The Register®

Biting the hand that feeds IT

The Register » Internet and Law » Digital Rights/Digital Wrongs »

Original URL: http://www.theregister.co.uk/2006/08/04/cloning_epassports/

How to clone the copy-friendly biometric passport

By John Lettice
Published Friday 4th August 2006 13:08 GMT

Analysis At Black Hat yesterday, security consultant Lukas Grunwald of German company DN-Systems demonstrated the cloning of a biometric passport, observing beforehand to Wired (http://www.wired.com/news/technology/0,71521-0.html?tw=rss.index) that the "whole passport design is totally brain damaged." But should we be surprised? Not exactly, because that's precisely what it says on the tin.

Grunwald boned-up on ICAO (International Civil Aviation Organisation) documentation, bought an ePassport reader and reading software, read a passport (German, but other ePassports would do the trick too), then cloned it. We should however be clear about what he has done here - he hasn't cracked anything, but he *has* brought the fundamental flakiness of the ePassports that are now shipping to wider attention. People will no doubt be appalled, but they could just as easily have been appalled some considerable distance back in the production process because that *really is* what it says on the tin.

The ICAO documentation Grunwald consulted is publicly available, and explains the detail of the various levels of security of the ePassport system, the baseline level being something not unadjacent to zero. For standard ePassports including chip and facial biometric the ICAO assumption is that an open passport can be taken as the bearer's acceptance that the passport is willingly being made available for the data to be read, ICAO's intent here being to duplicate as closely as possible the inherent Ts & Cs of traditional passport inspection systems. But the ePassport is RFID, and therefore vulnerable to skimming and eavesdropping (i.e. being read by a concealed reader and/or having the transaction between passport and 'official' reader snooped on.

Two mechanisms will be used in ePassports to impede this; first, there is the 'tinfoil hat', a mesh of metal in the cover that blocks access to the chip when the passport is closed, and second the machine-readable zone (MRZ) of the passport. The MRZ is designed to be read visually when the passport is open, and this is then compared to the copy of the MRZ held on the chip. If the two match, then the data on the chip can be read.

There are other, optional levels of security that we'll go into shortly, but what we've covered so far is what most countries will be shipping in this generation, and what Grunwald had to deal with. Here what he did again, in slow motion this time.

Grunwald bought an official inspection reader (N.B. this is legal, and even if it weren't the volumes of machines the market will need would make it trivial to obtain one) and placed his passport on top of it. Using Golden Reader Tool (http://www.secunet.com/content.php?text=k_biometrie_epassport&ln=2) software from secunet Security Networks he read the chip in the passport. Golden Reader Tool is again freely available, and is widely used in the current round of ePassport interoperability testing. From there, Grunwald was able burn the data onto a chip in a blank sample passport page, giving him a blank document that looks to readers like the original passport.

Note that there's nothing particularly special about the official reader here, so it would be feasible with this level of security to use a homebrew reader. Note also that this is precisely what ICAO says you can do if this level of security is all that's used. MRZ comparison: "Adds (minor) complexity. Does not prevent an exact copy of chip AND conventional document."(*PKI for MRTDs offering ICC Read-Only Access V1.1*)

So what can you do with this? You've got an exact copy of the chip from one person's passport, but you do not at the moment have a mechanism for changing the data on the chip, and in order to produce an entire copy of the passport you'd need to get over the more conventional speedbumps to forgery in the rest of the document. But you do have something that's potentially quite useful, and under certain circumstances can brush aside what border security exists.

ICAO (we mentioned this quite recently) stresses that machine checking of the document is not intended to substitute for ID checking of the bearer. The ICAO systems are designed to impede the forgery or falsification of the document itself, and not to give any kind of guarantee that the bearer matches the document. Grunwald's demo doesn't quite knock the hell out of this, because all it produces is a copied chip, but it does tend to indicate that the authenticity of the full document may not be entirely rock-solid. Whatever ICAO says, however, using machines as substitutes for 'fallible' human checkers is a major part of the exercise for some governments, and opportunities for forgers can be seen here.

A full copy passport will pass a machine, and the picture (which is on the chip) only provides a barrier here if there's also a machine trying to match the face of the bearer to the face in the passport. Even then, current systems can only rationally be used as an aid or indicator for a human checker, so if there isn't one of these present it's not likely to be used. Where there is likely to be a human checker present, it will still be feasible for people carrying copied passports to pass by provided they look approximately like the picture in the passport (i.e., just the same as the good old days), because the chip in the passport will validate in the reader. Note also that the mere presence of the reader, the chip and the general ePassport security pixie dust will - no matter what the circulars say - have a psychological effect on border control staff. They will tend, because the machine says the passport's clean, to drop their guard, not really inspect either picture or bearer properly. This kind of effect is well documented, and it's the same kind of thing as people walking in and out of companies unchallenged despite wearing a security tag in the name of 'Michael Mouse'.

The *Wired* write-up suggests that "a terrorist whose name is on a watch list could carry a passport with his real name and photo printed on the pages, but with an RFID chip that contains different information cloned from someone else's passport" - but although this is possible in some circumstances, it's chancy because it oughtn't to work for reading terminals where the chip data is put onto a screen for border control. And then, nabbed with a definitely mucked-around passport, the bearer is in trouble. Grunwald suggests that the ePassport data could also be put onto a card, and then put between the chip on the ePassport and the reader, meaning that the reading comes from the card rather than the ePassport.

This is basically the same exploit, producing a data mismatch that is vulnerable to visual inspection, but is potentially helpful to the intruder because the ePassport can be genuine (although possibly on a watchlist), and because the card could be used or not depending on whether an opportunity were available.

Note also that the ability to produce a copy that will pass an unattended machine scan easily severely impedes the use of the ePassport as a general identity document and, provided what goes for ePassports goes for ID cards (which the Home Office tells us it does) undermines the UK ID card's ability to act as one. And ask yourself how you close an ID card - we'd like to know too.

ICAO suggests higher levels of security to protect additional biometrics such as fingerprint and iris, and some of these could also be used to protect the 'vanilla' ePassport. Encryption, for example, can be used to combat skimming, but in a document with a ten year lifespan encryption (as ICAO freely admits) is likely to have a limited effect. Nor does it prevent an exact copy being made. A PKI system can also be used in an attempt to ensure that the reader itself is authorised, and thus to protect the additional biometrics. This requires processing on the passport chip, and again doesn't stop a complete copy being made. This PKI system, as explained here (http://www.theregister.co.uk/2006/07/31/eu_fingerprinting_kids/) with reference to the European biometric passport, is run by the issuing authority, and is different from the PKI system administered by ICAO, which is intended to ensure that the passport chip itself has been signed by a bona fide issuing authority.

Other security, as we are all aware, is envisaged by at least some countries in the form of an online check of a central register. For facial-only biometric passports the subversion routes detailed above clearly still work here, because the copy is of a genuine chip, and it will therefore any record of that chip held on the register. Local fingerprint checking means you (you the suspect, that is) have probably got a problem because your prints don't match those on the chip. But as most of the passports in the world aren't going to have fingerprints in them for many years, it's entirely unclear why you (you the terrorist, that is) have decided to copy a fingerprinted passport.

Although online fingerprint checks aren't specifically relevant to the Grunwald demo, it's worth considering them briefly here as they're being presented by the UK, and are currently being used by the US, as a component of border defence. Effectively, an online check needn't relate to the passport at all (in the US case it doesn't), because it just checks the subject against a register of existing images. So if you'd already been into the US on one passport and you came in on another, copied passport, the fingerprint check in theory ought to get you. In the case of the UK, where the register doesn't exist and there's severe doubt that it ever will, it's more a case of in theory on steroids, but it's the same deal *provided* it works and provided the terminal actually does an online check. Even for those countries that do intend to check fingerprints against a central register, this will almost certainly be done only at limited number of points of entry, and possibly not all of the time at all of these.

Which, really, leaves us dealing with the baseline ICAO security, the obvious vulnerabilities in its specification, and sufficiently porous borders for these vulnerabilities to be exploited. Kind of like the good old days (i.e., today), isn't it? Except it costs us more. ®

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/
Bigger, dafter, creepier - Gordon Brown's ID scheme rescue plan (7 August 2006)
http://www.theregister.co.uk/2006/08/07/brown_id_expansion/
Blackjacking and RFID passport exploits star at DEF CON (1 August 2006)
http://www.theregister.co.uk/2006/08/01/defcon_blackhat_preview/
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/
Not delayed, not sleeping, dead - UK ID card scheme goes under (12 July 2006)
http://www.theregister.co.uk/2006/07/12/idcards_getting_elbow/
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/
Fortress Blair - PM bets on biometric ring of steel to 'fix' immigration (22 May 2006)
http://www.theregister.co.uk/2006/05/22/blair_biometric_migration_fix/
Passport data checks go live (14 March 2006)
http://www.theregister.co.uk/2006/03/14/passport_data_checks_live/
UK extends airport iris scan scheme (10 March 2006)
http://www.theregister.co.uk/2006/03/10/project_iris/
Biometrics and web tests for immigrants (8 March 2006)
http://www.theregister.co.uk/2006/03/08/biometric_and_web_tests_for_immigrants/
Face and fingerprints swiped in Dutch biometric passport crack (30 January 2006)
http://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/
EU ministers approve biometric ID, fingerprint data sharing (1 December 2005)
http://www.theregister.co.uk/2005/12/01/jahc_biometric_id_standards/