

August 8, 2008 3:00 PM PDT

Lock picking with a credit card, a photocopier, and some luck

Posted by [Elinor Mills](#) [5 comments](#)



Security experts Tobias Bluzmanis, Marc Weber Tobias, and Matt Fiddler speak at Defcon about creating fake keys to high-security locks with credit cards.

(Credit: CNET News.com/Declan McCullagh)

LAS VEGAS--Don't have special lock-picking skills or equipment but want to pick a high-security lock?

A security researcher explained at the Defcon hacker conference here how to make a fake key out of a credit card that can open certain types of Medeco M3 locks used in the White House, Pentagon, and high-security areas around the world.

You need to make a picture of a legitimate key to have an image to transpose onto the plastic, which means an insider or someone with access to the key would need to cooperate, said [Marc Weber Tobias](#), a lawyer who has written a book about breaking into high-security Medeco locks called *Open in Thirty Seconds*.

Basically, someone could grab an image of the key with a camera, cell phone, copy machine or scanner, print the image on a label or sheet of plastic, and cut along the outline with an X-Acto knife.

"Everybody has known about this forever with conventional locks, like Kwikset," Tobias said. "But high-security locks advertise that they have key control, especially Medeco."

Medeco claims they have key control for the high-security locks, which means control of the ability to duplicate or simulate keys with blanks, and only authorized locksmiths are supposed to be able to make duplicates, he said. "We've shown that's all out the window," he said.

More complex cylinder configurations in the Medeco locks will require extra steps, he said.

"So we've demonstrated the ability to simply make keys for this particular high-security lock," Tobias said of a recent live demonstration. "We didn't have to break the cylinder; we were able to look at pictures that were e-mailed to us and determine the angles on the key."

Potentially millions of high-security locks are at risk, according to Tobias. The technique does not work on other types of high-security locks; Medeco locks have an integrated design that makes the technique relatively easy, he said.

A Medeco spokesman did not return an e-mail seeking comment.

Medeco executives [have previously complained](#) about Tobias disclosing vulnerabilities with the locks to the public, even though Tobias had contacted the company as well. Tobias and other security researchers defend their actions in publicly disclosing flaws, saying that if they didn't do so the vendors wouldn't fix the products.

Tobias, and the Lock Picking Village organizers, were [also showing their skills](#) at the Last HOPE hacker conference in New York last month.

During the first part of the presentation, the panelists criticized the standards that apply to high-security locks, saying that they were not broad enough to encompass the range of possible picking and breaking attacks. In other words, a lock could be perfectly standards-compliant--but able to be bypassed in under a minute.