RFIDprotect℠

case studies 2010

www.rfidprotect.co.uk

Case Study # 1:
Bio-metric passports hacked

Hi-tech biometric passports used by Britain and other countries have been hacked by a computer expert, throwing into doubt fundamental parts of the UK's £415m scheme to load passports with information such as fingerprints, facial scans and iris patterns.

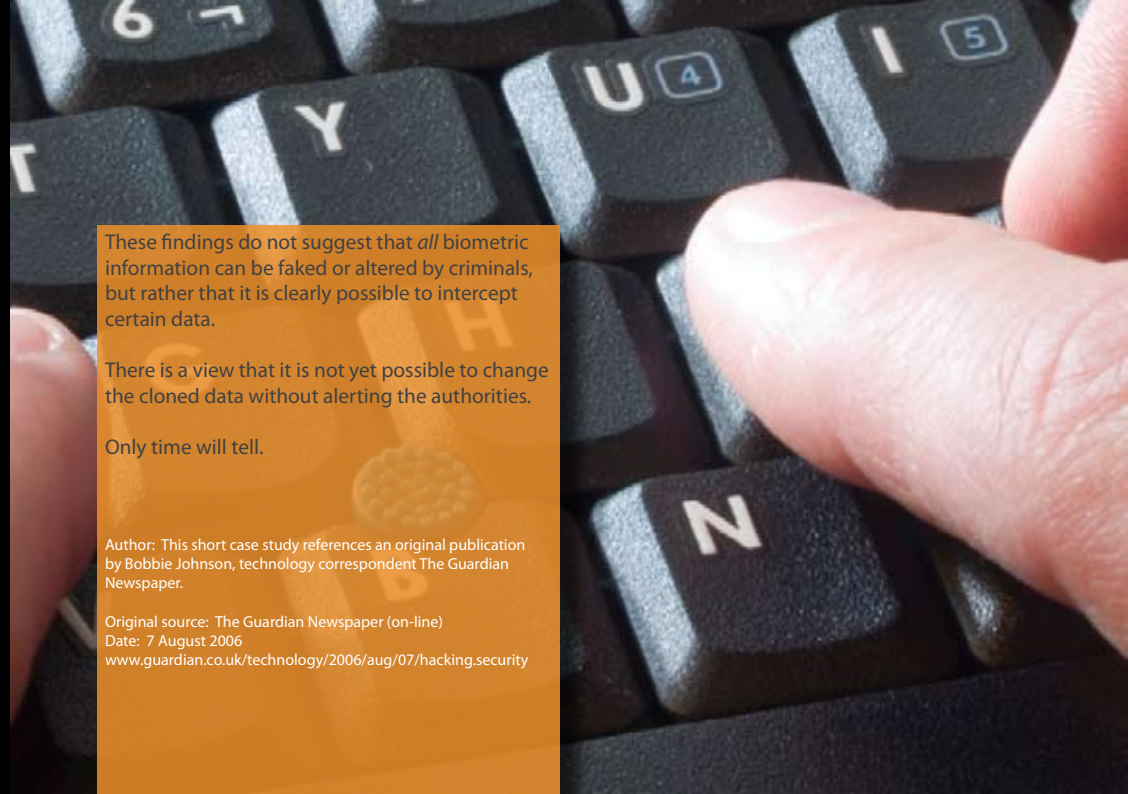
Lukas Grunwald, consultant with a German security company, told the *Defcon Security Conference* in Las Vegas that he had discovered a method of cloning information stored in the new bio-metric passports. Cloned data can be transferred onto blank chips, which could then be implanted in fake passports, a flaw which Mr Grumwald said undermined the project.

This could also, potentially cause major concerns for the UK's national ID card, which is believed could contain much of the same information.

In an interview with *Wired.com* Mr Grumwald said, "*The whole passport design is totally brain damaged*," he continued stating that, "*...from my point of view all of these [biometric] passports are a huge waste of money - they're not increasing security at all.*"

Since 2006 all UK passport have been issued with a biometric data, which contains physical identification information.

It is believed the hacking principle could be applied to any new passport issued in Britain, the US and other countries.



These findings do not suggest that *all* biometric information can be faked or altered by criminals, but rather that it is clearly possible to intercept certain data.

There is a view that it is not yet possible to change the cloned data without alerting the authorities.

Only time will tell.

Author: This short case study references an original publication by Bobbie Johnson, technology correspondent The Guardian Newspaper.

Original source: The Guardian Newspaper (on-line)
Date: 7 August 2006
www.guardian.co.uk/technology/2006/aug/07/hacking.security

Case Study # 2:
Oyster Card at Risk

Recent reports suggest that Transport for London's *Oyster Card* could be at risk following the release of code used in RFID-based access systems.

The code implements an attack in the widely used *Mifare Classic* chip. The code was released, non maliciously, as part of the so called *Crapto1project*, and is based on information published in a paper, produced by scientists from the Dutch Radboud University.

In the past, researchers have demonstrated by cloning cards, how easy it is to enter buildings via RFID access control systems, without releasing any additional details or software.

Combined with readily available hardware, users now have all the tools required to execute a successful attack.

RFID readers are available to purchase on line for less than £200, along with the necessary software which is also easily available.

Author: This short case study references an original publication by Brenno de Winter.

Original source: Computer World UK
Date: October 27, 2008
www.computerworlduk.com/technology/mobile-wireless/apps-rfid/news/index.cfm?newsid=11667

RFIDprotect™

www.rfidprotect.co.uk

Case Study # 3:
Contactless credit cards hacked

In 2006 research carried out by Tom Heydt-Benjamin and Kevin Fu, professor at Massachusettes University RFID-CUSP *(RFID Consortium for Security and Privacy)* demonstrated how easily criminals could retrieve sensitive information from the latest generation of contactless credit cards without physically stealing the card.

Attacks on these cards can be carried out using relatively cheap ($150) off the shelf RFID reading hardware and software.

Their research suggests that attacks commonly fail to retrieve verification codes, which are normally required before an on line purchase can be made, although it was potentially possible to use the data obtained to order goods and services from on line retailers that don't require the verification code.

Issuing companies have given strong assurances that data contained within RFID enabled credit cards will be encrypted. However, a growing body of research indicates that the majority of cards tested do not contain encrypted data, nor make use of alternative data protection technology.

In a sample of 20 cards tested from different issuing companies potential security risks were revealed. Furthermore, The New York Times has reported that cards can be read through items of clothing, handbags or wallets. Although, RFID technology is designed to be scanned at relatively close proximity to a reader, certain researchers have suggested that in fact cards can be read from a number of feet away. In such instances, victims would be totally unaware that they had fallen victim to an attack.

An executive from VISA has argued that additional anti-fraud measures are now in place to protect their customers. Brian Triplett, Senior Vice President for Emerging-product Development at Visa has said, *"...this is an interesting technical exercise," "..but as a real threat to a consumer — that threat really doesn't exist."*

Author: This short case study references an original publication by John Leyden

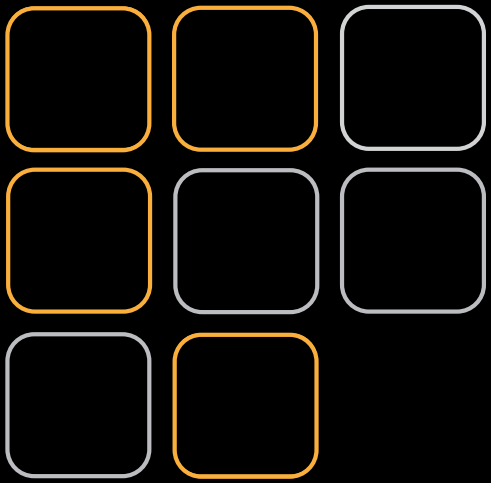
Date: 24, October 2006

Contacting us

Business hours are 9:30am to 5:30pm GMT

For further information:

T: +44 01234 772632
E: sales@rfidprotect.co.uk



RFIDprotect™


RFIDprotect
SM