Biting the hand that feeds IT

Original URL: http://www.theregister.co.uk/2006/08/04/e-passport_hack_attack/

e-passport cloning risks exposed

By John Leyden
Published Friday 4th August 2006 13:38 GMT

A security consultant has shown how to clone electronic passports based on internationally agreed designs due to begin distribution this year.

The demo came as part of a presentation by Lukas Grunwald, CTO of German security consultancy DN-Systems Enterprise Internet Solutions, on hacking new RFID technologies used for dual-interfaces cards, such as within credit cards and passports, at the Black Hat conference in Vegas yesterday.

Grunwald said the data held on RFID cards within e-passports can be copied simply, undermining claims by governments that e-passports will help stamp out forgeries. "The whole passport design is totally brain damaged," Grunwald told (http://www.wired.com/news/technology/0,71521-0.html?tw=rss.index) *Wired*. "From my point of view all of these RFID passports are a huge waste of money. They're not increasing security at all."

Two weeks close scrutiny of the RFID chips within passports already issued by the German government allowed Grunwald to develop his cloning technique. Much of that time was spent acquainting himself with e-passport standards, developed by the UN's Civil Aviation Organisation. Since all e-passports will adhere to this standard, including US e-passports due to begin circulation in October.

Grunwald first placed his German passport on an official passport-inspection reader, though access to this specialised equipment might not be necessary since he reckons its possible to adapt a standard RFID by installing a suitable antenna for around $200. Next, he booted up program used by border guards to read passports, Golden Reader from Secunet Security Networks. This data was written onto a blank passport embedded with a fresh RFID tag. Grunwald used a program he'd helped develop, called RFDump, to program the chip. The process allowed him to produce a clone of his passport that would look the same as the original document to a passport reader even though it wouldn't withstand physical inspection.

At present, data held on RFID chips within passports is not encrypted, a factor that would otherwise has frustrated the cloning attack. However the data on the chips *is* digitally signed, so it wasn't possible for Grunwald to change the data been written onto the blank

template without giving the game away. But if someone wrote the data onto an RFID chip held in a smart card they might be able to fool a passport reader into reading this data instead of that on a genuine passport. This is possible because readers only read one chip at a time and are designed to read the chip in closest proximity to a reader.

Frank Moss, deputy assistant secretary of state for passport services at the State Department, told *Wired* that even if the chips on electronic passports are cloned other security measures, such as a digital photo of its holder and the physical inspection of passports, would foil attempts to use forged or modified passports. A feature called Basic Access Control within passports means that border officials need to unlock a passport's RFID chip before it can be read. However some security experts reckon this technique provides insufficient protection over the long run and that conventional smart-cards are preferable to RFID chips.

"I'm not opposed to chips on ID cards, I am opposed to RFID chips. My fear is surreptitious access: someone could read the chip and learn your identity without your knowledge or consent," writes (http://www.schneier.com/blog/archives/2006/08/hackers_clone_r.html) security guru Bruce Schneier. "The [US] State Department is implementing security measures to prevent that. But as we all know, these measures won't be perfect. And a passport has a ten-year lifetime. It's sheer folly to believe the passport security won't be hacked in that time. This hack took only two weeks," he added. ®

Related stories

US gets RFID passports (15 August 2006)
http://www.theregister.co.uk/2006/08/15/us_gets_rfid_passports/
Industry group defends e-passports (11 August 2006)
http://www.theregister.co.uk/2006/08/11/e-passports_defended/
Kiddiprinters! EU biometric ID plans reach out for the children (31 July 2006)
http://www.theregister.co.uk/2006/07/31/eu_fingerprinting_kids/
Passport fees balloon by almost 30% (24 July 2006)
http://www.theregister.co.uk/2006/07/24/passport_fees/
UK ID card scheme near collapse, as Blair pushes cut-down 'variant' (9 July 2006)
http://www.theregister.co.uk/2006/07/09/st_id_cards_doomed_emails/
UK passport forgery free-for-all ends tonight (6 June 2006)
http://www.theregister.co.uk/2006/06/06/passport_forgery_loophole_fix/
US tests e-Passports (16 January 2006)
http://www.theregister.co.uk/2006/01/16/us_retests_epassports/