E-passports.. a neverending story!

Contributed by Roberto Preatoni (SyS64738)
Friday, 04 August 2006

The introduction of electronic passports brought about many polemics and conveyed many controversies about security. Are they completely safe, or at least safer than normal ID cards?

It doesn’t seems so. Actually, during the HOPE congress that took place in New York last month, two hackers have demonstrated yet the leaks of the RFID chips, and some days ago also a German computer consultant managed in cloning it.

The problem is that the Radio Frequency ID (RFID) contained in e-passport could be easy to copy, according to Lukas Grunwald, an expert in DNS-Systems.

"The whole passport design is totally brain damaged," Grunwald says. "From my point of view all of these RFID passports are a huge waste of money. They're not increasing security at all."

But… why is this chip so problematic? And why nobody foresaw weaknesses in the system while developing it?

The technology behind the chip, is considered so advanced because it marks each document with a sort of digital signature by the issuing country, that will help in distinguishing between official documents and forged ones.

Data encryption was the solution to most security matters, but a complicated infrastructure should have been built first, and until this infrastructure won’t be ready, data will be recorded on the chip as unencrypted.

…And if read the data, you can clone it and put it in a new tag…

Undoubtedly an uncommon ability is needed to overcome the RFID security system, but a longer testing period and a deeper studying could have contributed to a higher level of protection.

Since in all countries e-passports will be issued by the same ICAO standard, consequently once a cracker discover the method to clone one’s country e-document, he can easily reproduce all of them.

Grunwald, during a demonstration, according to wired.com, " placed his passport on top of an official passport-inspection RFID reader used for border control. He obtained the reader by ordering it from the maker -- Walluf, Germany-based ACG Identification Technologies –"… but this could be obtained also by adding an antenna to a standard RFID reader, for a global cost of $200.

Even if he managed in cloning the document, he stated that it is quite impossible to change the data (such as birthday and name) on the chip without being detected.

That's because the passport uses cryptographic hashes to authenticate the data.

This means that a terrorist whose name is in a watchlist could use a passport with his own name and date of birth but a different RFID.. without being identified.

But a screener physically examining the passport to make sure the name and picture printed on it match the data read from the chip would be enough to thwart the plot.

The truth is that these are new items that could improve global security, but they are still in a testing phase… we just have to hope that terrorists and criminals in general aren’t as much skilled as Herr Grunwald!