

Expert Issues Warning About E-Passports

August 6, 2006 - 2:50PM

Electronic passports being introduced in the U.S. and other countries have a major vulnerability that could allow criminals to clone embedded secret code and enter countries illegally, an expert warned.

A demonstration late Friday by German computer security expert Lukas Grunwald showed how personal information stored on the documents could be copied and transferred to another device.

It appeared to contradict assurances by officials in government and private industry that the electronic information stored in passports could not be duplicated.

"If there is an automatic inspection system, I can use this card to enter any country," Grunwald said, holding up a computer chip containing electronic information he had copied from his German passport.

The research is the latest to raise concerns about the growing use of RFID, short for radio-frequency identification, which allows everyday objects such as store merchandise, livestock and security documents to beam electronic data to computers equipped with special antennas.

Countries such as Germany already use RFID in passports to help border officials guard against forgeries and automate the processing of international visitors. U.S. officials plan to start embedding RFID in passports in October.

A State Department spokeswoman said late Saturday she did not have enough information on the matter to comment.

The presentation was one of dozens delivered at the Defcon conference being held through Sunday in Las Vegas. The conference, attended by many of the world's best-known security experts, has become an annual showcase of the latest discovered weaknesses in computers, phone equipment and other machines.

Another security professional showed how people can have their phone numbers hijacked when using certain types of equipment that route calls over the Internet.

The research, from Arias Hung, a security professional with Media Access Guard in Seattle, showed how to control the inner workings of Internet phone routers made by Linksys, which is owned by Cisco Systems Inc. of San Jose, Calif.

Once the routers are accessed, a person can change the device's so-called media access control address, which acts as a serial number that Internet phone providers such as Vonage Holdings Corp. use to verify the identity of customers. A person exploiting the flaw could intercept calls made to a legitimate Vonage user and make calls that would appear to come from the user's phone number.

"The service providers should be very concerned," Hung said. "The general consumer should stay away from this router," he said, referring to two models that Linksys designates the WRTP54G and the RTP300.

Cisco spokeswoman Molly Ford said she could not immediately comment on Hung's research.

Although Defcon focuses largely on computers, not all the research focused on circumventing high tech gizmos.

Marc Tobias, a South Dakota lawyer who authored a textbook for locksmiths, showed how a simple technique can allow a person to secretly pick the locks of most homes, businesses and post office mailboxes.

The method, known as bumping, requires a person to file down a key and then gently tap it into a lock.

"You can do this with virtually every lock," said Tobias, who is calling for a change to U.S. postal regulations to prohibit the trafficking of bump keys, which are advertised for sale on the Internet.

—

On the Net:

<http://www.defcon.org>

<http://www.security.org>

© 2006 [AP DIGITAL](#)

This story is sourced direct from an overseas news agency as an additional service to readers. Spelling follows North American usage, along with foreign currency and measurement units.

[Get The Age home delivered for as little as \\$2.70 a week*](#)

More Technology

Copyright © 2006. The Age Company Ltd