



**Breaking Tech Information,
When You Need It Fast**

Sponsored by



COMPUTERWORLD Security

Print Article Close Window

\$10 hack can unlock nearly any office door

Erik Larkin

August 06, 2007

(PC World) Cut a couple of wires, insert a small, easy-to-make device between them, and you can walk right through all those supposedly card-protected locked office doors.

At the Defcon security conference over the weekend, a hacker and Defcon staffer who goes by the name Zac Franken showed off how a small homemade device he calls Gecko can perform a classic man-in-the-middle attack on the type of access card readers used on office doors around the country. Gecko is simply a small, programmable PIC chip with a wire connector on either side. Once it's connected to the wires behind the card reader, it's not only trivial to use a 'Replay' card to get through the door, but you can also disable the system so that nobody else can come in behind you.

What's more, making a Gecko is easy and cheap. Franken says the hardware costs about \$10.

According to Franken, the hack subverts the Wiegand protocol, commonly used for communication between the card reader and the back-end access control system, and doesn't take direct advantage of any problems with any of the hardware involved. When you swipe your card at the office, the reader very likely sends a signal using the Wiegand protocol to the control system, when then opens the doors.

"The problem is, this is what we call a plain-text protocol," Franken says. "There's nothing secure about it."

For many card readers, getting Gecko in place is just a matter of popping off the reader's cover with a knife or screwdriver and undoing two screws, he says. That provides access to the wires that carry the signal from the reader to the control system.

In a real-world situation you'd quickly cut the wires and insert one cut end into one side of the Gecko, and the other cut end into the Gecko's other side. In Franken's demonstration he used pre-made connectors so he could easily disconnect and reconnect the device. When you put the reader's cover back, the Gecko would be hidden behind it.

The card reader also continues to work fine with the Gecko attached. It passes along the signal from the reader to the control system as it's supposed to. But when someone swipes an authorized card that unlocks the door, Gecko saves that signal.

Respond now
for your free guide to
faster WAN application delivery.

Speed Brief
**MAKE YOUR WAN
WORK LIKE A LAN**
A GUIDE TO FAST
APPLICATION DELIVERY
AT THE BRANCH

CITRIX

With that saved unlock signal, the attacker can swipe a 'replay' card that tells Gecko to re-send that saved signal, and the doors unlock. What's more, any saved access logs would only show that the same person who originally swiped the saved signal swiped his card again.

The replay card isn't anything special, and could be any card -- it's just one that Gecko knows about beforehand. When it sees that card's code -- which it does because the card reader passes it along -- Gecko knows to send its saved signal in response.

The device also knows to look out for another card code -- again, just a regular card -- and in that case, disable the system. Only the recognized replay card can unlock the door. Every other card, authorized or not, will fail.

With nobody else able to use that door, an invader would have plenty of time to steal data or work his mischief. Other, non-Gecko modified doors would continue to work, though. And the attacker can re-enable the system and turn everything back to normal by swiping a third 'enable' card.

Franken says you wouldn't need to add the device right behind the card reader. If you knew where the wires went through a wall panel or anywhere else in the building, you could splice it in there.

Also, he says that biometric devices use the Wiegand protocol as well and could also be vulnerable to a Gecko inserted behind it. For a Gecko to work well behind a high-security retina scanner, for example, he would add the ability for the device to accept a wireless signal. In that case, the Gecko would save an authorized signal, and then replay that command when the attacker sent a Bluetooth signal from his PDA -- with no need to fake an eyeball.

According to Franken, building security could mitigate the risk by using tamper-resistant card readers that might break if you tried to unscrew them from the wall, or at least set off an alarm if you pop the cover. Such protections can be subverted, he says, but they'd help.

But the real solution, he says, is to replace the Wiegand protocol with one that uses secure communications between the reader and the control system.

Robert McMillan of the IDG News Service contributed to this story.