How The Lock Industry Put Its Head In The Sand, Rather Than Deal With Vulnerabilities To Locks

from the *bump,-bump-away* dept
Fri, May 29th 2009 5:30pm — **Mike Masnick**

Too Much Free Time

We've discussed in the past how locksmiths are apparently upset that geeks online have **revealed that lockpicking is really easy**, but it's not just the locksmiths. It's the lock makers themselves. Wired has a fascinating article about one of the world's **most well known lock picker**, who makes it a practice to publicly expose how vulnerable certain locks are. Not so long ago, he and a colleague figured out how to quickly open Medeco locks, which many had considered to be the most secure locks of all -- and are used all over the world in gov't high security buildings. So how has Medeco responded? Basically by trying to ignore the guy... then to insult him and then to discount what he clearly has done. It's just like software companies who try to deny software vulnerabilities, except that it's much easier to patch some software that to patch a vulnerable lock. While many in the lock world are apparently pissed off at this guy, Marc Weber Tobias, they should be happy that he's making sure the locks are really secure. Because, you can pretty much be assured that he's not the only one doing all of this -- but the others who are figuring it out aren't talking about it, but are using the knowledge to their own advantage.

Essential Reading

Hot Topics

5.3 Laying Out All The Evidence: Shiva Ayyadurai Did Not Invent Email

5.1 Funniest/Most Insightful Comments Of The Week At Techdirt

5.1 As Record Labels Still Are Demanding Mandated Filters; Facebook's Copyright Filter Takes Down A Guy Playing Bach

New To Techdirt?

Explore some core concepts:

Step One To Embracing A Lack Of Scarcity: Recognize What Market You're Really In

Advertising Is Content; Content Is Advertising

The Grand Unified Theory On The Economics Of Free

read all »

Filed Under: lock picking, marc weber tobias, obscurity, security
Companies: medeco

60 Comments | Leave a Comment

If you liked this post, you may also be interested in...

- FTC The Latest To Discover 'Smart' Locks Are Dumb, Easily Compromised
- Senator Blumenthal Is Super Mad That Zoom Isn't Actually Offering The End To End Encryption His Law Will Outlaw
- Teleconferencing Company Zoom Pitching End-To-End Encryption That Really Isn't End-To-End
- Security And Privacy In A Brave New Work From Home World
- Cybersecurity Firm Hired By Voatz To Audit Its System Finds Voatz Is Full Of Vulnerabilities

Reader Comments

View by: Time | Thread

Subscribe: RSS

Bettawrekonize, *29 May 2009 @ 5:59pm*

If someone wanted to get in your house badly enough they'll simply break your window or something. If someone really had something to secure they would spend more money on more reliable security. Locks aren't meant to be foolproof but neither are Windows and doors. People can kick doors down, etc... People shouldn't rely on a lock to protect them from a determined burglar.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 6:08pm*

Re:

+1 on this.

Locks are really intended to keep out the casual thief, someone who would just walk in. Most people are not going to pick locks or bust down a door to get in, they aren't interested in attracting attention to themselves. Think of doorlocks as a solution that is 99% effective. The last 1% will get in pretty much no matter what you do.

[reply to this | link to this | view in chronology]

Bettawrekonize, *29 May 2009 @ 6:11pm*

Re: Re:

Exactly my point.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 7:54pm*

Re:

If someone really had something to secure they would spend more money on more reliable security.

Such as?

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 8:01pm*

Re: Re:

Armed guards for a start. All a lock does is slow someone down. Ideally it will slow them down enough to catch them in the act. For a truely secure facility you plan you guard patrolls based on how long the lock will take to pick.

[reply to this | link to this | view in chronology]

zcat, *29 May 2009 @ 8:54pm*

Re: Re: Re:

Exactly the point.

If you've been told (by the manufacturer) that the lock takes at least half an hour to pick and you have fifteen-minute security patrols you're going to feel pretty safe, right.

You're not going to feel quite so safe when Marc Weber Tobias walks in and picks that lock in fifteen seconds.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 11:22pm*

Re: Re: Re:

Or you have cameras with monitors in various places, like they do in stores, that allow employees to constantly watch things from various places.

[reply to this | link to this | view in chronology]

Recent Stories

Sunday

13:00 Funniest/Most Insightful Comments Of The Week At Techdirt (0)

Saturday

12:00 This Week In Techdirt History: April 5th - 11th (2)

Friday

19:39 Happy Birthday, Statute of Anne (32)

15:43 Apple, Google Join Forces To Create Free Tools For Coronavirus Tracking (11)

13:37 FTC The Latest To Discover 'Smart' Locks Are Dumb, Easily Compromised (12)

12:08 'Free Speech' Supporter Jerry Falwell Jr. Thinks It's Criminal To Report On His Dumb And Dangerous Response To The Pandemic (40)

10:46 Opening Up Information In A Pandemic, Rather Than Locking It Down: The Open COVID Pledge Is Important (6)

10:41 Daily Deal: Cudoo Pro Online Learning (0)

09:27 Court Dumps Almost All Of A New York Sax Player's Lawsuit Against Fortnite Over Use Of His 'Likeness' (17)

06:22 Corporations Not Happy Innovators Have 'Hacked' The Crappy U.S. Binding Arbitration System (56)

More

Advertisement

Anonymous Coward, *29 May 2009 @ 11:23pm*

Re: Re: Re:

I can't walk into a store without seeing a cameras pointed at me, and when I walk to the cashier there is a monitor, yes, a monitor that has like four windows each following different cameras.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 11:19pm*

Re: Re:

Surveillance (cameras), an alarm system, or even security guards (if it's that important). A gun.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 11:36pm*

Re: Re: Re:

Also a safe. In the case of money we have banks.

[reply to this | link to this | view in chronology]

Dominic Sayers, *1 Jun 2009 @ 2:02am*

Re: Re: Re: Re:

in the case of money we have banks Have you been asleep for the last 2 years?

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 6:33pm*

Those arguments about locks simply being there to stop casual thieves are rendered moot by the fact that complex locks exist.

If it were simply the case that locks are there to keep out someone who would otherwise just stroll in, but can't be bothered forcing a door, then all locks would be simple ones. But they're not.

Some people, and companies, have gone out of their way to use locks that are supposedly hard to pick or otherwise force. And apparently, they're not that hard to pick or force at all. It's an important thing that the manufacturers and consumers need to realise, rather than just ignore.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 6:39pm*

For some, it takes 5 minutes, others it may take 5 hours to break a lock. It depends on the skills of the user. Nonetheless, the result is all the same. It's all about the skill, right? Why not just be honest with us?

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 6:42pm*

Locks only keep honest people out.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 7:58pm*

Re:

Locks only keep honest people out.

You don't need locks to keep honest people out.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 6:47pm*

No, there's hidden meaning here.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 6:57pm*

Kinda sad, actually.

[reply to this | link to this | view in chronology]

Alias (profile), *29 May 2009 @ 7:07pm*

+ + FW LW

Locks

...are only made to keep honest people out. If someone wants in bad enough, they'll get in. Period.

[reply to this | link to this | view in chronology]

BTR1701, *1 Jun 2009 @ 6:40am*

+ + FW LW

Re: Locks

> ..are only made to keep honest people out.

This little cliche never made any sense to me. An honest person wouldn't enter someone's home uninvited regardless of whether there was a lock or not.

[reply to this | link to this | view in chronology]

What, *29 May 2009 @ 7:09pm*

+ + FW LW

Uhhh... Article Fail.

Medeco being cracked, old news. Lock companies not liking it, old news.

Why the fuck is this on Techdirt?

[reply to this | link to this | view in chronology]

Esahc (profile), *29 May 2009 @ 7:35pm*

+ + FW LW

Re: Uhhh... Article Fail.

It's a metaphor for DRM.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 8:02pm*

+ + FW LW

Re: Uhhh... Article Fail.

Techdirt isn't a news site. Epic fail for you.

[reply to this | link to this | view in chronology]

Mike Masnick (profile), *29 May 2009 @ 8:04pm*

+ + FW LW

Re: Uhhh... Article Fail.

Medeco being cracked, old news. Lock companies not liking it, old news.

The Wired article is new and does a good job relaying the story, and adding a bit to it, showing the guys actually break the locks, after Medeco denied it was possible.

Why the fuck is this on Techdirt?

Because I found it interesting. We're not a news site, but a discussion and opinion site. I thought it was an interesting concept that deserved some discussion. Apparently you feel otherwise.

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 8:36pm*

+ + FW LW

Re: Re: Uhhh... Article Fail.

Mike,

Your blue background highlights should be flashing. Don't make me contact Mr. Ho to have it actually done for you, as that would be a disappointment for all here.

[reply to this | link to this | view in chronology]

Anonymous Coward, *30 May 2009 @ 5:19am*

Re: Re: Uhhh... Article Fail.

Or perhaps because we will see a link in a future story that says "DMR is like a door lock, easily picked in the end"?

[reply to this | link to this | view in chronology]

What, *29 May 2009 @ 11:18pm*

Re: All comments to my comment.

@ Esahc: How so? Because MWT went straight to news outlets instead of the company?(Unlike someone I will mention later) Rather than abide by the concept "responsible disclosure" he decided to go for sensationalism and profit(via his book that contains information freely available on the internet). Yes, lets encourage that.

@ Mike: Umm, maybe you missed the Wired article when Medeco first responded. They crunched the numbers and worked to figure out how many different keys it would take to bump the locks. Then, they were faced with the Medecoder tool that was disclosed responsibly to them. They met with the person and have begun putting the milled(rather than broached) pins in the new locks. Not exactly ignoring the issues...are they?

As for your insinuation in the original post that others are not talking about it... Perhaps look up how many talks have been given at conventions in the past 5 years related to locks, responsible disclosure, access control, lock forensics(I just attended a talk on that), and other similar issues(or just go to a forum). Plenty of people are talking about it. And there has not been a surge in crime(nor is it even reasonable to suspect such). For a thief, what is easier, picking a lock and being hunched down in front of a house, or breaking a window and walking right in? This is all without mentioning that Medeco locks have been picked since... before I got into lockpicking(ca. 2004). Not exactly something surprising.

It was an interesting concept that deserved discussion 2 years ago, now it is just over played and sensationalized. Congrats.

[reply to this | link to this | view in chronology]

Mike Masnick (profile), *30 May 2009 @ 9:30pm*

Re: Re: All comments to my comment.

@ Mike: Umm, maybe you missed the Wired article when Medeco first responded. They crunched the numbers and worked to figure out how many different keys it would take to bump the locks. Then, they were faced with the Medecoder tool that was disclosed responsibly to them. They met with the person and have begun putting the milled(rather than broached) pins in the new locks. Not exactly ignoring the issues...are they?

They refused to take part in the experiment run here and the article described plenty of stuff that was happening in the space. We had not discussed it here, and I thought it was interesting, so I wrote about it.

Once again, this site is my site, and I write about what I find interesting. This was interesting to me. And, given the comments from others -- to plenty of others as well.

It's great that you're so knowledgeable on the subject. It would have been nicer if rather than a pointless insult, you actually added to the conversation.

[reply to this | link to this | view in chronology]

Steve Pordon, *25 Jul 2010 @ 10:46pm*

Re: Re: All comments to my comment.

"Because MWT went straight to news outlets instead of the company?"

No he didn't. Read the book again.

[reply to this | link to this | view in chronology]

Paul Brinker, *29 May 2009 @ 11:24pm*

Tamper evident

Locks need to show evidence of tamper, Nothing can stop someone with a crowbar, C4 charge, or basic lock smith training.

As long as the lock shows evidence it has been bypassed then its a good lock.

If I wanted to stop someone from geting into my house I would fill my door and walls with concrete, install extra strong hinges and motion detection security cams with email notification. (or a security guard)

[reply to this | link to this | view in chronology]

Anonymous Coward, *29 May 2009 @ 11:31pm*

Re: Tamper evident

These days you can have a camera that sends the motion picture over the Internet where you can monitor it from a remote location I suppose (or pay someone else to monitor it. In fact, that's not a bad idea. A service where someone sits at a desk and gets paid to monitor a bunch of home cameras for burglars where the signal is sent to them over the Internet. If they see something suspicious, they call the police. Perhaps alarm companies can add this to their already existing service, since they already need someone to sit around and wait for an alarm to call them up and then they call the police if an alarm does dial in).

[reply to this | link to this | view in chronology]

What, *30 May 2009 @ 1:27am*

Re: Re: Tamper evident

All locks have *some* evidence of being tampered with, I suggest you go look at this nice site run by a friend of mine: http://www.lockpickingforensics.com/

[reply to this | link to this | view in chronology]

Brian, *31 May 2009 @ 1:42pm*

Re: Re: Tamper evident

Yeah, and you will be oh so satisfied when you can review in the casual comfort of your friends' house how an unidentifiable disguised person picked your lock and took all your valuables. Even a 911 call placed at the time of entry takes longer than it will take a burglar to get in and out of your home.

[reply to this | link to this | view in chronology]

Wolfy, *30 May 2009 @ 7:16am*

I enjoyed Robert Heinlein's definition of "ownership"... (I paraphrase) "what you can carry comfortably and securely at a dead run."

[reply to this | link to this | view in chronology]

Thomas M, *30 May 2009 @ 2:32pm*

Locks

This was a good story to read and I wonder if Mr. Marc Weber Tobias reads these blogs and would answer a question. I am sure that every lock can be picked but what is the best and is it possible to make a keyed lock that can not be picked. I'm guessing no because I have not seen any "Tobias" locks around.
Thank you.

[reply to this | link to this | view in chronology]

What, *1 Jun 2009 @ 4:06am*

Re: Locks

Thomas, it is a popular belief, and in my opinion, a correct one that any locking system will have flaws. There will never be a lock that cannot be picked, decoded, bypassed, or otherwise compromised. There have been many novel approaches to it, many by companies like Abloy, EVVA, Fichet, Dom, and Emhart. But in the end, all these locks have shortcomings and failings.

To be entirely honest with everyone, unless you are a *very* important person(who should have other security measures than locks) or a large, influential company, you do not need to worry too much about surreptitious entry. The amount of break-ins that involve lockpicking or bumping are still such a small percentage of the whole that they should not be a huge concern to the average, everyday homeowner.

(My front door has a simple Schlage deadbolt pinned up with two security pins, I am not worried about my lock being picked but rather my front window being smashed, or one of the ones on the side of our house.)

[reply to this | link to this | view in chronology]

Agonizing Fury, *31 May 2009 @ 10:48am*

Kinda funny how that works.....

You know what I love about this article? It points out the ridiculousness of the anti-circumvention laws in the DMCA. This guy can video tape himself picking a lock, and you can pick a lock in your own home and it's perfectly legal (as long as you aren't committing some other crime by doing so). However, if I own a DVD or Blue-Ray, I cannot legally circumvent the locks on that disc to be able to make my Home Theater PC into a Video Jukebox. Could you imagine the flurry of legal notices this guy would have gotten if he made a video showing how to "unlock" a Blu-Ray!!

[reply to this | link to this | view in chronology]

Anonymous Coward, *1 Jun 2009 @ 10:53am*

Re: Kinda funny how that works.....

great point

[reply to this | link to this | view in chronology]

lulz, *31 May 2009 @ 10:56am*

Lock picking is fun. I picked my teacher's cabinet locks to practice (i told him about it of course; he thought it was cool)

[reply to this | link to this | view in chronology]

Bradley Stewart, *31 May 2009 @ 2:58pm*

Locks and Bagels

If this fellow is correct he is actually doing the public a great service. Its the Bagel Brains that run these Lock Manufacturing Companys that should take this issue seriously.

[reply to this | link to this | view in chronology]

Paul Brinker, *1 Jun 2009 @ 12:26am*

Is there a type of lock that uses disks instead of pins, that cant be picked. At least by normal ways like found on that site posted above? The kind my safety deposit box uses that spins freely?

[reply to this | link to this | view in chronology]

What, *1 Jun 2009 @ 3:56am*

Re: Disk locks

Paul, yes there are a few types of locks that utilize disks. Look into the Abloy Protec system(forget Cliq, it is next to worthless). There is a similar system made by Abus, but it is considered less secure and it can be picked by someone with moderate skill.

As for the Abloy Protec, the only real way to get in is to bypass the lock(has been fixed after it was brought to Abloy's attention) and the destructive method that can be found on YouTube(involves significant damage to the lock). In the US you may have trouble sourcing them, but there are a decent number of locksmiths that carry them.

Another lock to look into is BiLock, which uses two rows of pins and a sidebar system, as far as I know, it has never been picked or decoded when fully pinned(though, someone has worked out a system for certain pinnings, it does not work all the time).

[reply to this | link to this | view in chronology]

Nicholas Overstreet (profile), *1 Jun 2009 @ 9:07am*

Interesting Article

My eyes were really opened to the vulnerability of common every day locks a couple years ago. My girlfriend found her old Master Lock combination lock and wanted to use it again, unfortunately she had no idea what the combination for it was. I did a little research online and had the combination cracked in about 20 minutes. I practiced the skill a bit more and was eventually able to open most Master Lock dial-combination with in 2 minutes. I was really shocked at how easy it was to do.
I've lost the skill since then since I haven't had a use for it... but it really opened my eyes.

[reply to this | link to this | view in chronology]

Anonymouse, *1 Jun 2009 @ 1:10pm*

"Gov't high security buildings?"

Not quite. More like X-09 locks.

[reply to this | link to this | view in chronology]

JK_the_CJer, *3 Jun 2009 @ 2:03am*

Medeco's Response

As What pointed out, Medeco has responded to some of the vulnerabilities being released lately. My research (Medecoder) came out around the same time Marc's did (different exploit). I worked with them and demonstrated the flaw (which was thought to be not easily exploitable) with my tool. They responded by upgrading the pins coming off the assembly line going into cylinders and pin kits. Marc's work was not met with anywhere near as friendly a response (and he did contact them multiple times).

Just wanted to point that Medeco's head is not completely in the sand on this stuff (though it may be in Marc's case). If you're interested in my tool and the company's response, check out http://theamazingking.com/medecoder.html

[reply to this | link to this | view in chronology]

Jason Scheide, Locksmith (profile), *16 Jun 2010 @ 3:17pm*

Kicking Down Sandcastles

I stand by my comment about people taking joy in kicking down other people's work (sandcastles).

Let's see these hackers and lock pickers design a better lock instead of just saying the best locks in the world are not good enough.

Medeco has earned the UL 437 rating. That means that it is good enough for the insurance companies.

It is not easy to get a UL 437 rating and they should have earned your respect for investing the money, time and expertise in making one of the best locks in the world.

I am not a Medeco dealer. I prefer Mul-T-Lock. I realize that if I am called out to open a door for a customer and there is a UL437 rated lock on the door I am not picking that lock. I am opening the door using a bypassing technique.

I look forward to seeing the perfect lock that Marc Weber Tobias invents - if he ever does.

[reply to this | link to this | view in chronology]

JK_the_CJer, *25 Jul 2010 @ 1:24am*

Re: Kicking Down Sandcastles

I don't agree with the sandcastles stance. We generally don't care about the company aspect of this stuff. Unfortunately, as we find flaws; the politics, disclosure, and business issues become relevant.

As for designing better locks, there are ongoing efforts in the community to do just that. The problem is that megacorporations like Assa-Abloy dominate the market. They generally deny that there is a problem with the current locks. The result is an industry that cares more about making sure their patents stay current than security (see Medeco m3, Schlage Primus XP and MTL Interactive for examples). Designing locks is all good fun, but if they don't hit the market there isn't much point. Not to mention that hackers/locksporters aren't nearly as interested in money as they are in creative problem solving.

On the subject of UL437, it is failed standard from this perspective. One can argue that it was never meant to address dedicated attackers using unconventional methods, however.

Your line about "respect" caught my eye. Has Marc not earned your respect for investing the money, time and expertise in defeating one of the best locks in the world?

Also, it is generally recognized that locksmiths will not be using these experimental techniques and advanced tools (in other cases) on calls. The threat perspective that security researchers usually take is that of a well-funded sophisticated attacker (an intelligence agency for example).

[reply to this | link to this | view in chronology]

Jason Scheide, Locksmith (profile), *25 Jul 2010 @ 7:50pm*

Still Kicking Down Sandcastles

A mass produced lock is designed for the mass market. They are serviced by Locksmiths and do a fair job of securing the customer until something happens. Then locks evolve.

The skeleton key forced the industry to re-invent the lock and key. Bit keys were excellent security when they were first used.

When knowledge of skeleton keys became common people had to pay locksmiths to change their locks.

The saw-toothed para-centric key, commonly used today is being replaced by high security UL437 rated keys. High security locks and keys are not perfect.

Locksmiths keep secrets to protect their customers.

People who tell burglars how to get past locks are only helping the burglars, not earning my respect. If only he could keep a secret...

[reply to this | link to this | view in chronology]

JK_the_CJer, *25 Jul 2010 @ 10:37pm* + + FW LW

Re: Still Kicking Down Sandcastles

Your brief history of how locks have evolved points something out: The locks being used are upgraded because vulnerabilities in the older generation were exposed (skeleton key, bumping, etc..) Just because you locksmiths don't know or don't tell about a serious problem, that doesn't mean that the bad guys don't already have the technique/tool.

The ethics of disclosure are far more complex than the old guard trade-secrets mentality that most locksmiths have. Hackers and locksporters understand this which is why there is a constant debate about the impact of releasing various findings.

Let make this a little more personal. If I had a special tool that would allow the easy opening of the lock on your business (MTL I assume), would you want to know about it? If the company refused to fix or even acknowledge the problem; do you, as a consumer and dealer, have the right to know? Or should I just keep my mouth shut and hope that no one else figures it out that has ill intent?

For inspiration, look at the world of academic cryptanalysis. If a vulnerability is found in a cipher, it is generally published and modifications are made or a new one is used. The timeline for fixing the problem is shorter but the concept is exactly the same. The result is an improvement to the state-of-the-art in both attack and defense. The advantage is that the attack is no longer useful for the bad guys who aren't talking about it.

I'm not arguing for or against the release of a particular exploit. Just pointing out that the situation is more complicated than the typical locksmith stance: "just keep it a secret".

[reply to this | link to this | view in chronology]

Jason Scheide, Locksmith (profile), *3 Aug 2010 @ 8:51am* + + FW LW

Re: Re: Still Kicking Down Sandcastles

In the real world (as opposed to the information world) when a vulnerability is discovered it can take years to implement a solution.

If we tell the burglars how to exploit a vulnerability then we will have hundreds of thousands of burglaries instead of just a few.

There is no quick fix, like changing a cipher. Once the lock is improved it is often advertised as being superior to the prior model.

I just read an article saying that UL437 standards are not useful because they are not stringent enough for the author. In fact, the requirements of UL437 are simpler than one would expect - still they satisfy the insurance companies.

Remember that locks meeting the UL437 requirements are the best locks in the world. The manufactures have spent tens of thousands of dollars testing them against professional standards.

If the best locks in the world are not good enough then what are you really suggesting? Don't lock your door?

When better locks are available we offer them in place of the older locks. Some people are willing to invest in the better locks, some are not.

I am happy to recommend Mul-T-Lock products to my customers. My customers have not experienced a successful attack through this lock.

If you discover a tool that can open locks - let's call it a Sonic Screwdriver - should high security companies inform the public about this device? No of course not. Don't tell anyone! Behind closed doors attack the makers of this product. Anyone who makes burglary tools and sells them to the general public should be charged.

It is easy to kick down a sandcastle. It is much harder to build a better one to take it's place. In the meantime there is no sandcastle.

The lock manufactures are being blamed because an old picking technique has become public knowledge. '999' or lock bumping. Picking isn't new. The information that is now public is not new. Nothing has really changed except the public is aware that locks can be picked.

Mul-T-Lock has always been bump resistant. For many years it was un-pickable. Then some locksmiths invested hundreds of hours learning to pick the un-pickable locks.

Mul-T-Lock immediately improved it's pick-resistance. Adding top pins that create a false shear line. Then adding mushroom shaped bottom pins. More recently adding a pin that splits apart when bumped.

Cordless drills have become more powerful in the last few decades so Mul-T-Lock added stainless steel pins to make it harder to drill the cylinder.

When I reviewed high security locks to sell I became very impressed with all UL437 cylinders. They offer more quality than most common cylinders and great ideas to prevent unauthorized key copying, drilling and picking of the cylinder.

I chose Mul-T-Lock to sell because it offered more features to my customers. This has become more true over the years as Mul-T-Lock has improved it's products.

My question: "If the best locks in the world are not good enough, what do you recommend we replace them with?"

[reply to this | link to this | view in chronology]

JK_the_CJer, *3 Aug 2010 @ 12:04pm*

Re: Re: Re: Still Kicking Down Sandcastles

On the whole software vs. locks front, we can at least agree that the decision and timeline for disclosure is different. This does not automatically mean that the answer is to shut up about a problem. A good example is the Medecoder thing; the company fixed it but isn't telling anyone about the upgrade. This means that every already deployed Medeco lock is vulnerable. Unless the public is informed, they are unable to take steps to correct the issue. This pool of unknowing folks included every Medeco dealer I've spoken to; they were unable to protect their own customers.

The only reason you or any other locksmith respects UL437 and ANSI 156.30 is because they are the ONLY high-security standards in the US. There is no alternative. Our issue is with the picking portion of the standard: 10 minutes of resistance using commercial tools. Who takes a stab at it? Is it a handful of crusty old ALOA locksmiths that think Medeco and MTL are pickproof? I can tell you that almost all of the UL437 locks have been picked by our community in under that time; sometimes with normal commercial tools as well. The main problem is that it does not address dedicated attackers that build their own tools or find vulns. Coincidentally, this standard is used by organizations that have exactly those sorts of adversaries to be concerned about.

I find it odd that you brought the bumping thing up. Most of us don't care about bumping at all. That said, the release of the technique did get a ton of publicity and directly resulted in lots of replacements and very few burglaries. Not to mention, the two largest residental lock companies (Kwikset and Schlage) now have bump-proof locks on the shelves of Home Depot for a decent price because of it. As for your stance that lockies knew about it; we perfected it and opened a ton of high-sec cylinders. You guys did not know about the minimal-movement method which is substantially more effective. Also remember that YOUR locksmith supply websites were selling (to the public) pickguns that work like bumpkeys long before bumping was disclosed.

The entire theory that we are just stealing super-secret locksmith info and releasing it is completely bogus. Here is a quick list of stuff you guys had/have no clue about: Medecoder, Michaud MTL overlift, Protec padlock vuln, Bilock vuln(unreleased), Smartkey decoding, Securekey decoding, Abus disc impressioning.

There is much more, but that'll do for now. We don't fault locksmiths for not looking for vulnerabilities these days. You guys have a business to run. On the other hand, we have all the time in the world to analyze and report.

"If the best locks in the world are not good enough, what do you recommend we replace them with?"

The answer is better locks or improved versions of the current locks. UL437 covers everything from Mul-T-Lock to Abloy Protec. The security in regard to picking is not even comparable between these. Protec is a far far better lock if pick resistance is a consideration. After MTL fixed the Michaud overlift problem, they got a lot better but are still quite pickable using the H&M tool.

Personally, I recommend Abloy Protec or Evva MCS. Assa makes good locks as well, but those two are

the best right now.

If society settled for the "best locks in the world" and called it good; we would all still be using thieves knots to secure our doors.

[reply to this | link to this | view in chronology]

Jason Scheide, Locksmith (profile), *3 Aug 2010 @ 12:44pm*

+ + FW LW

Re: Re: Re: Re: Still Kicking Down Sandcastles

Reality Check:

"'If the best locks in the world are not good enough, what do you recommend we replace them with?"

The answer is better locks'

By definition there are no better locks then the best.

You are telling burglars how to break into our homes and businesses. You could have chosen to tell the lock manufactures only - giving them time to improve their products before burglars found out.

Do a Google search for "Medecoder" and the first hit is "Build your own Medecoder".

Are you proud of teaching burglars how to defeat our best locks? You sound proud.

Locksmiths are proud of being able to protect people and belongings. Yes we need new techniques. Perhaps one is to pass a law against groups that expose and publish break and enter techniques.

I can tell you from personal experience that Toronto locksmith suppliers do not sell pick guns, picks or other locksmith tools to the general public. They quickly get a service call from a police office if that happens. It is easy to enforce local laws.

I still have no idea what you are trying to do. There is no benefit to society from your public display of defeating locks.

Are you trying to help me sell alarm systems?

[reply to this | link to this | view in chronology]

JK_the_CJer, *3 Aug 2010 @ 6:46pm*

+ + FW LW

Re: Re: Re: Re: Re: Still Kicking Down Sandcastles

Your goofy semantics argument is invalid. The point is that your definition of the "best locks" is everything UL437. Not all UL locks are created equal.

Actually, the first hit for your very specific query (without quotes or capital is different) is the medecoder page. The very first part of that page is about upgrading your locks.

Find me one burglary involving a medecoder and I'll buy you a beer. I'm more interested in getting locks upgraded from attacks by sophisticated and well-funded attackers; not thugs with a crack habit. My pride comes from discovering a 25 year old vulnerability and getting it fixed.

Trying to solve a technical problem with a legislative solution is silly. Do you think that dedicated people with an actual passion for locks are going to stop because a group of locksmiths lobbied to get a law passed? I'm not even going to go into how fascist a law like the one you proposed is.

Well great, I guess burglars that walk into a locksmith supply store in Toronto are screwed. The rest of the world has the internet.

We don't expect locksmiths to understand. Locksmiths don't spend all night hunched over a disassembled cylinder measuring tolerance errors looking for a way in. Locksmiths have invested too much money in their high-sec product lines to fathom a vulnerability. Locksmiths don't care about the far more secure locks used in Europe. Locksmiths don't tell the public that the American 5200 padlock they just bought has an easy bypass so they can protect themselves. Locksmiths don't care about locks. Just keep selling what the manufacturers send you and leave the technical work to us.

You joke about selling alarm systems. Frankly I think its a good idea to have one. Everyone knows that the bad guys are coming in by force not an elegant surreptitious attack they read about on the internet.

[reply to this | link to this | view in chronology]

Jason Scheide, Locksmith (profile), *3 Aug 2010 @ 8:29pm*

Re: Re: Re: Re: Re: Re: Still Kicking Down Sandcastles

Semantics aside. I still do not have a better lock to install for my customers who have lost faith in the locks being criticized on the net.

Many locksmiths I know are well aware of bypassing and opening techniques. We are an organized and educated profession. Many of us became locksmiths because we have an interest in locks and opening them. Just because you found a vulnerability in a lock does not mean you are the first. Making the vulnerability public does not make you Robin Hood.

Real people get burgled. Real people have their prised possessions scattered around their house and lose thousands of dollars of valuables in burglaries. Real people.

That is why locksmiths are not so quick to tell the public "this is how you defeat this lock". We often help clean up the mess after a burglar has left.

Yes padlocks can be opened, and no I don`t tell my customer`s that it is possible for a padlock to be opened with bolt cutters. I also do not tell my customers that the lock they are buying is perfect.

I sell peace of mind. The old lady who is worried that a burglar is going to hurt her dog sleeps better believing that bad men cannot open her door. Why do you want to take that away?

Instead of tearing down the products that people have built, why not try to improve them. Work within the system. Don't kick down the sandcastle, grab a pale and put up a new turret.

Here is an example from my career: Mul-T-Lock keys have a larger plastic head than most keys. Since I also sell access control systems I recommended Mul-T-Lock add a proximity keyfob in the head of their keys. It took years, but now we have the Synerkey. Three keys in one!

It is not perfect but people like to have less keys in their pockets. It does the job.

Should we start talking about alarm system bypassing techniques?

There is a saying that I keep in mind when someone asks me if a lock is un-openable: Made by man, broken by man. Every lock that will ever be made will have a weakness.

[reply to this | link to this | view in chronology]

Jon King, *4 Aug 2010 @ 12:25am*

Re: Re: Re: Re: Re: Re: Re: Still Kicking Down Sandcastles

You do have a better lock. Take a look in your MTL pin kits and notice the small extendable rod on top of the driver pins. This modification was made in response to Michaud's inner pin overlift attack which was then published.

Although its a fine ethical line to walk; public disclosure gets things fixed. Some company have the view that if most don't know about it, its not a problem. Combine this with the expense of implementing a fix and you have an ignored vulnerability after reporting it. By contacting a company early and working out a release date together, it ensures a fix will be made. During this process, however, it is important to not involve money. My opinion is that when money enters the equation, it strays too close to extortion and calls into question the ethics of both parties.

Of course we are not the first to discover some vulns (although in many cases we are). I was simply making the point that we don't go browsing copies of locksmith newsletters and releasing the juicy parts. Its not about being Robin Hood; its about informing the consumer that a better lock or an upgrade is available. We have no stake in any particular brand and thus can provide unbiased information.

Details are released for a few reasons. People are generally skeptical of what they read. If I said "MTL is vulnerable, buy Protec"; you'd laugh at me. If I handed you a well-written whitepaper with photographs and a technical explanation of the problem, you'd take it a little more seriously. Other companies would be less likely to make similar design flaws. Details also allow for an improvement in the attacker state-of-the-art so that the improvement cycle can continue.

Peace of mind is not security. When a customer comes to you, they are looking for security. They aren't looking for lies to make them feel safer. I hope you don't take this same approach when .gov .mil and .com come looking for locks.

Excellent job on getting the prox feature added to MTL keys. The electronic side of things is emerging fast and is providing a sort of stop-gap for mechanical vulns. This technology must remain nimble, however. Once the hackers take notice, we should expect problems to be found and hopefully fixed.

As for alarms, there is already a cat-and-mouse game happening between the manufacturers and crooks. Alarm systems have the advantage of being a little more difficult to reverse engineer than mechanical locks. With locks, literally anyone and buy one, take it apart, and look for problems. Alarm systems tend to be a bit tougher to do this to. I'd like to see a sort of 'alarmsport' emerge but we haven't focused on the disclosure ethics for something like that yet.

Your saying is quite true and I keep that in mind when looking for issues. If we can find the obvious weaknesses, raise awareness, get them fixed, and recommend better alternatives; the result is improved security.

[reply to this | link to this | view in chronology]

Jason Scheide, Locksmith (profile), *4 Aug 2010 @ 5:04am* + + FW LW

Re: Re: Re: Re: Re: Re: Re: Re: Still Kicking Down Sandcastles

It would be nice to have the perfect lock.

My residential customers need more education. A good lock is a good start - the window beside the door also needs fortification.

Government, military and commercial customers are more aware of their vulnerabilities. Often the lock is the strongest part of their security system.

Government and military don't depend on a lock for security. They depend on human guards. That opens a whole other discussion about how dependable a human being is.

A good security system is like an onion. Layers make it difficult for a burglar to achieve his goals. A good lock, even if it is not UL437, an alarm system to let you know when the door has been opened and a safe for what the burglar really wants is a very effective system. These are all products that I sell.

Peace of mind is different.

I am sure the little old lady knows that a burglar can come in through the window she keeps open at night, but the burglar came through her front door last time. She needs a good night sleep, not top of the line security or a perfect lock.

Many customers are only looking to do their due diligence so their insurance company will cover their losses.

Peace of mind is not security. A full security system is too much for most people. All they want is peace of mind that they are not the easiest target.

It has been a pleasure discussing locks with you. All the best in your endeavors.

[reply to this | link to this | view in chronology]

locksmith, *25 Jan 2012 @ 6:51am* + + FW LW

locksmith

There is a way to deal with this the locksmith companies have to wake up and do something before its to late.

[reply to this | link to this | view in chronology]

Jason Scheide, *25 Jan 2012 @ 8:29am* + + FW LW

Re: locksmith

Hey Locksmith...

We are open to suggestions.

Have you seen the SNL skit about the economy? "Fix it!"

Sometimes it feels like that in the lock industry. We know about the problems, recommend solutions, and the feedback we get from the public is "Fix it!"

There is a small fact that humans are resourceful animals who can figure out new ways of opening locks. That

fact is not going to change because of a new lock design.

There are bigger problems in the industry than really good locks being less than perfect.

For one, there are look-a-like locks being sold to the public. These "locks" are designed to fool the consumer into thinking they have a measure of security. They often fail to keep the door closed when attacked.

Security locks that we, the professional locksmith, recommend you install on all exterior doors, are not being opened by burglars.

[reply to this | link to this | view in chronology]

Charly Jones Locksmith, *20 May 2012 @ 2:08am* + + FW LW

certification

I just want to say top everybody locksmith for a locksmith, you should always check if your local locksmith is certified and also if he is a member of BBB, there is a lot of scamers around that's a quick way to know who you are dealing with

[reply to this | link to this | view in chronology]

patrick smith, *22 Dec 2012 @ 8:49am* + + FW LW

Coming out of the Sand

We agree that any lock can ultimately be defeated but when locksport enthusiasts expose our weaknesses on YouTube, Commando Lock embraces them openly. We've pulled our heads out of the sand and have asked the industry to help us create a better padlock.

In 2013 we will launch new products based almost entirely on the hundreds of ideas given to us by locksmiths around the world. We welcome the challenge and understand we will ultimately be defeated but in the long run, we're creating the best product with the help of the best people in the industry. These are locks want to take a beating.

patrick smith
commando lock company

[reply to this | link to this | view in chronology]

jason scheide, *23 Dec 2012 @ 9:07am* + + FW LW

Re: Coming out of the Sand

Hi Patrick,

That is a great attitude and you make a good looking padlock.

I look forward to seeing what you come up with in 2013.

If you start making a deadbolt for residential and commercial doors I might be able to sell it for you.

[reply to this | link to this | view in chronology]

Add Your Comment

Have a Techdirt Account? **Sign in now**. Want one? **Register here**

name

email

Subscribe to the **Techdirt Daily** newsletter

url

subject

comment

Comment Options:

- Use markdown. Use plain text.
- Remember name/email/url (set a cookie)

Submit Preview

Less Than A Third Of Australia's Censor List Actually Abo… Could US Copyright Agenda In China Help Stifle Speech?