Too Cool for Internet Explorer

A new attack on electronic locks: The magnetic ring

June 16th, 2008 by Barry

There has been quite some speculation about this video (YouTube) of a magnetic ring that is used to open some model of Uhlmann & Zacher lock. By now it is confirmed by the company itself the trick works. They claim a software update will fix the problem (and even log opening attempts).

(click on image for a high resolution version)

The ring used in the video now has a name: 'the ring of the devil' and is already available on the market (just 25 euro!).

And the questions now are: What is in the ring, how does it work and what locks are affected?

Well … I have some answers. Saturday I received my own magnetic ring and can give you some details.

keyrings that are stuck to the ring by the magnetic fields. So far I did not pry open my ring to see what it looks like inside.

The next question is why does this open (some) electronic locks? Electronics is not my strongest point (as you could have read in my previous posting), but by now I understand a little more about it.

Solenoid VS Electro motor

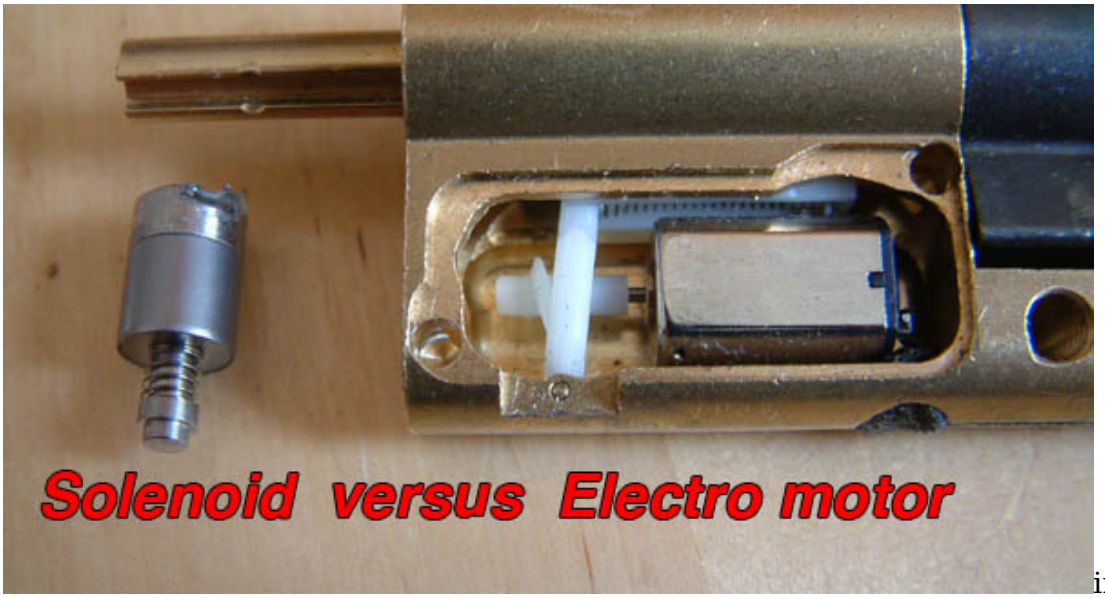

image: Winkhaus BlueChip solenoid vs electro motor from Burgwachter (ring will NOT open this lock!)

First things first: Over the years we have visited many lock companies, and if they had electronic (or electro mechanical) locks they all proudly showed us their lock was not using a solenoid. A solenoid is a metal pin that is being pulled into its housing by an electro magnet. So when current is applied to this coil, the electro magnetic field will pull the pin in, allowing the lock to open. The problem with a solenoid is that a nearby magnet can pull the pin down as well, and thus open the lock (like in the first generation Winkhaus BlueChip, problem fixed in later generations). On top of that vibrations also sometimes can bypass solenoids. So instead of a solenoid most manufacturers nowadays use a small electronic motor. If the motor makes a couple of rotations, a blocking element is pulled back and the lock opens. Turning the electronic lock the other way pushes back the blocking element and the lock is closed. A foolproof system…. until now.

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

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.

Currently we are testing with this magnetic ring. Jord Knaap and Han Fey already found one other electro/mechanical lock that seems to open under some conditions with this technique. As with all problems we personally discover, we are first going to notify the manufacturer to give them some time to analyze the problem. But with the 'devils ring' out on the free market it will probably be a matter of day's/weeks before other people will find (and report) locks that are vulnerable to it.

I can assure you this is not the last post about this new attack on electronic (and electro mechanical) locks on this weblog .....

Posted in English, news, picktools |

27 Responses to "A new attack on electronic locks: The magnetic ring"

1. *Jaakko Fagerlund* Says:
   June 16th, 2008 at 13:29

   So the ring was made from available materials, because the magnet I showed (radially magnetized) is basically the same but with only two poles. THe four pole version works faster and it is easy to make specific sizes.

   Indeed very clever attack and I can't wait to see what is the fix for these :)

2. *JackNco* Says:
   June 16th, 2008 at 17:40

   Thanks for the update Barry. I just emailed a small company I know who are developing a lock which I think could be susceptible to this (or possible the bluechip style) attack, maybe this will get the problem fixed before it even goes on sale.

   John

3. *Francis* Says:
   June 16th, 2008 at 18:29

   Besides having the electronics detect this type of attack (either by using a mouse like decoder or current sensing) and applying power to keep the motors in place, I'm curious how they can design around it. Are there non magnetic electronic devices capable of movement? Muscle Wires probably wouldn't fit this bill. (Apply heat to open lock ;-))

4. *Ryan* Says:
   June 16th, 2008 at 18:40

software update would be able to detect this attack by sensing the current generated from the “the ring of the devil”, log that event, and then apply current in the reverse direction to keep the motor from turning. If power was removed (by a determined individual), the attack would still work. If backup power was battery supplied, it is still possible to use the attack long enough to drain the battery to the point where the ring would overpower the controller. However, if the security system is still active, the cops will show up before you can drain it far enough.

I wonder if it also has a solenoid to prevent the motor from turning in the event of an attack?

Another possibility is that if you apply a magnetic field intense enough, the motor’s windings may eventually overheat, short circuit, and disable the controller. The magnets inside of the motor would still respond to the external magnetic field and the lock would open.

Anybody interested in creating a more complicated “ring of the devil”? One could create a toroid (doughnut shape) with multiple windings and then attach a controller to apply current to the coils in a “rotating” manner. This could be made powerful enough to probably overpower the lock controller’s reverse “anti-attack” current. At the very least it would be faster way of draining the backup battery. It would also be silent and less conspicuous than a power drill. Battery and controller in your pockets, toroid in your hand, and a long sleeve shirt to conceal the wires.

Then there’s the issue of how the security system communicates with the lock. If wirelessly and with a battery backup, metal bracelets are a sure thing. If the lock is in the door frame with a battery backup and secure shielding of the wires, metal bracelets are in your near future unless you can detect the communication frequency and jam it and the lock doesn’t continuously communicate with the security system. If wired with a battery back up, then the placement of the wires or contacts inbetween the door and frame would be critical, but could still be suceptible if the lock doesn’t continuously communicate with the security system.

Anyway, I should probably get back to my electrical engineering homework. Thanks for reading my two cents. Ryan

5. *Ryan* Says:
June 16th, 2008 at 18:47

O.K., I’m procrastinating from my homework. This attack could be rendered completely useless if the lock’s motor consisted of two sets of coils instead of coils and permanent magnets like all conventional electric motors. Ryan

6. *ChillyWilly* Says:
June 16th, 2008 at 18:58

One kind of muscle wire may not be affected by the magnets but will definetly be affected by heat. Raising the material’s temperature makes it change length (that’s the short version of the explanation). There is a second kind of “muscle wire” that

Ryan, what you desribed is working only if the small DC-motor is such that there is stator coils and rotor magnets. BUT, the motor in the picture also seems to have only two leads, indicating a basic brush type DC-motor that has rotor coils and stator magnets.

Thus, if the software in the lock keeps the motor winding circuit open-loop (opposite to having the wires shorted), the magnet attack doesn't work, because there is no current induced in the coils or more precisely, it has nowhere to go, so the motor doesn't turn.

8. *Ryan* Says:
June 16th, 2008 at 20:50

Jaakko, great point, but it does raise another question: How would a rapidly rotating magnet field penetrate the metal case and stator magnets to produce a current to generate electromotive force strong enough to turn the rotor and counter the external magnetic field in the first place? Wouldn't any induced current create the same/wrong polarity of magnetic field anyway?

Maybe I should get back to learning about this stuff...

9. *drew* Says:
June 16th, 2008 at 20:54

There is a rather low-tech way to protect against this attack: shield the motor/solenoid with magnetically soft material. If you've ever taken apart a hard drive, generally the magnets will be stuck to Mu-metal(see link) - which transmits the magnetic field very poorly, if at all. Although, wikipedia says that it works best against low-frequency magnetic fields so if you spin the ring fast enough you can get by it. If you want to get really fancy, use superconductive shielding and be impervious to external magnetic fields

Jaakko: I think you're right that any brushed DC motor will be invulnerable as long as the rotor coils are kept open when it's off. I think Ryan was saying the same thing - use a motor with both rotor coils and stator coils.

10. *mh* Says:
June 16th, 2008 at 21:06

One big flaw you could introduce into electronic locks is to put the locking mechanism into the outside knob where magnets and sledge hammers etc can reach it. To be fair though these locks are not marketed for doors where sledge hammer attacks are to be expected.

For ideas that don't involve magnetic fields see this example: http://www.wipo.int/pctdb/en/wo.jsp?wo=2007022910

Cheers,

How about fixing the problem by mounting he small motor 90°/perpendicular to the axle/shaft inside the knob?

12. *rugelindinda* Says:
June 17th, 2008 at 03:18

You can find a devil's ring in a pc hard drive, but with 8 poles.

13. *Ryan* Says:
June 17th, 2008 at 04:52

Any mounting inside the knob would be extemely vulnerable to a sledge hammer type attack (thanks mh). Even inside of a door or frame, an electomagnetic field could be created that could be effective as an attack if permanent magnets are used on the motor's rotor. It's somewhat common these days to have high-performance DC motors with magnets on the rotor.

Shielding would defintely limit the potential for attack except to very strong magnetic fields. It seems to me that the only way to eliminate the possibility of this type of attack would be a motor with coils for both rotor and stator, I think it's called series-winding? Or at least a solenoid that locks the motor's rotor unless both the lock controller and security system deems it necessary.

14. *Lars* Says:
June 17th, 2008 at 05:24

Why not just use a design where there are two motors, and each need to remove an obstacle, but need to turn in opposite directions to do so. You\'d be hard pressed to generate any external interference that would spin two similar (and similarly aligned) motors in two opposite directions.

15. *ejonesss* Says:
June 17th, 2008 at 08:09

updating the firmware will do no good because it looks like the magnet ring works the magnets of the motorized lock.

all the firmware can do is log any openings of the door.

16. *Jaakko Fagerlund* Says:
June 17th, 2008 at 11:52

ejonesss, learn electronics first, because it is possible to turn a DC-brush-motor with a magnet, if the leads are shorted. Microprocessor outputs can be in three different modes: high, open or low. If the motor lead outputs are high and low, or low/high, the motor turns. If the outputs are high and high, or low and low, the motor is shorted and the magnet can open it. BUT, if you modify the software to keep the other or both outputs as open, the motor windings are open circuit and the magnet doesn't work.

Normally a microprocessor can't source that much current.
Since the motor can go both forward and reverse i would guess there to be a H-bridge or equal. so lets think about it:

1) What is the most common way to drive a small DC motor ?
2) Even if the microprocessor sets its motor control pin(s) to input (after a firmware update) how would the common driver circuit react ?

Regards
Benjamin

18. *jim a.* Says:
June 17th, 2008 at 14:18

To design around this, I think that the way to go would be to have two motors close to each other (perhaps co-axial?) S.T. an external magnetic field that would turn one to the unlocked position would simultaneously turn the other to a locked position.

19. *Jaakko Fagerlund* Says:
June 17th, 2008 at 15:21

Benjamin, the motor I see in the picture is probably some 3V model and those operate on very low currents. Even a regular PIC can source/drain 25mA per pin and was it 100mA total continously and even more when operated in short amounts, like this application.

If there is external H-bridge, nothing changes to my description.

20. *Jean-Claude* Says:
June 17th, 2008 at 17:50

Poking around the U&Z website reveals some interesting patents. Watching the bypass video also reveals something, at least to me. Has anyone found an exploded diagram of the lock in question? LSS is lacking (at least my edition), and U&Z isn't giving much up.

21. *Anon* Says:
June 17th, 2008 at 19:20

This is a well-known principle and one that can be easily protected against. Simply create a compound motor - one that is, in effect, two motors with their coils opposed. Forced induction (of the type mentioned above) will be useless against this design as an equal current will be induced in both sets of coils, hence two forces will be generated that oppose each other. In order to manually operate the motor two currents are required, in opposing polarity - something that can not be achieved by induction, but is possible when the motor contacts are accessible.

A similar principle is employed in guitars using hum-bucking pickups - just google

I would expect you can use stepped motors to prevent this type of attack.
Any other motor I think is susceptible, no matter if its ac or dc, with magnets or without.

23. *Jaakko Fagerlund* Says:
June 20th, 2008 at 01:31

    Breakable, think again: It realy has difference if it is AC or DC and with permanent magnets or not.

24. *mh* Says:
June 21st, 2008 at 08:11

    http://uk.youtube.com/watch?v=c0tr-rUQ3ZI&feature=related

    So what can we see here?
    Is that the firmware update at 1:20 and should this show that the lock now detects the attack and prevents it?

25. *Barry* Says:
June 23rd, 2008 at 10:41

    mh: Thaks for pointing to that link ;)

26. *Datsun* Says:
July 16th, 2008 at 04:12

    Just shield it well.

27. *Harald* Says:
July 23rd, 2008 at 09:24

    A simple (and cheap) reed contact/sensor will thwart this attack.

    Harry

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Enter the code shown in the image:

Submit Comment

search

- **Pages**
  - About me
- **Archives**
  - July 2008
  - June 2008
  - May 2008
  - April 2008
  - March 2008
  - February 2008
  - January 2008
  - December 2007
  - November 2007
  - October 2007
  - September 2007
  - August 2007
  - July 2007
  - June 2007
  - May 2007
  - April 2007
  - March 2007
  - February 2007
  - January 2007
  - December 2006
  - November 2006
  - October 2006
  - September 2006
  - August 2006
  - July 2006

- bumping (20)
- Dutch (27)
- Dutch Open (14)
- English (158)
- news (171)
- picktools (19)
- Uncategorized (27)

Links

Blogroll

- Sportsfreunde der Sperrtechnik

Meta

- Login
- WP FORGED
- W

---

blackbag is proudly powered by WordPress ♦ Entries (RSS) and Comments (RSS). ♦ 20 queries. 0.213 seconds.
Theme Darkfall by jINKs