E-Passport ally responds to cloning claims

Robert Lemos 2006-08-09

An industry association released a statement disputing the importance of a recent demonstration of the ability to copy e-passport data to a smart chip, saying the ability does not amount to any actual break in the security of the digital document.

"Recent reports that there is a 'major vulnerability' that criminals could use to 'enter countries illegally' are untrue and demonstrate a lack of understanding of how the multiple security layers in place at the U.S. border work in the new e-passport system," Randy Vanderhoof, executive director of the Smart Card Alliance, said in a statement released on Tuesday.

The statement followed a demonstration at the DEFCON hacking conference by Lukas Grunwald, a security expert and writer, showing that the digital data could be read from a German passport and copied onto a smart chip emulating the radio-frequency ID tag embedded in the digital passport. Researchers from security firm Flexilis also demonstrated that a passport built to the U.S. specifications leaks information if not completely closed.

The concerns focus on the U.S. government's initiative to create machine-readable passports that have already started to be rolled out to the public. Privacy and security experts have criticized the move as ill-considered, saying that the technology would leak data to those with specialized equipment, allowing Americans to be automatically identified by the passports they are carrying.

To answer the fears of privacy advocates, e-passports will have two countermeasures to make the surreptitious reading--known as skimming--of the passports more difficult. The covers of passports will have shielding material to make data leakage less likely, and use Basic Access Control (BAC) technology to authenticate the reader.

In downplaying the security threat of cloning, the Smart Card Alliance pointed out that two checks during the processing of passports make successfully cloning difficult, if not impossible. First, the written data and digital data are checked against each other by an agent. And the data on the chip inside the passport is signed with a specific key from the country of origin. Assuming the keys are not compromised, such digital signatures attest that the data originated from the nation's passport authority.