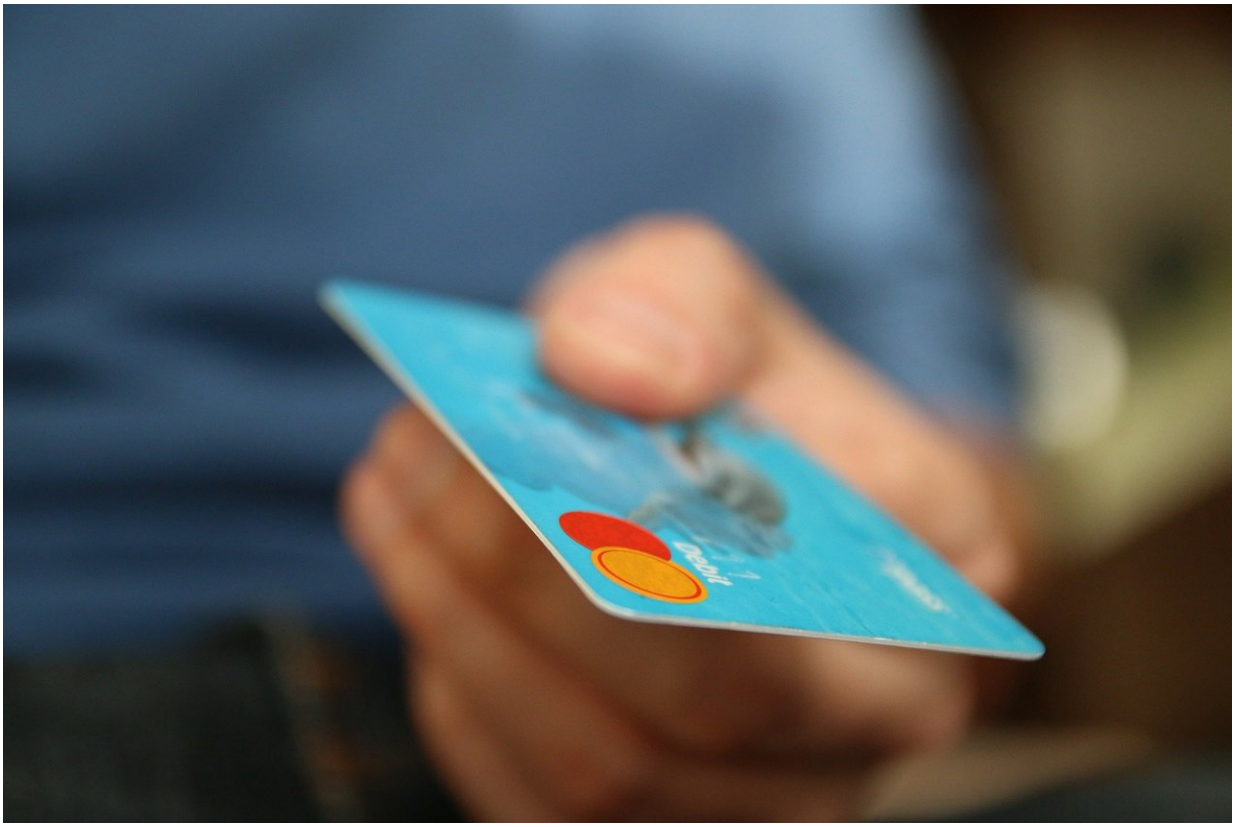
Security flaw detected for the second time in credit cards

February 23 2021, by Leo Hermann



Credit: CC0 Public Domain

After finding a vulnerability in certain credit cards for the first time last year, ETH researchers have now found a way to outsmart the PIN codes for other payment cards.

Making a contactless payment with a credit or debit card is quick and easy, and has proved particularly useful during the current pandemic. For added security, the user has to enter a PIN code above a certain amount (usually CHF 80 in Switzerland) – at least, that's the theory. As three researchers in the Information Security Group at ETH Zurich were able to show, these security measures can be bypassed with certain cards. The first time the researchers were able to document how credit cards could be used without a PIN code was in summer 2020, using Visa cards. The team have now disclosed that another bypass is possible with other types of payment cards, namely Mastercard and Maestro.

The methods used by the researchers are based on the "man-in-the-middle" principle, where attackers exploit the data exchanged between two communication partners (in this case the card and the card terminal). To replicate this effect, the researchers used an Android app they had created and two NFC-enabled mobile phones. The app falsely signaled to the card terminal that no PIN was required to authorize the payment and that the card owner's identity had been verified. Initially, the method worked only on VISA cards, as other providers use a different protocol (a protocol governs data transmission).

Security measures outsmarted in two ways

At first glance, the second idea behind bypassing the PIN code verification step appears simple: "Our method tricks the terminal into thinking that a Mastercard card is a VISA card," explains Jorge Toro, who works at the Information Security Group and is one of the authors of the research paper. Toro goes on to add that the reality was much more complex than it sounds, with two sessions having to run concurrently for it to work: the card terminal performs a VISA transaction, while the card itself performs a Mastercard transaction. The researchers used these methods on two Mastercard credit cards and two Maestro debit cards issued by four different banks.

The researchers informed Mastercard immediately after they made their discovery. They were able to confirm experimentally that the defenses put in place by Mastercard are effective. "It was both enjoyable and exciting to work with the company on this," explains Toro. Mastercard updated the relevant safeguards and asked the researchers to try to attack the payment process in the same way again, and this time it failed. The researchers will present their paper with a full overview of the method at the USENIX Security '21 symposium in August.

EMV standard as a source of error

The security flaws found in contactless payment cards are due primarily to EMV, an international protocol standard that applies to such cards. Errors in logic within this set of rules are difficult to detect, not least given that the standard is more than 2,000 pages in length. The ETH researchers emphasize on their project website that such systems must increasingly be reviewed automatically, as the process is too complex for human beings.

Provided by ETH Zurich