Do you know what you're paying for? How contactless cards are still vulnerable to relay attack

August 3 2016, by Steven J. Murdoch

With home-made sleight-of-hand, it’s possible that the cardholder may buy more than they bargained for. Author provided

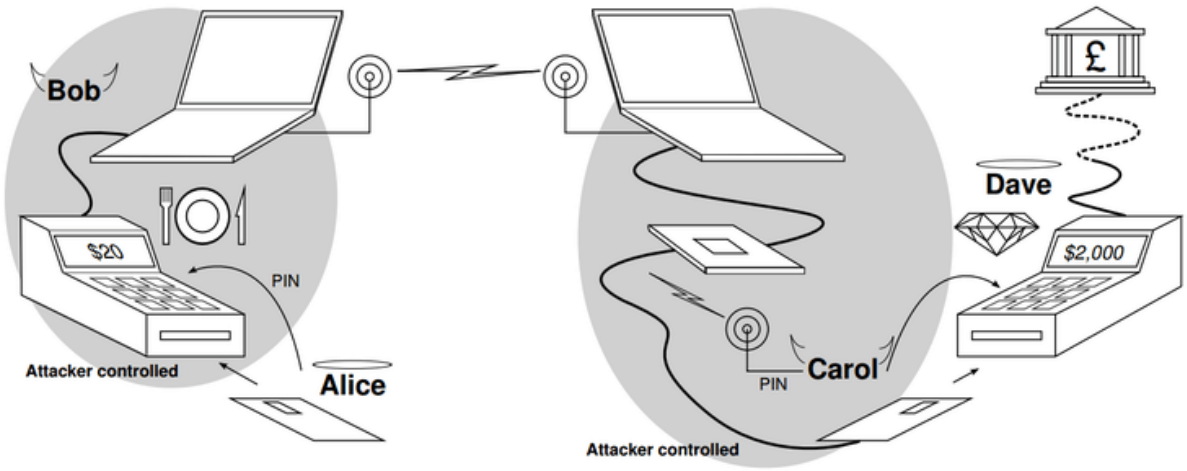
Contactless card payments are fast and convenient, but convenience comes at a price: they are vulnerable to fraud. Some of these vulnerabilities are unique to contactless payment cards, and others are shared with the Chip and PIN cards – those that must be plugged into a

card reader – upon which they're based. Both are vulnerable to what's called a relay attack. The risk for contactless cards, however, is far higher because no PIN number is required to complete the transaction. Consequently, the card payments industry has been working on ways to solve this problem.

The relay attack is also known as the "chess grandmaster attack", by analogy to the ruse in which someone who doesn't know how to play chess can beat an expert: the player simultaneously challenges two grandmasters to an online game of chess, and uses the moves chosen by the first grandmaster in the game against the second grandmaster, and vice versa. By relaying the opponents' moves between the games, the player appears to be a formidable opponent to both grandmasters, and will win (or at least force a draw) in one match.

Similarly, in a relay attack the fraudster's fake card doesn't know how to respond properly to the payment terminal because, unlike a genuine card, it doesn't contain the cryptographic key known only to the card and the bank that verifies the card is genuine. But like the fake chess grandmaster, the fraudster can relay the communication of the genuine card in place of the fake card.

For example, the victim's card (Alice, in the diagram below) would be in a fake or hacked card payment terminal (Bob) and the criminal would use the fake card (Carol) to attempt a purchase in a genuine terminal (Dave). The bank would challenge the fake card to prove its identity, this challenge is then relayed to the genuine card in the hacked terminal, and the genuine card's response is relayed back on behalf of the fake card to the bank for verification. The end result is that the terminal used for the real purchase sees the fake card as genuine, and the victim later finds an unexpected and expensive purchase on their statement.



The relay attack, where the cards and terminals can be at any distance from each other. Author provided

Demonstrating the grandmaster attack

I first demonstrated that this vulnerability was real with my colleague Saar Drimer at Cambridge, showing on television how the attack could work in Britain in 2007 and in the Netherlands in 2009.

In our scenario, the victim put their card in a fake terminal thinking they were buying a coffee when in fact their card details were relayed by a radio link to another shop, where the criminal used a fake card to buy something far more expensive. The fake terminal showed the victim only the price of a cup of coffee, but when the bank statement arrives later the victim has an unpleasant surprise.

At the time, the banking industry agreed that the vulnerability was real, but argued that as it was difficult to carry out in practice it was not a serious risk. It's true that, to avoid suspicion, the fraudulent purchase

must take place within a few tens of seconds of the victim putting their card into the fake terminal. But this restriction only applies to the Chip and PIN contact cards available at the time. The same vulnerability applies to today's contactless cards, only now the fraudster need only be physically near the victim at the time – contactless cards can communicate at a distance, even while the card is in the victim's pocket or bag.

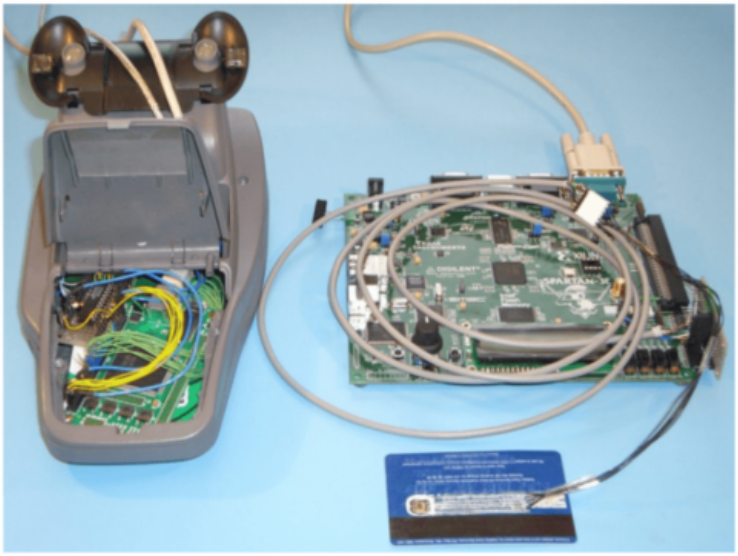
While we had to build hardware ourselves (from off-the-shelf components) to demonstrate the relay attack, today it can be carried out with any modern smartphone equipped with near-field communication chips, which can read or imitate contactless cards. All a criminal needs is two cheap smartphones and some software – which could be sold on the black market, if it is not already available. This change is likely the reason why, years after our demonstration, the industry has developed a defence against the relay attack, but only for contactless cards.

Closing the loophole

The industry's defence is based on a design that Saar and I developed at the same time that we demonstrated the vulnerability, called distance bounding. When the terminal challenges the card to prove its identity, it measures how long the card takes to respond. During a genuine transaction there should be very little delay, but a fake card will take longer to respond because it is relaying the response of the genuine card, located much further away. The terminal will notice this delay, and cancel the transaction.

We set the maximum delay to 20 nanoseconds – the time it takes a radio signal to travel six metres; this would guarantee the genuine card is no further away than this from the terminal. However, the contactless card designers made some compromises in order to be compatible with the hundreds of thousands of terminals already in use, which allows far less

precise timing. The new, updated card specification sets the maximum delay the terminal allows at two milliseconds: that's two million nanoseconds, during which a radio signal could travel 600 kilometres.



(a) With the exterior intact, the terminal's original internal circuitry was replaced by a small factor FPGA board (left); FPGA based smartcard emulator (right) connected to counterfeit card (front).

(b) Customer's view of terminal. Here, it is playing Tetris, to demonstrate that we have full control of the display and keypad.

A rigged payment terminal capable of performing the relay attack can be made from off-the-shelf components. Author provided

Clearly this doesn't offer the same guarantees as our design, but it would still represent a substantial obstacle to criminals. While it's enough time for the radio signal to travel far, it's still a very short window for the software to process the transaction. When we demonstrated the relay attack it regularly introduced delays of hundreds or even thousands of milliseconds.

It will be years before the new secure cards reach customers, and even then only some: there is only one Chip and PIN specification, but there

are seven specifications for contactless cards, and only the MasterCard variant includes this defence. It's not perfect, but it makes pragmatic compromises that should prevent smartphones being used by fraudsters as tools for the relay attack. The sort of custom-designed hardware that could still defeat this protection would require expertise and expense to build – and the banks will hope that they can stay ahead of the criminals until the arrival of whatever replaces contactless cards in the future.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation