*Homeland Security News Wire*

# Homeland Security News Wire

### Black Hat-DefCon round-up

# The world (supposedly) safest locks easily defeated by paper clips, screw drivers

Published 2 August 2010

Share
(http://www.addthis.com/bookma
v=250&username=newswirepubs)

| (#)    (#)    (#)    (#)

**Security experts demonstrate how locks which tout themselves as the safest lock available — fingerprints-based Biolock Model 333; Kwikset, a programmable "smartkey" lock , the innovative iLoq C10S which uses the action of a key being pushed into the lock to generate power for electronics that then checked data in a chip on the key to determine whether the user is cleared for access; AMSEC electronic safe Model es1014; KABA InSync deadbolt — can be easily defeated by using nothing more than wires, magnets, air, shock, paper clips, screw drivers, and other improvised tools**


If it can be locked, that lock can be picked // Source: blogs.com

Security maverick Marc Tobias showed hackers on Saturday how simple it is to defeat some of the world's top high-tech locks. "These locks might be winning awards but they are forgetting the basics," Tobias said while giving (http://www.google.com/hostednews/afp/article/ALeqM5gqbsdBcYfpKPMDNmlAO 4-KXiAqcA) AFP a first-hand look at how to crack several models. "They might be clever, but they aren't secure."

A Biolock Model 333 (http://www.biolockusa.com/) , designed to scan fingerprints and unlock for chosen people. was opened by simply pushing a paper clip into a key slot. An Amsec ES1014 digital safe was breached by sliding a flat metal file folder hangar through a crack at the edge of the door and pressing an interior button allowing the access code to be reset.

AFP reports (http://www.google.com/hostednews/afp/article/ALeqM5gqbsdBcYfpKPMDNmlAO 4-KXiAqcA) that Tobias grew passionate when it came to an award-

winning electromagnetic lock made in China for Finland-based iLoq. The innovative iLoq C10S used the action of a key being pushed into the lock to generate power for electronics that then checked data in a chip on the key to determine whether the user is cleared for access.

Tobias and lock-cracking colleague Tobias Bluzmanis pointed out that the iLoq design counted on a small hook being tripped to reset the devices as a key was removed. In what they referred to as a viable inside attack possible on locks geared for office settings, someone could borrow a key and shave tiny bit of metal from the tip and it would no longer catch the iLoq reset hook.

A pocket-sized tool available in U.S. stores for about $60 could be used to grind down the hook in seconds, the two demonstrated.

With either method, the result would be that once a valid key is used to open the iLoq it will yield to any key or even a screw driver stuck in the slot because it remains stuck in the unlocked position.

An audit trail left by a compromised iLoq would stop at the person whose key legitimately opened the lock.

It is really clever, but it is also very defective," said Tobias, a longtime advocate for tougher standards in the lock industry. "Electromechanical locks are more secure if done right. The question is whether the technology is implemented properly."

The security.org (http://www.security.org/) crew opened a smartkey deadbolt from Kwikset (http://www.kwikset.com/KeyControl/default.aspx) — a programmable "smartkey" lock — with a key blank, a screw driver, and a vice grip tool.

The lock picking team of Marc Weber Tobias, Toby Bluzmanis, and Matt Fiddler consistently shows up at the annual DefCon gathering in Las Vegas to pop locks with wires, magnets, air, shock, screw drivers, and other improvised tools. AFP notes that their presentation this year was met with hoots and applause.

Lock-picking holds a natural appeal to hackers, who thrive on bending hardware or software to their wills.

Share (http://www.addthis.com/bookmark.php? v=250&username=newswirepubs) |

(#)  (#)  (#)  (#)

## More Stories: