Cloned e-passport heightens RFID security fears

By: Dave White on Thu. Aug. 3rd, 2006, 3:24PM EST
URL: http://www.mobilemag.com/content/100/102/C8965/

The e-passport might well become a thing of the present, but it's still vulnerable to hacking, as proven recently by a German computer security expert.

At a demonstration at the Black Hat security conference in Las Vegas, Lukas Grunwald, a security consultant with a German technology firm, successfully copied data from one e-passport to another, resulting in a maneuver that would fool e-passport readers into thinking that one person was passing through security when, in fact, someone else entirely was there.

The demonstration resulted in a totally cloned tag, but the hacker couldn't change any of the data... yet. Enterprising hackers of the future might be able to improve on Grunwald's demonstration.

But do they need to? The demonstration also highlighted the fact that screening computers, which can read only one RFID chip at a time, isolate the signature of the chip closest to the reader and then move on. Conceivably, someone who didn't want to be identified could carry a passport containing his real name, face, and address but which had an RFID chip that said he was someone else superimposed on the passport itself. The computer would read the top chip and then move on. If no human screener were there to double-check, the screening-evader could then confidently board an airplane or bus, or enter any sort of public building with impunity, having been identified as someone else.

So far, the U.S., which plans to begin distributing e-passports this fall, has no plans to go to a fully automated screening system. Thus, the demonstration has no bearing on intended security systems, since a person will be at the screening station to verify the scanner's findings. For his part, Grunwald said he acted in the best interests of RFID chips and e-passports, to highlight what he perceived as a flaw, calling attention to the need for heightened security. Such methods obviously need to be improved.

Company URL: