BBC NEWS

Oyster card hack details revealed

By Peter Price
Click reporter

Details of how to hack one of the world's most popular smartcards have been published online.

The research by Professor Bart Jacobs and colleagues at Radboud University in Holland reveals a weakness in the widely used Mifare Classic RFID chip.

This is used in building entry systems and is embedded in the Oyster card used on London's transport network.

Publication of the research was delayed by legal action taken by the chip's manufacturer.

Paper chase

Prof Jacobs and his team first identified the vulnerability in a research paper that was due to be published in March 2008.

However, the release of the article was delayed after chip manufacturer NXP attempted to secure a court injunction against its publication.

The paper was finally released on Monday at the European Symposium on Research in Computer Security (Esorics) 2008 security conference held in Malaga, Spain.

Sensitive data stored on the Mifare Classic chip is protected by a unique number that acts as a key. When the chip, or a card bearing it, is placed near a reader it transmits and receives information based on its key. The security of the system depends on the key remaining secret.

In March Prof Jacobs and his colleagues discovered a flaw in the chip's design which makes those keys easy to calculate and copy.

"Once we knew how the system worked and what the vulnerabilities were, it turned out to be very simple to actually clone cards, steal someone's identity and enter a building as someone else", he said.

After making the discovery the researchers informed the Dutch government and the chip's manufacturer, NXP.

When it knew about the research NXP moved to delay publication by seeking an injunction.

Steve Owen, vice president of sales and marketing - identification at NXP Semiconductors, told the BBC's Click programme that it was motivated to take legal action to give its customers time to update their systems.

"We sought the injunction to cause a delay, not to completely stop the publication," he said.

Mr Owen recommends that the card alone should not be relied upon for secure access to buildings.

"We do not recommend the use of Mifare Classic for new installations," said Mr Owen. "We are working with customers to review their security."

Spot check

The Mifare Classic is widely used on many public transport systems including the Oyster card in London. The researchers say their security flaw can be used to copy cards. They claim to have even been able to adjust the amount of credit stored on a pre-pay card.

Earlier this year members of Prof Jacobs's team visited London to test their findings, travelling on the London Underground using a modified Oyster card.

Shashi Verma, director of fares and ticketing at Transport For London, told the BBC its system spotted the security breach.

"We knew about it before we were informed by the students," said Mr Verma

He stressed that the Mifare Classic chip in the Oyster card is only part of a larger system. "A number of forensic controls run within the back office systems which is something that customers and these students have no ability to touch."

"We will carry on making improvements to the security of the Oyster system."

Speaking in July, 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 the researchers were the only ones that knew about weaknesses with Mifare.

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

Commenting on the publication of their research, Prof Jacobs told Click the information being disclosed was: "not a guidebook for attacks".

This report will be broadcast in this week's edition of Click on Saturday 11 October at 1130 BST on the BBC News Channel. It will also air on BBC World - check

for transmission times.

Story from BBC NEWS:
http://news.bbc.co.uk/go/pr/fr/-/2/hi/programmes/click_online/7655292.stm

Published: 2008/10/06 15:41:32 GMT