a listing of all of the e-mail/password/url combinations that were visible with trivial/no encryption.

There, on the wall, was a laptop betraying its owner every 30 seconds:
mtobias | eni*** | pop.security.org

Amusing, for sure, for many reasons.

Davi Ottenheimer • **July 20, 2008 5:01 PM**

Hobby groups are never very popular among the commercial crowd. It goes beyond security by obscurity, and into the economics and ethics of marketing. What constitutes "good-enough" for profit? Those who tinker have time on their side to challenge assumptions, which presents a serious risk to the margins of the companies who do not want to pay for people to tinker. If you work inside an American company and demonstrate a security flaw, don't be surprised if the response is "your standards are too

high -- who says this needs to be perfect" or "if there is such an obvious problem then why have x million people purchased already?"

---

bob • July 21, 2008 9:34 AM

@Davi: Actually if you work inside an american company, are not a relative of the president of the company and demonstrate a security flaw in their product (not one you could have remotely caused), you will probably be castigated, demoted or fired for "causing trouble".

Drebin • July 21, 2008 11:06 AM

This reminds me of the classic Police Squad line:

"Who are you and how did you get in here?"

"I'm a locksmith and ... I'm a locksmith".

John Ridley • July 22, 2008 9:35 AM

I made a master key for our dorm when I was a student there. It was never abused; we just used it for urban exploration in the storage rooms and mechanical rooms, and to let people in to their rooms if their roommates locked them out or something (I only let in people if I knew them and where they lived). Eventually the MA found out about it, and I had to give it up. He asked how I made it and I told him "it's just a simple lock, it's totally obvious to anyone who takes 5 minutes to think about the problem. Anyone could do this in a half hour with just a duplicate key and a chainsaw file. I saw a picture of how locks work in the Junior World Book encyclopedia when I was 8, I could have done it then." He was a humanities type in an engineering college, so I don't think he appreciated that comment.

Calum • July 22, 2008 10:27 AM

@Scote

Here in Edinburgh, where we have large numbers of tenements with blocks of 6-8 apartments sharing a common stair, the favoured attack method is to climb to the top and knock on each door. If there's a response, pretend to be lost. If not, kick it in and help yourself in the knowledge no-one will walk past and notice the kicked in door. Top floor insurance premiums are roughly double the other floors for this reason.

Subscribe to comments on this entry

Comments on this entry have been closed.

← Homeland Security Cost-Benefit Analysis TrueCrypt's Deniable File System →