Oyster card hack to be published

by BBC report via Kismo - BBC News *Tuesday, Jul 22 2008, 9:47am*
international / miscellaneous / other press

> Details of how to copy the Oyster cards used on London's transport network can be published, a Dutch judge has ruled. The ruling overturns an injunction to suppress the information won by NXP - makers of the travel smartcards used in London and many other cities.

The injunction was sought in June 2008 after Dutch researchers demonstrated how to copy cards and travel free on the London Underground.

The researchers plan to publish their research in October.

Cracked cards

The security weaknesses in the Oyster card were discovered by Prof Bart Jacobs and colleagues from Radboud University, Nijmegen in March 2008.

The weaknesses centre on the chip, called the Mifare Classic, that sits at the heart of the contactless card system.

As well as being used on 17 million Oyster cards, the Mifare chip is used by about 1bn smartcards worldwide, and is the basis of the Dutch Rijkspas card.

Many organisations, including governments, use Mifare technology as a secure entry system for buildings.

Given the many millions of cards in use Prof Jacobs held off publishing details about how the information on the chips can be copied and used. It told the Dutch government and NXP about its work to give them time to harden systems against the attack.

Despite this, NXP sought an injunction to ensure the details of the attack would never be aired.

The case went to court in Holland and now the court in Arnhem has overturned the injunction citing local freedom of expression laws.

In its ruling, the court said: "Damage to NXP is not the result of the publication of the article but of the production and sale of a chip that appears to have shortcomings."

In a statement, Radboud University hailed the ruling and said: "...in a democratic society it is of great importance that the results of scientific research can be published".

Christophe Duverne, a spokesman for NXP, told Reuters that it would take months or years for some users of the chip to adapt their systems to defend against the attack.

"We don't mind them publishing the effects of what they have discovered to inform society, I think

this is absolutely fine," he said. "But disclosing things in detail including the algorithm ... is not going to benefit society, it will create damage to society."

A spokesman for Transport For London said: "Transport for London remains confident in the security of the Oyster card system. We take fraud and the security of personal data extremely seriously and constantly review our security procedures."

He added: "Any fraudulent card would be identified within 24 hours of being used and blocked. Using a fraudulent card for free travel is subject to prosecution and we would seek to enforce this wherever possible."

Security expert Bruce Schneier said: "As bad as the damage is from publishing - and there probably will be some - the damage is much, much worse by not disclosing."

Mr Schneier said it was a "dangerous assumption" to think that only the researchers know about weaknesses with Mifare.

"Assume organised crime knows about this, assume they will be selling it anyway," he said.

Information about the research will be published in a journal and shown at a security conference held in Malaga. The Dutch group is one of three known to have cracked the Mifare Classic technology.

http://news.bbc.co.uk/2/hi/technology/7516869.stm
