Outsmarting the PIN code

1 September 2020, by Felix Würsten

Credit: CC0 Public Domain

A PIN code is usually required at the checkout when paying large sums by credit card. ETH researchers have now discovered a flaw in the security system of some credit cards.

Credit cards that enable contactless payments are extremely popular. Small amounts can be charged quickly and easily at the till, and the cards are considered safe because a security code is required to debit large sums.

Most of these transactions are based on the EMV standard, which applies to over nine billion cards worldwide. The standard was developed in the 1990s by the three large companies Europay, Mastercard and Visa (hence the abbreviation EMV). Although it has been revised several times since then, the complex set of rules has several vulnerabilities that can be exploited.

The systematic search for weak spots

With other security specialists already finding errors in the standard, scientists at ETH Zurich have now reported an additional, serious security loophole. The ETH researchers will present their findings, which are currently available as a preprint, at the IEEE Symposium on Security and Privacy in 2021.

As a first step, Professor of Information Security David Basin joined with Ralf Sasse, a senior scientist in the Department of Computer Science, and Jorge Toro Pozo, a postdoc in Basin's group, to design a purpose-built model so they could take a closer look at the central elements of the EMV standard. They discovered a critical gap in a protocol used by credit card company Visa.

This vulnerability enables fraudsters to obtain funds from cards that have been lost or stolen, although the amounts are supposed to be validated by entering a PIN code. Toro puts it in a nutshell: "To all intents and purposes, the PIN code is ineffective here." Other companies, such as Mastercard, American Express and JCB, don't use the same protocol as Visa, so these cards are not affected by the security loophole. However, the flaw may also apply to the cards issued by Discover and UnionPay, which use a protocol similar to Visa's.

Simulated authorisation

The researchers were able to demonstrate that it is possible to exploit the vulnerability in practice, although it is a fairly complex process. They first developed an Android app and installed it on two NFC-enabled mobile phones. This allowed the two devices to read data from the credit card chip and exchange information with payment terminals. Incidentally, the researchers did not have to bypass any special security features in the Android operating system to install the app.

To obtain unauthorized funds from a third-party credit card, the first mobile phone is used to scan the necessary data from the credit card and transfer it to the second phone. The second phone is then used to simultaneously debit the amount at the checkout, as many cardholders do nowadays. As the app declares that the customer is the authorized user of the credit card, the vendor does not realize that the transaction is fraudulent. The

crucial factor is that the app outsmarts the card's security system. Although the amount is over the limit and requires PIN verification, no code is requested.

Successfully put to the test

Using their own credit cards at various points of sale, the researchers were able to show that the fraud scheme works. "The scam works with debit and credit cards issued in different countries in a range of currencies," Toro says. The researchers have already alerted Visa to the vulnerability, at the same time proposing a specific solution. "Three changes should be made to the protocol, which could then be installed in the payment terminals with the next software update," Toro explains. "It could be done with minimum effort. There is no need to replace the cards and all changes comply with the EMV standard."

More information: Basin et al. The EMV Standard: Break, Fix, Verify. arXiv:2006.08249 [cs.CR] arxiv.org/abs/2006.08249

Provided by ETH Zurich