Schneier on Security

Blog >

Magnetic Ring Attack on Electronic Locks

Impressive:

> The 'ring of the devil' is capable of attacking this kind of electronic motor lock on two ways.
>
> Scenario 1: An electronic motor is nothing more then a metal part on an axe that turns because of a changing magnetic field. Turning electro magnets on and off will generate a pulling force on the metal part, making it rotate. The ring does the same thing. By turning the ring, the metal part in the electro motor starts turning, opening the lock. As Rop suggested in the comments of the previous posting, a bunch of bigger magnets and maybe a high-speed drill can amplify this effect some more.
>
> Scenario 2: A dynamo is nothing more then a coil charged by a changing magnetic field. So any coil in the lock will start generating current when a magnetic field is rotating around it. If the coil is in the path of the electro motor, it might generate enough current for the motor to start turning.

Tags: locks, physical security

Posted on June 18, 2008 at 6:35 AM • 17 Comments

Comments

Jacson Querubin • June 18, 2008 7:18 AM

Well,

I would make a plastic one =)

done!

Trichinosis USA • June 18, 2008 8:01 AM

And for those nimrods who build their secure room with a heavy door, electronic or otherwise sophisticated lock, and sheetrock that has been screwed to the studs for walls with #2 phillips heads, there is... the sceptre of the she devil. ;-7

http://www.pelicanparts.com/catalog/images/tools2003/BD-VP750.jpg

---

RealName • June 18, 2008 8:13 AM

I would not be too worried about this kind of attack.

In scenario 1, the device needs to have a motor with the magnets on the rotor. Most DC motors have the magnets on the stator and brushes to create an AC current through the coils on the rotor. The rotor does not have a magnetic field alone and thus the external ring magnet has nothing to influence.

A brushless DC motors with the coils on the stator needs special inverter circuitry to create an alternating magnetic field around the magnets on the rotor. I doubt many manufacturers would introduce more complexity and cost for no apparent reason.

In scenario 2, even if there is a coil in the circuit of the motor, you still need a closed circuit. The motor will be driven either by a diode-clamped power transistor, or a relay switch. When the transistor is saturated, it will not conduct current, hence the whole field of semiconductors. And obviously, if the relay is open, the circuit is open.

Wyle_E • June 18, 2008 8:54 AM

The attack works against _some_ motor-operated locks.
I would guess that success depends on the geometry of the system. I can think of a few countermeasures, like a permanent magnet that detects the external field and moves to lock the mechanism, or two motors with differential gearing that requires the motors to turn in opposite directions.

Clive Robinson • June 18, 2008 9:14 AM

Bruce,

THis is very very old news... I f you look back on your blog you will see it has come up in another form before and I commented on it then.

Nearly all electronic locks use some kind of magnetic component to actuate the locking mechanisum as a clutch, motor or solonoid.

Any sufficiently strong magnetic field (static or otherwise) will replace that generated by the winding in the device and if orientated correctly will make the device actuate as though there was current flowing in the winding.

I used to design electronic locks for the hotel industry in the early 90's (UniQey) and I was well aware of this as are Underwriters Laboratories Inc. (UL) which makes me think the locks in question do not have UL approval.

The solution to the problem is very simple you put a soft iron shield around the device so it forms an incompleate magnetic circuit. To compleate the magnetic circuit you put a light weight soft iron bolt held open against a weak spring. If a large magnetic field is applied to the lock then the soft iron bolt closes and at the same time breaks or blocks the gear train to the locking mechanisum, so even if the attackers do turn the motor etc then it is wasted effort.

Another method that a lot of electronic locks fail to is due to the protection circuit on the magnetic device. Due to the back EMF frome the device winding you can get very high revese voltages across your switching device (transistor or fet) that if not delt with will destroy the switch. There are a number of ways of doing this (snubber networks etc) but offten it is a diode in the revers direction across the device and or the switch transistor. A small number of the arangments allow the device to be actuated simply by putting a reverse polarity voltage across the powersupply line as the network effectivly bypasses the switch. Often it is not obvious from the circuit diagram as the diode is built into the switching device (ie the FET).

Now as these locks usually run off of a battery and the circuit is offten designed for minimum leakage and lossess little or no protection for the battery or device and switch is included (as it's the highest current part).

Also as batteries fail there is often a handy set of contacts on the underneath of the lock based around a small telephone jack which connects to the battery and device and switching circuit.

Add your own batter in the wrong polarity and twist the door knob and hey presto open lock...

There are a few other more sophisticated attacks for the better designed locks but they all appear to have a simple weakness of one kind or another. And as for those high tech ultra expensive fingerprint reader types see a previous blog post,

http://www.schneier.com/blog/archives/2005/09/fingerprint-loc.html

Oh and if you do ever design a better lock expect to get a sales enquiry from an Israeli company or some unheard of subsidiary of IBM at some time or another asking for a demonstration unit for evaluation. You probably will not make a sale as it is most likly a Mossad front. Apparently Mossad pride themselves on knowing how to pick any lock in existance...

Yup I thought it was somebody pulling my leg when I was first told, and I was pointed to the book "By Way of Deception" by Mossad deffector Victor Ostrovsky, who said in it that Mossad, which was famous amongst the western intelegence agencies for its lock-picking talents. Apparently British intelligence used to send new designs of locks for testing in Israel. Mossad would figure out how to pick the new model of lock, but would send back a report to SIS saying that the model was unpickable.

Also it has been known that Mossad agents have a collection of keys to most hotels in Europe, North America and the Middle East. Apparently they often use hotel rooms that are known not to be occupied for meetings / survalance etc and that way not only do they not leave a paper trail they also don't have to pay 8)

Secret duck • June 18, 2008 9:28 AM

@Clive Robinson

Why do they need a collection of keys for all the hotel rooms, if they can pick any lock in existence?

Clive Robinson • June 18, 2008 10:26 AM

@ Secret duck,

"Why do they need a collection of keys for all the hotel rooms, if they can pick any lock in existence?"

First off I personaly do not think they can pick every lock in existance as I noted and nore do they need "keys for all the hotel rooms".

However to address your point's,

Lock picking like many other physical activities is a skill one has to learn, and like playing the violin it is best to ensure you are more than moderatly capable before you have to perform in public otherwise it could be more than your face that goes red 8)

Also lock picking takes time I know in films they just walk up and stick the rack in and jiggle but seriously it can take quite a while to pick a lock (several hours or more in some cases). Go over to Mat Blazes site for more info on lock picking in the Physical and "human-scale" security section of http://www.crypto.com/papers/

Likewise in most parts of the world carrying "lock picks" is considered as a crime of "going equiped to commit". Which could be a real pain to sort out.

Finaly having a key legitimises you at every stage, you simply walk up stick the key in turn and enter, if anybody is in the corridor they see what they expect to see ie the use of a key. Then if somebody is already in the room etc then you simply indicate that there must have been a mistake at the front desk etc and make your excuses.

Master of the blatently obvious • June 18, 2008 10:33 AM

@Secret Duck

I can think of a number of reasons:

1) It's less obvious to have someone open a lock with a key/keycard than it is to pick one. Faster, too.

2) If you're discovered in possession of lockpicks, in many jurisdictions that's prima facie evidence that you intend on breaking in somewhere. At the very least, it should alert a reasonably bright guard/cop that something odd might be happening. Getting discovered with a key? Not so much.

3) If caught in a hotel room that they weren't supposed to be in, the agents might be able to play it off as drunken businessmen who found the wrong room when their key opened the door ("We forgot what room we were in, so we tried all of 'em!")

Davi Ottenheimer • June 18, 2008 10:46 AM

This does remind me of the discussion from 2005:

http://www.schneier.com/blog/archives/2005/03/flaw_in_winkhau.html

---

Sparky • June 19, 2008 2:58 AM

@RealName: You are correct about the brushed and brushless DC motors.

However, there are other types of motors; a stepping motor, much like a brushless DC motor, does have a magnetic rotor. Using strong magnets, you could probably make it turn, if you overcome the (small) residual holding torque, provided, ofcourse, that the lock itself is not providing a holding current.

Cheap AC motors are generally of the "squirrel cage" type, which do not have a magnetic rotor, but one with closed single-turn windings. If a rapidly changing magnetic field is applied, there will be a current induced and the motor will turn.

So it really depends on the type of motor, although I would suspect most small locks use simple DC motors.

Scenario 2 sounds like someone slept thought a few classes in college.

Personally, I'd use electromagnets, they can generate a far stronger magnetic field in the same size and weight (if the batteries are not included), and don't require drills to rotate them, because it is far easier to make the field rotate instead.

I wonder how they plan to fix this with a software update; my guess is they have an end switch that they monitor, and they power up the motor if the end switch contact is broken when the controller is not opening the lock.

(I am an electrical and computer science engineer)

Sparky • June 19, 2008 3:12 AM

One of the comments below the article raises a good point; a common way to stop a DC motor with a H-bridge, is to enable both low or high sides, effectively shorting the motor. Because of this, there is a path for the induced current. If they have a way to disable the H-bridge altogether (which requires an extra output from the controller, or some logic hardware), this is preventable.

(A H-bridge is the common way to control a DC motor from a controller, allowing one to turn it in both directions)

---

annienomous • June 19, 2008 9:16 AM

@Trichinosis: I was thinking more along the lines of this "sceptre"

---

annienomous • June 19, 2008 9:22 AM

no html links huh? shoulda previewed
http://www.amazon.co.uk/Estwing-E3-17-Drywall-Hammer/dp/B0002JT0CI

---

pentagon hammer • June 19, 2008 12:41 PM

Who'd pay 46 pounds for one of those hammers?

---

greg • June 20, 2008 3:19 AM

@Sparky

Electromagnets for a 1T field are a lot larger than a rare earth magnet with surface strength of just over 1T. A hallback array can get over 2T. Electromagnets can't do that in a compact package....

Barry Wels • June 23, 2008 3:04 AM

There is a new video on Youtube. It seems to show an update will fix the problem ....

http://www.toool.nl/blackbag/?p=206

David • July 15, 2008 6:05 AM

You could also follow the mechanical locksmiths of 100 years ago. Add a moving steel part, which will be attracted by an external magnetic field. Being attracted, it moves to block the motor's rotation.

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

← LifeLock and Identity Theft

Security Through Obscurity →