Hacker Cracks, Clones RFID Passport

By Jay Lyman
TechNewsWorld
08/07/06 3:10 PM PT

Back to Online Version
E-Mail Article
Digg It
Reprints

A security consultant demonstrated at the Black Hat and Defcon security conferences in Las Vegas last week the method he used to crack an RFID-based e-passport like the one the U.S. government plans to begin issuing to citizens this fall. He also showed how he was able to clone the RFID chip inside the passport.

The wireless data transfer capabilities of radio frequency identification (RFID) tags are intended to speed and assist transactions, but it appears the RFID chips of new U.S. passports are speeding and assisting circumvention, according to a German expert's demonstration at last week's Black Hat hacker conference in Las Vegas.

DN Systems consultant Lukas Grunwald showed conference attendees how he could not only crack the RFID-based U.S. passport, but also had the ability to clone the RFID chip inside, thereby creating a bogus passport that could theoretically allow easy access into the U.S. or other nation for its holder.

Experts following the technology, currently being introduced in the U.S. and Europe, contend that passports are the wrong place for RFID, even with protections vowed by the U.S. government such as its plan to use a card swipe or other type of secure transaction along with the passports.

"One of the difficult things about this technology is it's got an inherent privacy and security risk to it," Electronic Frontier Foundation (EFF) Senior Staff Attorney Lee Tien told TechNewsWorld. "The whole idea of having your information broadcast or transmitted via radio waves is something that creates privacy and security risk."

Circumvention Demonstration

At Black Hat and at the subsequent Defcon hacker conference, Grunwald showed just how simple and inexpensive it could be to circumvent the U.S. e-passport's RFID technology. Grunwald reportedly needed only a couple of weeks and less than $250 to accomplish the cloned U.S. passport chip.

Tien said the demonstration illustrates that for those with some technical understanding and expertise, cracking RFID is not difficult, as there is a signal to intercept and study, along with the data being transferred.

Tien also voiced concern that increasing use of the technology will nonetheless breed confidence in it, and as a result we may see a marked increase of so-called "unattended transactions," where there is no other person or contact required to complete those transactions.

Only Disadvantages

Some RFID and security experts, such as Johns Hopkins University Information Security Institute Director Avi Rubin, believe that using the technology in passports now is premature.

Rubin, whose research team has poked significant holes in other RFID systems, said he could understand why the technology would be useful for shipping, inventory or other applications, but stressed it is the wrong type of technology for personal identification and passport transactions.

"I can't see the need for wireless," Rubin told TechNewsWorld. "I can only see negatives. I can't see any positives. I only see disadvantages to this."

What's the Point?

EFF's Tien echoed that criticism. Cryptography and encryption are techniques aimed at safeguarding information and making sure it does not get out, while RFID is intended for the opposite, he noted.

"The whole modus operandi of this product is that it's being broadcast over the airwaves," Tien said.

He reported the biggest concession from the U.S. government on the matter has been a recognition of the need for continued contact transactions, as information exchanges currently are. However, the added step seems to defeat the purpose of the passport's RFID technology, according to Tien.

"Once you're doing that, you've translated the contactless transaction into a contact card, and the next question is, why?" ECT

Next Article in Security: Dangerous Web Site Ahead, Google Warns