Protect Your Pocket From Hackers

TODD LEWAN

Editor's Note: I use a metal wallet myself. More because I don't want to sweat on my cards or smash receipts and such, but also for RF protection.

To protect against skimming and eavesdropping attacks, federal and state officials recommend that Americans keep their e-passports tightly shut and store their RFID-tagged passport cards and enhanced driver's licenses in "radio-opaque" sleeves.

That's because experiments have shown that the e-passport begins transmitting some data when opened even a half inch, and chipped passport cards and EDLs can be read from varying distances depending on reader techonology.

The cover of the e-passport booklet contains a metallic sheathing that can diminish the distances radio waves travel, presumably hindering unwanted interceptions. Alloy envelopes that come with the PASS cards and driver's licenses do the same, the government says.

The State Department asserts that hackers won't find any practical use for data skimmed from RFID chips embedded in the cards, but "if you don't want the cards read, put them in an attenuation sleeve," says John Brennan, a senior policy adviser at the Office of Consular Affairs.

Gigi Zenk, a spokeswoman for the Washington state Department of Licensing, says the envelope her state offers with the enhanced driver's license "ensures that nothing can scan it at all."

But that wasn't what researchers from the University of Washington and RSA Laboratories, a data security company in Bedford, Mass., found last year while testing the data security of the cards.

The PASS card "is readable under certain circumstances in a crumpled sleeve," though not in a well maintained sleeve, the researchers wrote in a report.

Another test on the enhanced driver's license demonstrated that even when the sleeve was in pristine condition, a clandestine reader could skim data from the license at a distance of a half yard.

Will Americans consistently keep their enhanced driver's licenses in the protective sleeves and maintain those sleeves in perfect shape — even as driver's licenses are pulled out for countless tasks, from registering in hotels to buying alcohol?

The report's answer: "It is uncertain ... "

And when the sleeves come off, "you're essentially saying to the world, 'Come and read what's in my wallet,'" says Marc Rotenberg, executive director of the Electronic Privacy Information Center in Washington, D.C.

By obliging Americans to use these sleeves, he says, the government has, in effect, shifted the burden of privacy protection to the citizen.

Meanwhile, researchers have raised other red flags.

- In 2006, a mobile security company, Flexilis, conducted an experiment in which the transponder of a partially opened e-passport triggered an explosive planted in a trashcan when a dummy carrying the chipped passport approached the bin. A video of the experiment was shown that year at a security conference.

Flexilis has suggested that the government adopt a dual cover shield and specifically designed RFID tag that would make the e-passport remotely unreadable until it is fully opened.

No changes have been made to the U.S. e-passport in response, according to the State Department.

- Some RFID critics wonder: Could government officials read the microchips in an enhanced driver's license or passport card by scanning people via satellite or through a cell phone tower network?

The short answer is no — because the chips in PASS cards and EDLs are "passive," or batteryless, meaning they rely on the energy of readers to power up. Passive tags are designed to beam information out 30 feet.

However, research is moving forward to make batteries tinier and more powerful, says Ari Juels, director of RSA Laboratories. A "semi-passive" tag that could transmit into the atmosphere when triggered by a reader "may be feasible at some point," he says.

Separately, a system called STAR, that adapts deep-space communications technologies to read passive tags from distances greater than 600 feet, was announced last year by a Los Angeles startup called Mojix, Inc. It uses "smart antennas" and "digital beam forming" to process signals in four dimensions — time, space, frequency and polarization. Mojix, founded by a former NASA scientist, promotes the technology for supply chain management and asset tracking.

Source URL (retrieved on *10/22/2014 - 1:01am*):
http://www.ecnmag.com/news/2009/07/protect-your-pocket-hackers?qt-recent_content=0