guardian.co.uk

Newly asked questions

Has London's Oyster travelcard system been cracked?

Charles Arthur
The Guardian, Thursday June 26, 2008

Yes, but it's difficult to determine how widespread the effects will be. Security researchers at Radboud University in Nijmegen, Holland, have been playing with Philips's Mifare RFID cards - used by Transport for London's contactless Oyster cards - for some time, and last week managed to crack the encryption on a card and clone it. They added credit to it and took free rides around London's Underground network.

The only equipment needed was a laptop and an RFID reader; Bart Jacobs, professor of computer security at the university and one of the team who did the work, told us it takes "a few seconds" to crack any Oyster card's encryption. "We need to eavesdrop on the communication between a card and a card reader. From that communication we can deduce secret cryptographic keys that are used to protect the contents of the card. Once we have the keys we 'own' the card and can manipulate it as we like."

How important is the flaw? "Very serious," says Jacobs. "These are things that should not be possible, not even with a single card." He was unsure how easy criminals might find it to copy his work.

Transport for London, however, is apparently unworried. "We run daily

tests for cloned or fraudulent cards and any found would be stopped within 24 hours of being discovered," it said in a statement. "The most anyone could gain from a rogue card is one day's travel."

Oyster is very important for TfL: more than 10m Oyster cards have been issued and 38m journeys are made each week using Oyster. Around 80% of all Underground and bus payments in London are now by Oyster card. The system uses an RFID (radio frequency identification) chip which activates when the card, and its chip, come close to a reader - in effect, the chip's aerial resonates to the frequency put out by the reader, and the two can swap data. Each card stores digitally encrypted information about its unique number and the amount of credit it holds. When you go through an Oyster turnstile and touch it to the reader, a digital conversation ensues which decrements the credit on your card. However, the digital conversation only applies within the station; TfL appears (judging by its response) to not have a real-time synchronisation with its central database of tickets and credit. But overnight, when the transport system is quiet, the database would spot a ticket that had acquired extra credit without a matching transaction in its favour, and ban it.

What's also unclear is how worthwhile it would be for criminals. An Oyster card costs £3 - enough for two trips in the inner Zone 1. Only those who can get hold of them virtually free could make a profit. Criminals probably have their ways. But this isn't going to lead to a collapse in Oyster's use.