Cloning chip-and-PIN cards: Brazilian job

By Alex Perekalin

Published: 2018-03-09 · Archived: 2026-04-05 14:48:00 UTC

Recently, the United States shifted from using insecure magnetic stripe in credit and debit cards to better-protected chip-and-PIN cards, which are regulated by the EMV standard. That's a big step toward increasing the security of transactions and reducing card fraud, and one might think that the end is near for the kind of card fraud that relied on cloning.

However, our researchers recently discovered that a group of cybercrooks from Brazil has developed a way to steal card data and successfully clone chip-and-PIN cards. Our experts presented their research at the Security Analyst Summit 2018, and here we will try to explain that complex work in a short post.

Jackpotting ATMs and beyond

While researching malware for ATM jackpotting used by a Brazilian group called Prilex, our researchers stumbled upon a modified version of this malware with some additional features that was used to infect point-of-service (POS) terminals and collect card data.

This malware was capable of modifying POS software to allow a third party to capture the data transmitted by a POS to a bank. That's how the crooks obtained the card data. Basically, when you pay at a local shop whose POS terminal is infected, your card data is transferred right away to the criminals.

However, having the card data is just half the battle; to steal money, they also needed to be able to clone cards, a process made more complicated by the chips and their multiple authentications.

The Prilex group developed a whole infrastructure that lets its "customers" create cloned cards — which in theory shouldn't be possible.

To learn why it's possible, you might first want to take a quick look at how EMV cards work. As for the cloning, we'll try to keep it as simple as possible.

How the chip-and-PIN standard works

The chip on the card is not just flash memory, but a tiny computer capable of running applications. When the chip is introduced into a POS terminal, a sequence of steps begins.

The first step is called *initialization*: The terminal receives basic information such as cardholder name, card expiration date, and the list of applications the card is capable of running.

Second is an optional step called *data authentication*. Here, the terminal checks if the card is authentic, a process that involves validating the card using cryptographic algorithms. It's more complicated than needs to be discussed here.

Third is another optional step called *cardholder verification*; the cardholder must provide either the PIN code or a signature (depending on how the card was programmed). This step is used to ensure that the person trying to pay with a card is actually the same person the card was issued for.

Fourth, the *transaction* happens. Note that only steps 1 and 4 are mandatory. In other words, authentication and verification can be skipped — that's where the Brazilians come in.

Carding unlimited

So, we have a card that is capable of running applications, and during its first handshake, the POS asks the card for information about the apps available to it. The number and complexity of steps needed for the transaction depend on the available applications.

The card-cloners created a Java application for cards to run. The application has two capabilities: First, it tells the POS terminal there is no need to perform data authentication. That means no cryptographic operations, sparing them the near-impossible task of obtaining the card's private cryptographic keys.

But that still leaves PIN authentication. However, there's an option in the EMV standard to choose as the entity checking if the PIN is correct…your card. Or, more precisely, an app running on your card.

You read that right: The cybercriminals' app can say a PIN is valid, no matter what PIN was entered. That means that the crook wielding the card can simply enter four random digits — and they'll always be accepted.

Card fraud as a service

The infrastructure Prilex created includes the Java applet described above, a client application called "Daphne" for writing the information on smart cards (smart card reader/writer devices and blank smart cards are inexpensive and completely legal to buy.) The same app is used for checking the amount of money that can be withdrawn from the card.

The infrastructure also includes the database with card numbers and other data. Whether the card is debit or credit doesn't matter; "Daphne" can create clones of both. The crooks sell it all as a package, mostly to other criminals in Brazil, who then create and use the cloned cards.

Conclusion

According to Aite's 2016 Global Consumer Card Fraud report, it is safe to assume that all users have been compromised. Whether you use a card with a magnetic stripe or a more secure chip-and-PIN card doesn't matter — if you have a card, its information has probably been stolen.

Now that criminals have developed a method to actually clone the cards, that starts to look like a very serious financial threat. If you want to avoid losing significant amounts of money through card fraud, we recommend you do the following:

- Keep an eye on your card's transaction history, using either mobile push or SMS notifications. If you notice suspicious spending, call your bank ASAP and block the card right away.

- Use AndroidPay or ApplePay if possible; these methods don’t disclose your card data to the POS. That’s why they can be considered more secure than inserting your card into a POS.
- Use a separate card for Internet payments, because this card is even more likely to be compromised than those you use only in brick-and-mortar stores. Don’t keep large sums of money on that card.
