Schneier on Security

Blog >

Hacking the Assa Solo Lock

Marc Weber Tobias again:

> The new Assa Solo was recently introduced in Europe and we believe is the latest Cliq design. We were provided with samples and were able to show a reporter for Wired's Threat Level how to completely circumvent the electronic credentials in less than thirty seconds, which she easily accomplished. This is the latest and most current example of a failure in security engineering at Assa.
>
> [...]
>
> In response to demonstrations and our disclosures about the bypass of Assa Cliq locks at Defcon 17, the product development manager of Assa in the U.S. told Wired Magazine that "From what I know of the CLIQ technology it can't be done," … "And until I've seen it done, it can't be done."
>
> We believe this statement typifies precisely the problem at Assa Abloy companies: a failure of imagination. It prompted our research and subsequent discovery of multiple vulnerabilities in Cliq, Logic, and NexGen locks. It is this attitude that will continue to allow us to break locks that are represented as the ultimate in security by these companies, and which often provide a false sense of security to the locksmiths and customers that rely upon these products.

Me on locks and lockpicking.

Tags: hacking, locks, physical security

Posted on August 21, 2009 at 6:03 AM • 27 Comments

Comments

Johannes Berg • August 21, 2009 6:48 AM

So which companies do incorporate proper security engineering into their locks?

Muffin • August 21, 2009 6:52 AM

So we've gone from "Cover Your Ass" (CYA) security to "LALALA-I-Can't-Hear-You" (LICHY) security now?

Heavens.

John Ridley • August 21, 2009 7:59 AM

Assa is all set then. All they have to do is keep that development manager in a box so he never sees this done, and it'll remain impossible.

Troy • August 21, 2009 8:37 AM

@John Ridley, Schrodinger in reverse? How odd.

So has anyone yet asked the question of locksmiths: Which locks do they use to protect their own stock of expensive, high security locks?

Baeck • August 21, 2009 8:52 AM

I love the file name of this post: hacking_the_ass.html

Troy • August 21, 2009 8:52 AM

I suddenly get it! Assa is actually using quantum encryption to secure their locks.

Tobias really needs to give this company more credit ;-)

LICHY security does have a certain ring to it. Didn't software go through the same thing, which prompted exactly the same disclosure debate that Tobias is stirring?

Lazlo • August 21, 2009 8:55 AM

@troy: I'd bet they have a fairly inexpensive, reasonably sound lock protecting a stock of products adequately insured against theft.

Critique • August 21, 2009 9:43 AM

No wonder. Their homepage says it all:

"ASSA ABLOY is the global leader in door opening solutions"

No mention of LOCKING doors :)

---

bob • August 21, 2009 10:03 AM

Militarily, if you are attacking an alliance of forces, the best place to attack is the junction between them.

If you are facing a lock which has electronic AND mechanical security components, the best place to attack is the interface between them. You can have the coolest, most sophisticated computer ever designed doing the validation and verification, but if the end result of all that processing is a simple electronic impulse traveling down a wire, that would be where I'd start.

Clive Robinson • August 21, 2009 10:12 AM

@ Muffin,

'"LALALA-I-Can't-Hear-You" (LICHY) security now?'

Hmm how do you pronounce LICHY?

As in Itchy or the fruit...

More seriously I used to design electronic locks and they are a bit of a problem to design in many ways.

I've generaly found that they all sucumb to relativly low level attacks on the mechanics so by and large the electronics can be ignored as "high tech pixi dust" (and offten a simple reverse polarity on the battery disposes of any electronic issues due to protection circuits ;)

Such low level attacks on the mechanics include, magnets freezer spray, good old fashioned grease, or plain old "spin the handle and jerk" attacks (another variety of "bumping" or Newtonian cradle attacks).

However it's nice to see somebody doing other things to high tech locks 8)

As somebody once put it to me in a jokey Bishops voice,

"My son, put not your faith in that, which others say cannot be broken, for delusion is but one of many grevious human failings"

---

bob • August 21, 2009 10:15 AM

"...Several companies, both in the U.S. and Europe have done precisely that [replace locks shown to be flawed], and at great cost to themselves. It is the responsible way to do business as a lock manufacturer..."

I would like to know which company backed their locks in this fashion so I can install theirs in place of what I have.

Benton Jackson • August 21, 2009 10:20 AM

"I would like to know which company backed their locks in this fashion so I can install theirs in place of what I have."
That's what I'd like to know too. Seems like a huge plus. But I can understand how lock companies would not like to do this. Unlike cars, which you can usually repair the defect, or software, where you can

just send a new binary or even just patch, locks usually have to be replaced in entirety. Unless they have HUGE markups, this would probably negate all of their profits and then some.

"Hmm how do you pronounce LICHY?"
Rhymes with "Vichy?"

---

anon • August 21, 2009 11:05 AM

> > "Hmm how do you pronounce LICHY?"
> Rhymes with "Vichy?"

The "LICH" part would be the same as "lich" and the "y" would be however you pronounce "y" at the end of a word (is "ee" where I live).

MarkM • August 21, 2009 11:10 AM

@bob:
Kryptonite (apparently owned by Ingersoll-Rand) instituted a free exchange program for all its tubular cylinder locks when it was discovered that some (but not all) models were susceptible to the "Bic pen" attack. Not useful as a door lock replacement, though.

Unix Ronin • August 21, 2009 11:49 AM

Tobias: "We taught a reporter how to crack one of these locks in thirty seconds..."

Assa: "LALALALALALALALALALALALA I CAN'T HEAR YOU!!!!"

Unix Ronin • August 21, 2009 11:52 AM

heh, I should have read the other comments first :) I see I'm far from the only one with this immediate reaction.

A friend proposes that LICHY be pronounced to rhyme with 'leaky'.

James Sutherland • August 21, 2009 12:55 PM

At work, we now have a bulk single-source deal for buying PCs - such a great deal, it's offered to all the staff and students for personal purchases too. Being intended for educational use, of course, each PC includes a common-keyed security lock and key. The combination of using a single key and selling the package to everyone seems slightly insecure... (Needless to say, my own department will be purchasing a batch of proper padlocks to go with our new batch of PCs. On the bright side, presumably if any of ours break down, we can just switch them with the "secured" ones in the building next door when nobody's looking.)

Clive Robinson • August 21, 2009 1:25 PM

I must admit I'm not that familiar with the locks shown but they appear to be a replacement for a standard mechanical cylinder that you would find in any fairly standard swing door such as those found on shops and office entrances and the slightly more security concious office door.

Let me start by saying if you put your trust in standard cylinder locks then you are setting yourself up for a world of disappointment, as you will see if you bother to take any cylinder lock apart. Put simply they have never been designed with security in mind just reliability.

That is the manufacture has made a simple calculation that locks that bind up in use cost them money and reputation, locks that are bypassed by intruders cost the lock purchasers insurance company money. So reliability in use not security is the key design criteria irrespective of what the marketing blurb might say (and do you really believe that SuperBright laundry powder really will make your grey with age T-Shirt glowing white again?)

That is they have done one of those things Bruce gets hot under the collar about "externalised the risk/cost"

If you read the web page and look for any technical details you will be sorely disappointed there really aren't any. The closest it comes to is this paragraph,

"The core technology consists of a key that contains mechanical bitting and a processor and battery, which communicates with the microprocessor and sidebar-control motor within the lock. When the proper mechanical and electronic credentials are simultaneously presented to the lock, an internal motor is activated, a rotor turns, and a sidebar is allowed to be pushed into the plug. If the key is properly bitted, then the lock can open."

To understand what this is saying you need to think about what this sort of lock really is,

"a simple mechanical latch"

Effectively it has three parts,

1, Latch
2, Rotational to linear motion converter
3, A removable handle

The difference between a simple mechanical latch and a lock is the removable handle (the key) is one half of a "security interlock". When the correct key is presented the interlock is removed and the lock is a simple mechanical latch from that point.

Thus two things become clear, the energy required to open the latch comes from the human holding the key so has very definite limits (for the weak of wrist) the entire security relies on the interlock. Thus if you can bypass or operate the mechanism from "down stream" of the interlock you are in.

The interesting part of the paragraph is this, "When the proper mechanical and electronic credentials are simultaneously presented to the lock, an internal motor is activated, a rotor turns, and a sidebar is allowed to be pushed into the plug."

If you read it backwards it becomes clear that you have three things,

1, A conventional mechanical key mechanism
2, An additional electromechanical element (actuator) that locks the key cylinder into the rotary to linear movement converter.
3, A microprocessor that reads a security token on the key and stores it's ID etc for audit and supplies current to the actuator.

This is where the fun starts, you apparently have,

Two security mechanisms operating in series if either does not work then the lock does not open.

On security mechanism is the mechanical key and cylinder (true).

The other security mechanism is the RFID on the key and cylinder microprocessor (false).

The second security mechanism is actually the sidebar.

So if you can copy the mechanical key or bump it the only other thing you have to do is somehow get the sidebar to work.

Without actually seeing the sidebar design and it's motor actuator and control electronics I could not specificaly tell you the best method of attack.

But,

1, It might just fall into place if subject to appropriately directed kinetic force (bumping).

2, It might be persuaded to stick by injecting grease into the lock such that the next valid operator causes the sidebar to stick in the active position.

3, Creating an intense magnetic field might either pull it into place or again make it susceptible to sticking the next time a valid user opens the lock.

4, If it is not fully blind to the key way it might be possible to push it back and insert a shim or other small mechanical item to act in it's place.

5, The design of the cylinder plug and sidebar locking sleeve might be such that the same effect as actuating the sidebar could be achieved with an external mechanical device.

If any of these don't grab you then you can take one step back and attack the actuator, magnetically electronically or mechanically.

It needs to be said at this point the microprocessor has not played any part in these base level attacks, so unless it has attack sensors (very unlikely) it will not log anything that can be audited at a later date even though a valid mechanical key might have been used and the door opened.

You can take another step back and attack the microprocessor in various ways by injecting out of band signals into it to create faults. One such method is applying an appropriate RF signal of sufficient power to inject a firmware or software fault that might well cause the microprocessor block to fail in useful ways. I won't go into details as nobody that I know of has published results on this sort of very viable fault injection attack yet and it would easily earn you a PhD (I know Ross Anderson is aware of it as I suggested it as a method to get around his non synchronous logic).

You could take another step back if you where up to analysing the RFID protocols attack the communications link between the token on the key and the microprocessor block in the lock.

But why start at the top when starting at the bottom is going to be oh so much easier.

Bryan Feir • August 21, 2009 2:22 PM

@Clive:
Nice analysis. Of course, if they bothered to add a physical 'key present' sensor to the lock the audit trail should include any time a key was entered, no matter what the RFID on it was. This would at least let you know that somebody tried picking the lock afterward. If they have a sensor to determine when the sidebar moves, or preferably when the bolt moves, you could determine when things actually open. This could let you distinguish between people using fake keys that worked and fake keys that didn't.

My reading of the article suggests that they did not include a bolt sensor, at least.

Elizabeth Greene • August 21, 2009 4:53 PM

"I would like to know which company backed their locks in this fashion so I can install theirs in place of what I have."

Medeco. When security researchers developed an exploit against the rotating tumbler mechanism for the sidebar, M spun up a new (old) production line to make new pins that were resistant to the attack. These new pins were made available for free.

(You still have to pay your dealer for labor though.)

-ellie

Elizabeth Greene • August 21, 2009 5:02 PM

I withdraw my prior comment. It looks like the gestures they made with the ARX pins were just a gesture and not a real policy change.

---

billswift • August 21, 2009 5:32 PM

Somewhat off topic, but this made me think the discussion a few months ago about how boobytraps are illegal. But not all of them are, a 3 foot tall Wolfhound named Rover would be a pretty good one.

Jon King • **August 23, 2009 12:43 AM**

Elizabeth and others:

The story of how Medeco reacted and started putting those ARX pins (closed-groove) in all locks and pin kits can be found here:

http://theamazingking.com/medecoder.html

Although I have not updated it yet; I have full confirmation from both the company and non-biased individuals that the upgraded pins are actually in the new locks. I do not know if they raised prices but Medeco is definitely not doing a free pin-swap for existing locks.

As for which folks employ "proper security engineering"; they all attempt. This industry is an old one that is not prepared for the hacker/researcher threat. Locksport folks and Marc are now finding vulnerabilities in high-sec locks that the locksmiths used to (back in the day). We do not share the same default-to-secrecy sentiments that the lockies did and I'd argue that our opinions on disclosure ethics are much more varied.

Also read deeper into this and you'll find that Marc refused to release his research to Assa-Abloy unless they agreed to a full recall and replacement of the locks. He is a lawyer so this agreement would surely be written up in contract-form. Without the details, the company would not have known to what depth he actually broke the locks (tricking the audit trail is not the same as surreptitiously opening the lock with absolutely no prior intel, for example). I wouldn't say what he asked was unreasonable (esp. given his history with Assa-Abloy), but there is more to this story than the companies just crossing their arms and saying "no!".

Dave Andersen • **August 23, 2009 8:19 PM**

Jon's point is worth re-reading. In particular, I'd draw a contrast between Marc's policy and a fairly standard practice on full-disclosure lists. The software security community often provides a bit of notification to a vendor, followed some time later by a full-disclosure notification. This practice leaves more of the decision about how to deal with the vulnerability up to the market: if the vendor is sufficiently (embarrassed, financially impacted), they issue a free fix. Of course, the cost of security upgrades is higher for physical systems, but we see similar issues with fixes for old software releases. In contrast, Marc is trying to force a particular upgrade path (and is *not* disclosing the exact vulnerability to the vendor) instead of letting the market judge whether it's worth it or not. Each to their own, but it is a strikingly different way of dealing with the vendors than many of us are used to.

AC2 • **August 24, 2009 4:22 AM**

*** Manager of Assa in the U.S. told Wired Magazine that “From what I know of the CLIQ technology it can’t be done,” … “And until I’ve seen it done, it can’t be done.” ***

As the man said - "It is difficult to get a man to understand something when his job depends on not understanding it"

Ursus • November 22, 2009 9:57 AM

these companies are just pissed off because they have spent millions in R&D plus the expensive machinery to produce these locks so naturally they would be in denial, It cost's thousands for the programmer, One Cylinder, Extra Keys and the programming keys just for one system, The're raking it in and to admit there is a flaw is development suicide as they have to recall all of the locks that they claimed were inpenetrable from those they sold them to, They'd look a right bunch of assholes to the customers so much they might go elsewhere, Personally I don't see the problem as ASSA Abloy own about 90% of the security companies anyway, Whichever the customer wishes to defect to ASSA Abloy probibly owns.

Joe • April 26, 2013 6:32 PM

There are a lot of claims from so called “security experts” like Marc Weber Tobias, how 10 seconds and 30 seconds lock picking and by passing of high security locks can be done with eyes closed.
Also wondering about the integrity, expertise, and hands on experience if any… of the followers of Tobias and others self proclaimed “master lock pickers”.
When Tobias and others like him calming that a 16 years old girl figured it out how to pick a Medeco lock open in 8 seconds without any previous locksmith experience…Well it it speaks volume.
All credibility is out the window.
Basically these so called “experts” like Tobias saying that the engineers and developers are all idiots at Assa Medeco & Mul-T-locks. Years of developments, planning and engineering can be hacked just about anybody.
And if that would be true, than how exactly makes this, Tobias an expert when a 16 year old girl can pick a high security lock open in seconds with no prior experience??
Many claims about Medeco locks or for that matter, even conventional locks being bumped is just not true.
Very simple solution to this bumping problem is stronger springs in the chamber.
That will put an end to the bumping discussion.
Of course there are the total idiots, pretending to be locksmiths and security experts on discussion forms and YouTube that cannot understand the basic laws of physics and will continue with their psycho babble about lock picking which they don’t understand what so ever.
Their ignorance is only overshadowed by their arrogance and narcissism.
If there would be any truth to this nonsense of Tobias madness many burglar would have capitalized on this to their benefits. But for some reason the good old fashioned burglars prefer a crow-bar to do the job.
I wonder how many of these experts can actually pinup a cylinder, take a mortise lock apart dump it in a sec than name the parts than put it back together in a dark cold and windy hall way, while you’re kneeling on the ice cold tile, while your phone is ringing off the hook.
I didn’t think so.
Most of these people on these forums could not last on a commercial or institutional locksmith assignment for an hour. None of these claims sound true to me. Sorry not today.

Subscribe to comments on this entry

Leave a comment

Login

Name (required):

E-mail Address:

URL:

□ **Remember personal info?**

Fill in the blank: the name of this blog is Schneier on ___________ (required):

Comments:

Allowed HTML: <a href="URL"> • <em> <cite> <i> • <strong> <b> • <sub> <sup> • <ul> <ol> <li> • <blockquote> <pre>

Preview Submit

← Developments in Lie Detection Embarrassing Terrorist Failures →