RJN 17

Jul 31, 2020

By Fahmida Y. Rashid

Share

The shift from payment cards with magnetic stripes to EMV chips was supposed to stomp out card cloning, except cybercriminals appear to have figured out a workaround.

With magnetic stripe cards, it was relatively easy for criminals to collect the information and copy onto a cloned card. In contrast, the EMV chip on the payment card encrypted the card number and personally identifiable information, making it harder to steal the data and create a cloned card. The EMV technology is also designed to generate a unique encryption key for each transaction where the card is present, so even if the criminal somehow had the card information, the encryption key to validate the transaction would be missing.

However, many companies still haven't fully implemented EMV card readers, five years after the "switch" to EMV cards. That means card issuers have had to encode the card information on both the magnetic stripe and the EMV chip so that people can use the card both ways—inserting the card in to the card reader or swiping the card. This is necessary for those situations when the user is in a country that doesn't have EMV terminals, or has to use an older point-of-sale terminal.

There is a subtle difference, though, because the magnetic stripe contains the card verification value (CVV), the three-digit code that is frequently printed on the back of the card, and the chip stores the a different code called the integrated circuit card verification value (iCVV).

Cybercriminals have been creating counterfeit cards by copying the EMV details—including the iCVV—onto the magnetic stripe. Since some banks don't verify that the magnetic stripe has the CVV and that the EMV chip has the iCVV, the criminals are able to use the magnetic stripe cards containing the EMV data, said cybersecurity company Gemini Advisory.

"EMV technology may have changed the underground market for CP [card-present] records, but EMV-Bypass Cloning has opened the door for cybercriminals to sidestep the central security features of EMV chips and channel a new source of CP cards back into the underground CP market," Gemini Advisory said.

The fact that this was possible to do has been known since 2008,but the assumption was that banks would shift all their customers to using EMV cards and that magnetic stripe cards would disappear because everyone would have EMV point-of-sale terminals. The official switchover was back in 2015, and the idea was that banks would verify transactions carefully until a time when magnetic stripe cards would no longer be needed. The fact that some banks were not verifying CVV and iCVV correctly created this loophole.

It is looking very likely that this technique is already being used, Gemini Advisory said. Analysts looked at two recent incidents where criminals breached point-of-sale systems at supermarket chain Key Food Stores and liquor store Mega Package Store and captured EMV data for more than 720,000 payment cards. The magnetic stripe clones with the stolen data could be used in card-present transactions if the issuing bank doesn't properly verify the CVV.

"While analysts have not found dark web chatter highlighting EMV-Bypass Cloning or malware capable of capturing such data from EMV-enabled POS devices, the Key Food Stores and Mega Package Store breaches came from two unrelated dark web sources," Gemini Advisory said. "This indicates that the technique used to compromise this data is likely spreading across different criminal groups."

Gemini Advisory's findings comes shortly after researchers at Cyber R&D lab examined Visa and MasterCards issued by 11 banks in the United States, United Kingdom, and a few other countries in the European Union and found four cards were not properly verified. Researchers were able to make transactions using counterfeit magnetic stripe cards that were generated with data collected from EMV chip cards because those card issuers did not catch the fact that the cards were using iCVV instead of CVV.

In the past, cybercriminals typically did not target EMV data because there wasn't a clear way to monetize the information. The fact that the criminals are increasingly trying to steal EMV data suggests that is no longer the case. For example, Visa issued a warning recently that known point-of-sale malware families such as Alina, Dexter, and TinyLoader have been stealing payment card data from EMV chip-enabled point-of-sale terminals, according to Brian Krebs of KrebsonSecurity.com.

This problem can be solved. The banks need to verify which code is being used when approving payment transactions.

"A higher verification standard involving data checks would raise the threshold of access and undercut fraudulent card use," Gemini Advisory concluded. "EMV-Bypass Cloning is dangerously effective, but through policy review and higher verification standards, card providers and financial institutions can close the security gaps that this method exploits and restore the security integrity of EMV chips."

Finance Bank Security Pci Dss