RFIDprotect℠

case studies 2010

www.rfidprotect.co.uk

Case Study # 4:
Grit in the Oyster?

Transport for London's popular *Oyster Card* was upgraded in 2006 to an improved version, since serious vulnerabilities were revealed with its earlier *MIFARE* contactless card. *MIFARE Classic* - the technology in question - had until recently remained a preferred choice for transport providers.

In 2010, saw Cardiff Bus and Oxford Bus Company rolling out their version of London's *Oyster Card* with over 20,000 issued in Oxford alone.

Five years down the line since the *MIFARE* fiasco, this technology is still causing problems. More specifically, in Oxford passenger cards could not be scanned, with many told that their new cards were invalid.

Although those affected were eventually allowed to travel, people were left queuing for more than three hours at Oxford Bus Company's helpdesk in the hope of resolving the problems.

We cannot help but wonder just how many more problems will come to light as contactless card technology is introduced to many more aspects of daily life.

Author: This short case study references an original publication by The Oxford Times transport correspondent

Original source: The Oxford Times (on-line)
Date: 3 November 2010
www.oxfordtimes.co.uk/news/8490381.
Glitchcreatesbuspaymentcard_chaos/

RFIDprotect™

www.rfidprotect.co.uk

Case Study # 5:
EMP shockwave destroys e-passport data

Shortly after the introduction of the new UK e-passports in 2006 hackers successfully accessed biometric data, (i.e. physical identification information), by using remote radio frequency identification (RFID) *'skimming'* devices. In 2007, yet another problem with this contactless technology was identified; this time in the USA.

Under the expert guidance of Professor Avishai Wool, (Tel Aviv University | School of Electrical Engineering), students successfully demonstrated how easy it is to corrupt the private information contained within the USA e-passport chip.

(NB: This is the same type of RFID device that is currently used in most contactless credit, debit and access cards.)

Even more worryingly, the device used was made by using a disposable camera costing less than £20, and some copper pipe.

Explains Professor Wool, *"…this device allows hackers who are not much more than amateurs to break the system."*

Wool's team replaced the camera's flash mechanism with an antenna; adapted to deliver an intense electro-magnetic pulse (EMP) that destroyed the data on the nearby passport chip.

Whilst this development may concern some people, there are very simple measures that can be taken to avoid an EMP attack.

RFIDprotect™

www.rfidprotect.co.uk

The easiest method is to place the e-passport or other RFID enabled credit, debit or travel card in a protective sleeve, wallet or holder such as those available at http://www.rfidprotect.co.uk

Author: This short case study references an original publication by The Ecomonic Times

Original source: The Economic Times
Date: April 16, 2010
www.economictimes.indiatimes.com/infotech/internet/Expert-picks-out-loopholes-in-US-e-passports/articleshow/5821074.cms

Case Study # 6:

Tracking your every movement…

For those concerned about safeguarding their anonymity, RFID tracking devices are about to rock their world.

In October 2010, students in Texas were issued with RFID enabled ID cards in a district-wide project to monitor classroom attendance rates. The Houston Chronicle reported that, *"…RFID-enabled badges (have been) issued to about 13,500 out of 36,000 students since December 2008."*

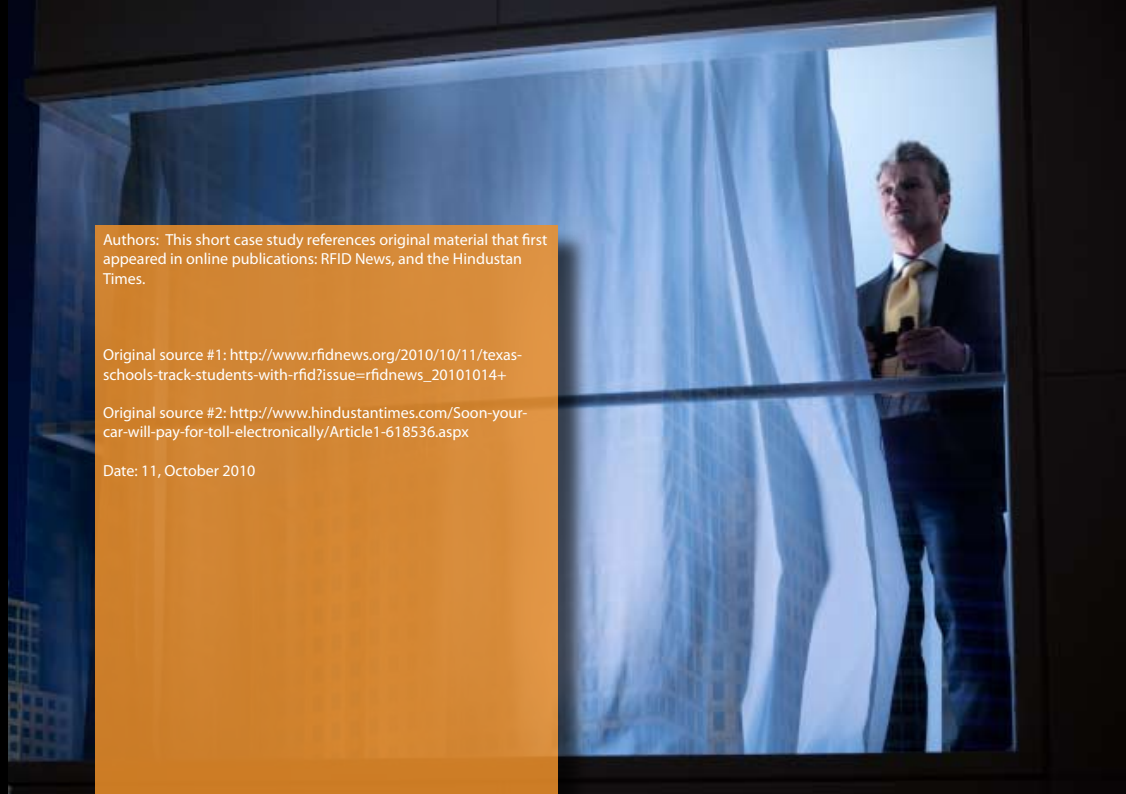
As investment funds are linked with student attendance rates, there is a compelling case for schools to adopt this new technology. At any one moment in time, the school is able to track the whereabouts of their students; so long as their ID card has not been disabled, shielded or swapped!

By April 2012, India will have made it a statutory requirement for all new vehicles to come equipped with a factory installed RFID tag. Nandan Nilekani, Chairman, Unique Identification Authority of India (UIAD), has stated that, *"…initially it will be used for toll collection on national highways - subsequently it will be used for other purposes."*

The possibilities are endless. Mr Nilekani continues by stating, *"…RFID uses communication via electromagnetic waves to exchange data between an object, in this case a vehicle and a terminal. The technology, generally used for identification and tracking purposes, can be used on any product, animal or person."*

RFIDprotect™

www.rfidprotect.co.uk



Authors: This short case study references original material that first appeared in online publications: RFID News, and the Hindustan Times.

Original source #1: http://www.rfidnews.org/2010/10/11/texas-schools-track-students-with-rfid?issue=rfidnews_20101014+

Original source #2: http://www.hindustantimes.com/Soon-your-car-will-pay-for-toll-electronically/Article1-618536.aspx

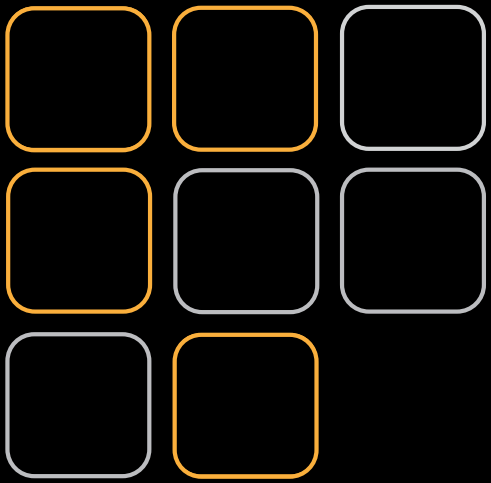
Date: 11, October 2010

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