RFID e-passports hacking and terrorism risk says experts

Contributed by Stan Beer
Sunday, 06 August 2006
Last Updated Sunday, 06 August 2006

Passports embedded with radio frequency identification (RFID) chips can be easily cloned and can potentially make passport holders a target for terrorists, security experts have warned at conferences this week.

The Black Hat security conference in Las Vegas has for the past week provided fascinating insights into the security issues of commercial technology such as Mac OS X and Windows Vista from the some of the leading security exponents around the world.

In the latest and perhaps most disturbing presentation to date, German researcher, Lukas Grunwald, demonstrated that he could access data from the RFID chip embedded in his own passport and copy it to another RFID chip embedded in a smartcard.

One of the most frightening aspects of the demonstration is that Grunwald was able to develop the system to accomplish this task using standard hardware, his own software, with minimal funds and in a few short weeks.

Even more frightening, Grunwald was able to demonstrate at the concurrent Defcon conference that the same system could also be used to copy building access cards.

Aside from the forgery aspects, which could potentially enable criminals to steal identities and unlawfully gain access to places where they should not be, security experts have raised an even more potentially serious threat posed by e-passports with embedded RFID tags - terrorism.

RFID tags can be read wirelessly from a distance. Security specialists have raised the spectre of strategically placed hidden RFID readers being able to recognise passport holders in the vicinity and even what nationality they are. {moscomment}