nomi

by S S

Submission date: 26-Sep-2023 11:34AM (UTC-0700)
Submission ID: 2147489929
File name: Week_2_Part_2.docx (19.58K)
Word count: 1074
Character count: 5795

Why do modern payment cards use a chip and not a magnetic stripe?

Modern cards use a chip often known as EMV as they are more secure as they do not transmit card real numbers; instead, they generate a unique code for every transaction and send that specific code only to the card reader. This provides more secure transactions than the magnetic stripes in which real card numbers are transmitted to the business card reader. It is also a global standardized process, making the cards simple to use locally and in international transactions. It also allows PIN verification and enhances authentication, making the payment system more secure and smooth. It also supports contactless payments, making it more convenient.

- **What are EMV Certificates, and why are they relevant for payment protection?**
- EMV certificates are the digital credentials used in Europay, Mastercard and Visa chip card technology. They are used as a standard for secure payment globally. They are relevant for payment protection due to the following reasons.
- This technology has effectively reduced card fraud by protecting cardholders and financial institutions.
- It helps to authenticate the payment terminal and chip card during a transaction, which helps to reduce counterfeit card usage.
- These certificates generate dynamic transaction-specific codes for each purchase, making it extremely difficult for fraudsters to clone cards.
- It enables secure payment encryption of payment data between the chip card and terminal, and this encryption prevents sensitive information from being intercepted and to be used for fraudulent activities.
- **What attacks exist against payment cards?**
    - **Card-not-present?**
    - **Contactless payment?**

Attacks against cards vary from case to case, primarily depending upon the type of transaction, and a few common attacks for card not present and contactless payment are listed below.

Card Not Present

Attackers use the stolen card information to make an online purchase. They get the card information through phishing or card skimming.

Brute Force Attacks

sHackers try to guess the card details, such as numbers, expiry date and CVC, to make unauthorized financial or CNP transactions.

Account Takeover

Attackers access cardholders' accounts and make CNP purchases using the login credentials accessed through unfair means.

Identity Theft

Hackers use stolen personal information, such as card details, to open a new bank account to obtain credit in the victim's name for CNP transactions.

A few of the contactless payment attacks are also listed below.

Near Field Communication (NFC) Relay Attacks

In this attack, attackers usually use the NFC relay to catch the communication between a contactless card and a payment terminal and use that information to make fraudulent transactions.

Lost or Stolen Device

If any of the contactless-enabled devices are stolen, such as contactless cards or mobile wallets, someone else can access them to use them for unauthorized transactions.

Eavesdropping

Hackers with advanced equipment can intercept wireless signals between contactless cards and payment terminals and use that data to make financial transactions.

Data Skimming

It is also similar to card skimming, in which hackers try to skim data from the cards or mobile wallets by getting close to the victim's cards or devices.

How is multi-factor authentication (MFA) used in banking

It comprises security measures that are majorly used globally in banking and financial institutions to protect customers and sensitive financial data. It adds an extra security layer to the system. Following are the ways through which they are used in banking systems.

- Whenever a user tries to access his banking details, he has to enter his username and password, which is the first authentication factor.
- Customers must provide a second-factor authentication such as a one-time password, biometrics or approval from a registered device.
- In addition to this, some banks also require some security questions.
- It is majorly required for huge transactions and initiating a transaction with a new recipient to ensure better security.

As it comprises multiple security layers, this system majorly help the user and banks to protect themselves from cyber threat.

How does multi-factor authentication increase payment security?

Multi-factor authentication increases payment security in the following ways.

- It requires time-based one-time passwords that expire quickly, reducing the risk of interception.
- Security layers such as biometrics and fingerprints add an extra hard-to-crack protection layer to the system.
- It reduces the account takeover and limits payments to authorized devices only.
- MFA is required to add a new payee and edit details, making it difficult to crack for the attackers.
- It safeguards against stolen credentials such as usernames and passwords.

What MFA methods are you using in your daily life?

I use the following Multiple Factor authentication methods in my daily life.

- 2 Factor authentication is enabled on all my financial and banking apps so that I can protect my financial information from hackers.
- Online transactions are turned off on my cards, and an OTP is received on my device whenever it turns on.
- All my email addresses and Clouds 2 FA are turned on, and no one can access them if they also have my username and password.
- All my social media accounts require a one-time password and a security question answer before accessing them on a new device.

What attacks exist against different forms of 2FA?

Time-based-one-time-password?

There are many through which 2FA could be comprised, and a few are listed below.

- One is a phishing attack in which the attacker sets a fake email or website campaign and asks the user to enter the TOTP. In this method, the second security layer becomes comprised as well.
- The second type of attack is the Man-in-the-Middle (MitM) Attack, in which an attacker intercepts the TOTP code between the communication between the server and the user and uses this to gain unauthorized access.
- In some cases, any malware or critical loggers on a user's device can capture TOPT as they enter it, compromising the second factor.
- Hackers get TOTP as the customers enter a scam website and try to predict the next TOTP if it has a predictable pattern.

Text Message?

It is receiving one one-time code via text message on the registered mobile number, and it is often considered less secure due to the following reasons.

- Attackers can convince the mobile operators to transfer the victim's phone number to a new sim card, which allows them to receive the 2FA-based codes.
- Sometimes, attackers with physical access to a user's phone through malware intercept the incoming messages and use them for fraudulent activities.
- SMS-based 2FA can be compromised through phishing attacks that trick users into revealing their codes.

nomi

ORIGINALITY REPORT

3%	3%	0%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	blogs.perficient.com Internet Source	1%
2	www.cnbc.com Internet Source	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		