Problem :

This paper identifies the security vulnerability that exists in EMV contactless credit cards, due to this vulnerability, fraudulent transactions can be collected from EMV contactless credit and debit cards without the knowledge of the cardholder, mishandling of foreign currencies, further presents a scenario in which fraudulent transactions details are transmitted over the net to an evil merchant who then uses the transaction data to take money from the victims account.

It works by allowing EMV contactless cards to approve unlimited value transactions without the cardholder’s PIN when the transaction is carried out in a foreign currency.

This attack can be operated on a large scale with multiple attackers collecting fraudulent transactions for a centralized evil merchant , an evil merchant who can be located anywhere in the world and where EMV transactions are accepted.

The flaw further identified that,

Mostly Visa credit cards will allow unlimited value transactions in a foreign currency, which helps attacker to maximize money that can be drawn from each debit / credit card.

EMV contactless interface helps attacker to perform transactions while the card is still in the cardholder’s wallet.

EMV cardholder’s PIN is not required for contactless transactions.

Visa contactless plastic money allows transactions in offline mode, and transactions can be performed without connecting card payment system , i.e avoiding validations and checks.

Merchant details are invisible and not part of data that is saved cryptographically protected by the card.

EMV authentication protocols ask plastic money to authenticate themselves to the POS , however there is not such mechanism available for POS terminals to validate their authenticity.

This paper presents two potential solutions which will mitigate this vulnerability

One attacks basically works with close synchronization between two attackers, the first will be in the close vicinity of the victims’ card whereas the second attacker will perform the purchase at POS terminal.

Chip & PIN attack helps attacker to buy items using terminals, whereas the attack discussed in this paper targets money in the victim’s bank account.

Chip and Skim attack is way of performing fraudulent transaction by creating the contactless transaction mobile app which act as skimming platform .

ATTACK

Attacker exploit this vulnerability by using Near Field Communcation enabled android devices , which can collect fraudulent transactions from unsuspecting cardholders…

Evil merchant (converting transaction into money) by sending transaction data to bank.

Collecting fraudulent transactions

A target oriented malicious app based on NFC abilities , will initiate itself to collect a transaction immediately upon detection of a contactless credit /debit card in the phone’s NFC field. It requires milliseconds from start to end of detection to completion of transaction.

App sends a request to the vulnerable card.

Target Victim Card can approve or reject.

If the card approves the transaction, it generates AC and SDAD which ensures the bank and POS terminal respectively the card which initiates the transaction is genuine.

The app is independent of internet connection and location because the app will store transaction authorization data returned by victim’s card.

When internet connectivity is maintained, the app will send stored transaction data to the evil merchant who will convert the transaction data into money.

The ability to capture fraudulent transactions offline and store them for later transmission is one of the novel features of this attack. This allows the attack to be operated on a large scale without the need for synchronization.

Internet-based listening service The rogue merchant provides an Internet-based listening service on a pre-arranged IP address and port number, to receive the fraudulent transactions from the attackers. The transactions are initially stored to be processed later, once the merchant details have been added to the transaction and the connection to the acquirer bank is available.