RFID Update
THE RFID INDUSTRY DAILY

About | Advertise | Contact

HOME ARCHIVES FORUMS MARKETPLACE SUBSCRIBE

New RFID Passport Scare -- Does it Matter?

Monday August 7th, 2006

The technology press is awash in articles today proclaiming yet another RFID security vulnerability, this time with respect to electronic passports of the variety the US will begin issuing by the millions in October. With headlines like "Biometric Passports Hacked!" and "E-passports waste of money, says security expert", the news appears, at first blush, to be damning. But as usual, upon even the slightest examination, it is revealed to be typical doomsday sensationalism. Here is what you need to know.

German security consultant Lukas Grunwald, who caused a ruckus two years ago by authoring the RFID-hacking utility RFDump, announced at a security conference last week his ability to copy the electronic contents of a German e-passport to a separate, blank RFID chip. This data-cloning technique reportedly took Grunwald only two weeks to noodle out, relying as he did on publicly available documentation for the e-passport data format. The equipment he used was simple and affordable, according to CNet: a laptop, a $200 RFID reader, and a smart card reader. And though Grunwald conducted his experiment on a German e-passport, those of many other countries would be similarly susceptible, as their data formats are standardized according to rules from the International Civil Aviation Organization, or ICAO.

The primary implication of the ability to clone e-passport data is that, in theory, a hacker could forge a passport. In a demonstration for Wired (which published this worthwhile article about it), Grunwald copied e-passport data to a common access control card. He then placed the newly programmed smartcard in front of an RFID reader and effectively tricked it into recognizing the card as a legitimate e-passport.

Sound threatening? Well consider the following, which Wired responsibly points out: e-passport data can only be "unlocked" and accessed with a unique key code that is printed on the passport itself. A hacker would therefore need physical access to the passport before she could read its electronic contents, making it impossible for her to "skim" an e-passport chip from afar and use that data to manufacture a cloned version.

And even if such a scenario were possible, the hacker would still not be able use a cloned passport because the information on the chip wouldn't match her physical appearance. Don't forget: the goal of e-passports, at least in the US, is not to automate travelers' passage through immigration points in countries around the world. On the contrary, according to Frank Moss, deputy assistant secretary of state for passport services at the US State Department, "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." (Emphasis ours.)

Notably, there are some countries, like Australia, that have considered automated passport inspection. In such cases, cloning could indeed present a problem. But it is unlikely that such countries would rely solely on the current implementation of the ICAO standards for data security. Wired reports that the designers of the e-passport specification are well aware of the potential for cloning. "What this person has done is neither unexpected nor really all that remarkable," said Moss.

It seems that the cloning demonstration is little more than an electronic version of the following: You hand me your passport. I open it and scribble down all your personal data onto a scrap of paper. I give you your passport back. Would the paper I hold up as a "copy" of your passport be much of a threat? Of course not.

The ultimate question is whether the ability to clone the electronic data offers any meaningful opportunity to the world's bad guys. At this point, it's not clear that it does.

Home | Archives | Forums | Marketplace | *Subscribe Free*
About | Advertise | Contact | Contributors | Privacy Policy
Read *RFID Update* in your favorite news reader: XML