GCN
GOVERNMENT COMPUTER NEWS

Cybereye | High-tech + high-value = high-risk

08/28/06
By William Jackson,

A recent demonstration of how to read and copy digital data from an electronic passport received a lot of attention. So much attention that the Smart Card Alliance quickly issued a press release, made a round of press calls and hosted a teleconference on “why this is not a risk.”

Actually, the ability to read the digital data with off-the-shelf equipment—as Lukas Grunwald did at the Black Hat Briefings in Las Vegas this month—is a feature, not a flaw. But that does not mean we should not be concerned about the technology embedded in these documents.

The United States, which doles out more than 10 million passports each year, has mandated the use of e-passports and plans to begin issuing them late this year. A number of countries already have begun using them. They eventually will be issued by hundreds of countries, and their specifications were set by the International Civil Aviation Organization to make reading them easy.

“The specs are not secret; they are available from ICAO for a small fee,” said Neville Pattinson, director of technology for Gemalto N.V. of Amsterdam, which recently received the first contract to produce U.S. e-passports. “We have a lot of checks and balances at the software level, the protocol level and the hardware level.”

Digital data is only one of three elements that will be used to verify identity at entry points. The other two are the paper document and the individual presenting it. Supposedly all three will match, making the ability to copy digital data pointless by itself.

Digital data is protected with Basic Access Control. To unlock the chip, a machine-readable code first must be read from the paper document into the reader. This ties the digital data to the hard copy. The digital data also is digitally signed, which should keep it from being altered even if it is copied.

“Cloning somebody’s passport doesn’t get you anywhere,” said Randy Vanderhoof, executive director of the Smart Card Alliance. “Hackers are going to look at ways to read electronic data. What they can do with that data is the important thing.”

Theoretically, they can do nothing with the passport data.

The problem is that U.S. passports have a 10-year life, and it will take 10 years to phase in new electronic versions. This means, barring some major policy change, the technology specified today will be in use for at least 20 years. That’s an awfully long lifecycle for a piece of digital technology.

It is hard to imagine a technology that will not be outdated and compromised within 20 years, especially when it represents a high-value target for hackers. Add to this the radio frequency interface, which gives would-be attackers a lot of leeway in structuring attacks, and you have a platform that is likely to be exploited either by organized crime or other nations well before its life span ends.

Grunwald’s hack probably is not a real threat to the security of anyone carrying an electronic passport today. But it is troubling.

The idea behind the new passport format was to create an additional layer of security and convenience, but it also creates an additional avenue of access to sensitive data.

We will have to keep a close watch on the work of Grunwald and others like him for decades to come to ensure that vulnerabilities do not result in unacceptable risks.

William Jackson is a GCN senior writer. E-mail him at wjackson@postnewsweektech.com.