Hackers Clone E-Passports

Story Images

Click thumbnails for full-size image:

Breaking News from AP:

- Dangerous John Coming Closer to Mexico
- Israel Rejects Annan Demand on Blockade
- Iran Ignores Powers, U.N. on Enrichment
- Lawyer Charged With Murdering Neighbor
- 9/11 Ads Ask Where You Heard the News
- Is Peru's Famed 'Ice Maiden' in Danger?
- Dow Closes Up 13, Nasdaq Finishes Up 13
- Nominees Announced for 2006 CMA Awards
- GM Withdraws CBS' 'Survivor' Sponsorship
- Nadal, Safin Win Openers at U.S. Open

See Also

- The RFID Hacking Underground
- Fatal Flaw Weakens RFID Passports
- Lawmaker Rips RFID Passport Plans
- Feds Rethinking RFID Passport
- Passport Chip Criticism Grows
- American Passports to Get Chipped

By Kim Zetter | Also by this reporter
02:00 AM Aug, 03, 2006

LAS VEGAS -- A German computer security consultant has shown that he can clone the electronic passports that the United States and other countries are beginning to distribute this year.

The controversial e-passports contain radio frequency ID, or RFID, chips that the U.S. State Department and others say will help thwart document forgery. But Lukas Grunwald, a security consultant with DN-Systems in Germany and an RFID expert, says the data in the chips is easy to copy.

"The whole passport design is totally brain damaged," Grunwald says. "From my point of view all of these RFID passports are a huge waste of money. They're not increasing security at all."

Grunwald plans to demonstrate the cloning technique Thursday at the Black Hat security conference in Las Vegas.

The United States has led the charge for global e-passports because authorities say the chip, which is digitally signed by the issuing country, will help them distinguish between official documents and forged ones. The United States plans to begin issuing e-passports to U.S. citizens beginning in October. Germany has already started issuing the documents.

Although countries have talked about encrypting data that's stored on passport chips, this would require that a complicated infrastructure be built first, so currently the data is not encrypted.

"And of course if you can read the data, you can clone the data and put it in a new tag," Grunwald says.

The cloning news is confirmation for many e-passport critics that RFID chips won't make the documents more secure.

"Either this guy is incredible or this technology is unbelievably stupid," says Gus Hosein, a visiting fellow in information systems at the London School of Economics and Political Science and senior fellow at Privacy International, a U.K.-based group that opposes the use of RFID chips in passports.

"I think it's a combination of the two," Hosein says. "Is this what the best and the brightest of the world could come up with? Or is this what happens when you do policy laundering and you get a bunch of bureaucrats making decisions about technologies they don't understand?"

Grunwald says it took him only two weeks to figure out how to clone the passport chip. Most of that time he spent reading the standards for e-passports that are posted on a website for the International Civil Aviation Organization, a United Nations body that developed the standard. He tested the attack on a new European Union German passport, but the method would work on any country's e-passport, since all

of them will be adhering to the same ICAO standard.

In a demonstration for Wired News, Grunwald placed his passport on top of an official passport-inspection RFID reader used for border control. He obtained the reader by ordering it from the maker -- Walluf, Germany-based ACG Identification Technologies -- but says someone could easily make their own for about $200 just by adding an antenna to a standard RFID reader.

He then launched a program that border patrol stations use to read the passports -- called Golden Reader Tool and made by secunet Security Networks -- and within four seconds, the data from the passport chip appeared on screen in the Golden Reader template.

Grunwald then prepared a sample blank passport page embedded with an RFID tag by placing it on the reader -- which can also act as a writer -- and burning in the ICAO layout, so that the basic structure of the chip matched that of an official passport.

As the final step, he used a program that he and a partner designed two years ago, called RFDump, to program the new chip with the copied information.

The result was a blank document that looks, to electronic passport readers, like the original passport.

Although he can clone the tag, Grunwald says it's not possible, as far as he can tell, to change data on the chip, such as the name or birth date, without being detected. That's because the passport uses cryptographic hashes to authenticate the data.

When he was done, he went on to clone the same passport data onto an ordinary smartcard -- such as the kind used by corporations for access keys -- after formatting the card's chip to the ICAO standard. He then showed how he could trick a reader into reading the cloned chip instead of a passport chip by placing the smartcard inside the passport between the reader and the passport chip. Because the reader is designed to read only one chip at a time, it read the chip nearest to it -- in the smartcard -- rather than the one embedded in the passport.

The demonstration means a terrorist whose name is on a watch list could carry a passport with his real name and photo printed on the pages, but with an RFID chip that contains different information cloned from someone else's passport. Any border-screening computers that rely on the electronic information -- instead of what's printed on the passport -- would wind up checking the wrong name.

Grunwald acknowledges, however, that such a plot could be easily thwarted by a screener who physically examines the passport to make sure the name and picture printed on it match the data read from the chip. Machine-readable OCR text printed at the bottom of the passport would also fail to match the RFID data.

Frank Moss, deputy assistant secretary of state for passport services at the State Department, says that designers of the e-passport have long known that the chips can be cloned and that other security safeguards in the passport design -- such as a digital photograph of the passport holder embedded in the data page -- would still prevent someone from using a forged or modified passport to gain entry into the United States and other countries.

"What this person has done is neither unexpected nor really all that remarkable," Moss says. "(T)he chip is not in and of itself a silver bullet.... It's an additional means of verifying that the person who is carrying the passport is the person to whom that passport was issued by the relevant government."

Moss also said that the United States has no plans to use fully automated inspection systems; therefore, a physical inspection of the passport against the data stored on the RFID chip would catch any discrepancies between the two.

There are other countries, however, that are considering taking human inspectors out of the loop. Australia, for one, has talked about using automated passport inspection for selected groups of travelers, Moss says.

In addition to the danger of counterfeiting, Grunwald says that the ability to tamper with e-passports opens up the possibility that someone could write corrupt data to the passport RFID tag that would crash an unprepared inspection system, or even introduce malicious code into the backend border-screening computers. This would work, however, only if the backend system suffers from the kind of built-in software vulnerabilities that have made other systems so receptive to viruses and Trojan-horse attacks.

"I want to say to people that if you're using RFID passports, then please make it secure," Grunwald says. "This is in your own interest and it's also in my interest. If you think about cyberterrorists and nasty, black-hat type of guys, it's a high risk.... From my point of view, it should not be possible to clone the passport at all."

Hosein agrees. "Is this going to be the massive flaw that makes the whole house of cards fall apart? Probably not. But I'm not entirely sure how confident we should feel about these new passports."

Grunwald's technique requires a counterfeiter to have physical possession of the original passport for a time. A forger could not surreptitiously clone a passport in a traveler's pocket or purse because of a built-in privacy feature called Basic Access Control that requires officials to unlock a passport's RFID chip before reading it. The chip can only be unlocked with a unique key derived from the machine-readable data printed on the passport's page.

To produce a clone, Grunwald has to program his copycat chip to answer to the key printed on the new passport. Alternatively, he can program the clone to dispense

with Basic Access Control, which is an optional feature in the specification.

Grunwald's isn't the only research on e-passport problems circulating at Black Hat. Kevin Mahaffey and John Hering of Flexilis released a video Wednesday demonstrating that a privacy feature slated for the new passports may not work as designed.

As planned, U.S. e-passports will contain a web of metal fiber embedded in the front cover of the documents to shield them from unauthorized readers. Though Basic Access Control would keep the chip from yielding useful information to attackers, it would still announce its presence to anyone with the right equipment. The government added the shielding after privacy activists expressed worries that a terrorist could simply point a reader at a crowd and identify foreign travelers.

In theory, with metal fibers in the front cover, nobody can sniff out the presence of an e-passport that's closed. But Mahaffey and Hering demonstrated in their video how even if a passport opens only half an inch -- such as it might if placed in a purse or backpack -- it can reveal itself to a reader at least two feet away.

Using a mockup e-passport modeled on the U.S. design, they showed how an attacker could connect a hidden, improvised bomb to a reader such that it triggers an explosion when a passport-holder comes within range.

In addition to cloning passport chips, Grunwald has been able to clone RFID ticket cards used by students at universities to buy cafeteria meals and add money to the balance on the cards.

He and his partners were also able to crash RFID-enabled alarm systems designed to sound when an intruder breaks a window or door to gain entry. Such systems require workers to pass an RFID card over a reader to turn the system on and off. Grunwald found that by manipulating data on the RFID chip he could crash the system, opening the way for a thief to break into the building through a window or door.

And they were able to clone and manipulate RFID tags used in hotel room key cards and corporate access cards and create a master key card to open every room in a hotel, office or other facility. He was able, for example, to clone Mifare, the most commonly used key-access system, designed by Philips Electronics. To create a master key he simply needed two or three key cards for different rooms to determine the structure of the cards. Of the 10 different types of RFID systems he examined that were being used in hotels, none used encryption.

Many of the card systems that did use encryption failed to change the default key that manufacturers program into the access card system before shipping, or they used sample keys that the manufacturer includes in instructions sent with the cards. Grunwald and his partners created a dictionary database of all the sample keys they

found in such literature (much of which they found accidentally published on purchasers' websites) to conduct what's known as a dictionary attack. When attacking a new access card system, their RFDump program would search the list until it found the key that unlocked a card's encryption.

"I was really surprised we were able to open about 75 percent of all the cards we collected," he says.

Â