Evening Standard
standard.co.uk

London, Sunday 11.05.08

News

Mark Prigg, Science Correspondent
14.03.08

Researchers claim to have broken the electronic security used in the Oyster card and warned the way could be opened for them to be "cloned" using home computers.

Oyster: Researchers claim to have broken security of the smartcards

German computer engineering students behind the discovery claim any of the 10 million Oyster cards in circulation could now be cloned in under 10 minutes using a standard PC and card reader.

The cloned cards could then be used by fraudsters to travel free.

The discovery has forced the Dutch government, which uses a similar card, to issue a security warning. Government institutions plan to take " additional security measures to safeguard security", said Guusje ter Horst, minister of interior affairs.

The technology used in the Oyster card, called the Mifare Classic RFID (radio frequency identification) chip, is used in a billion passes worldwide and is manufactured by a Netherlands company called NXP, founded by electronics giant Philips. The company said it was "taking these claims very seriously".

A spokesman added: "NXP has established an open dialogue with the researchers and is evaluating possible attacks." Two separate research teams have claimed to have broken the card's security.

German researchers Karsten Nohl and Henryk Plˆtz, who first hacked parts of the chip last December, this week published a paper demonstrating a way to crack the chip's encryption technology. Mr Nohl, a PhD candidate in computer engineering at Virginia University, said: "I don't want to help attackers, but I want to inform people about the vulnerabilities of these cards."

A second team, led by Bart Jacobs, an information security professor at the Radboud University in Nijmegen, has also published hacking details. However, Transport for London said today it was confident it would be able to spot cloned cards. A spokesman said: "All Oyster information is fully encrypted and we have adopted extra security measures on top of that available on the source chips."

Link to:

Reader Views (4)

| **Show all**

Here's a sample of the latest views published. You can click view all to read all views that readers have sent in.

No system is infallible, it seems. All forms of transport everywhere are susceptible to fraud. The real question is how much faster bus travel has become. This morning I was one of ten people who got on a bus at my stop. It was on its way in 30 seconds. How much longer would it have been - and therefore costlier if everyone had to pay for single ticket?
When will critics start to look at the task is to move as many people about as quickly and efficiency as possible? Why is the glass always 1% empty, rather than 99% full?

- Harold, London, England

Someone needs to tell the government that technology is not foolproof or perfect. The basic rule of thumb is, if you can encrypt something you can always decrypt it, otherwise it's useless! Walking around with RFID enabled devices will always leave you open to identity or information theft, of course the sales men who peddle this stuff wont be making ministers aware of this... Or maybe they just don't care?

- Asher Johnson, London England

Give me a travel card any day over the tracking technology used in Oyster cards. Oyster users might as well be sending out a homing signal. The Oyster cards are a major step backward in terms of efficiency. Ever notice that Oyster cards often have to be swiped multiple times across the reader before a gate opens, while travel cards let the user through first time without any problem? Ken made a huge mistake introducing the Oyster technology.

- Phil Jones, London, UK

Add your comment

Show all

Name:

Email: Your email address will not be published

Town and country:

Your comment: Terms and conditions

You have 1500 characters left. make text area bigger

Remember me - this will save your name, location and email address for when you leave your next comment.

Email me a link to these comments.

Clear submit comment