c|net NEWS.COM http://www.news.com/

Researchers: E-passports pose security risk

By Declan McCullagh
http://news.com.com/Researchers+E-passports+pose+security+risk/2100-7349_3-6102608.html

Story last modified Tue Aug 08 12:05:04 PDT 2006

LAS VEGAS--Radio tags used in everything from building access cards to highway toll cards to passports are surprisingly easy to copy and pose a grave security risk, researchers said this week.

At a pair of security conferences here, researchers demonstrated that passports equipped with radio frequency identification (RFID) tags can be cloned with a laptop equipped with a $200 RFID reader and a similarly inexpensive smart card writer. In addition, they suggested that RFID tags embedded in travel documents could identify U.S. passports from a distance, possibly letting terrorists use them as a trigger for explosives.

At the Black Hat conference, Lukas Grunwald, a researcher with DN-Systems in Hildesheim, Germany, demonstrated that he could copy data stored in an RFID tag from his passport and write the data to a smart card equipped with an RFID chip. The copied chip could be used in a forged passport, for example. "We programmed the chip to behave like a passport," Grunwald said in an interview with CNET News.com on Friday.

The threat of unauthorized duplication could affect millions of Americans who are scheduled to begin receiving RFID passports in October. It also calls into question assertions by government officials--who have defended implanting RFID tags in passports despite privacy worries--that the new passports will be more difficult to forge.

Video: E-passport flaws
Researchers warn of potentially serious risks.

Grunwald did say that he has not unearthed any flaws in the crypto that protect the integrity of the information stored in the chips in passports. In other words, while the data can be cloned merely by scanning the RFID tag, the information cannot be changed. Grunwald was able to read the data on the chip by duplicating a customs inspection station.

It took Grunwald "two weeks and $5,000 in legal fees" to complete his project, which uses RFID reading hardware and some homegrown software, he said. At Defcon on Friday, Grunwald also tested his setup with some corporate access cards, which he was also able to copy. This means an attacker could copy access cards and use the copies to open doors to secured buildings.

"You can add RFID in a secure way, but especially in electronic passports the standards are created by compromise, and by compromise you can not do it securely," Grunwald said. "You need a lot of research to do it right, and that research is not done right now." Grunwald is in the process of establishing a company focused on RFID security, he noted.

Around the world, governments are adding RFID tags to passports as a way to fight counterfeiting. Moving faster than the U.S., several European countries already issue passports with RFID tags. Privacy advocates and some security experts have warned about possible threats of moving to electronic passports.

Data leakage is one of those dangers. By design, RFID tags can be read by readers. In their current design, a slightly opened passport would be detectable, said Kevin Mahaffey, a researcher with wireless security company Flexilis. Although the actual data on the chip can't be read, "the simple ability for an attacker to know that someone is carrying a passport is a dangerous security breach," he said.

It may be possible to determine the nationality of a passport holder by "fingerprinting" the characteristics of the RFID chip, Mahaffey said. "Taken to an extreme, this could make it possible to craft explosives that detonate only when someone from the U.S. is nearby," he said. At Black Hat, Mahaffey showed a video that simulates just that.

Flexilis suggests a dual cover shield and a specifically designed RFID tag that will make it unreadable until the passport is fully opened. Grunwald, aware of the leakage danger, carries his passport in a pouch made of aluminum foil and noted that companies in Germany already sell specially made passport pouches to prevent the radio tag from being read.

Alternatively, Grunwald said, due to some problems with the RFID tag in the German passport, the government decided that the passport will still be valid, even with an inoperative RFID tag. The Chaos Computer Club, a German hacker club, came up with a creative solution, Grunwald said.

"The CCC is recommending to just microwave your passport," he said.