IEEE | DIT UNIVERSITY
STUDENT BRANCH

CYBERDOME

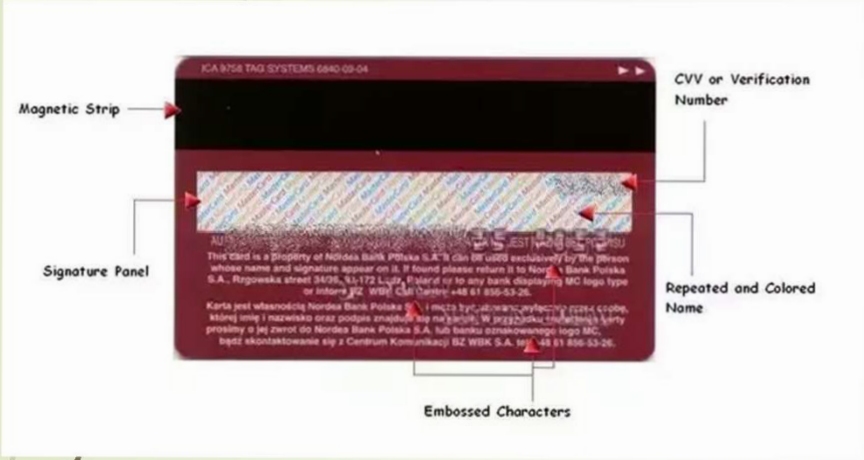
Playing With Cards

Nishchay Singh Muktawat
CSE-CSF 3rd year
Technical Head IEEE DIT University
9414974111
Linked In- /nishchay-singh-muktawat-a1358a138/
Instagram- @nishchaysm

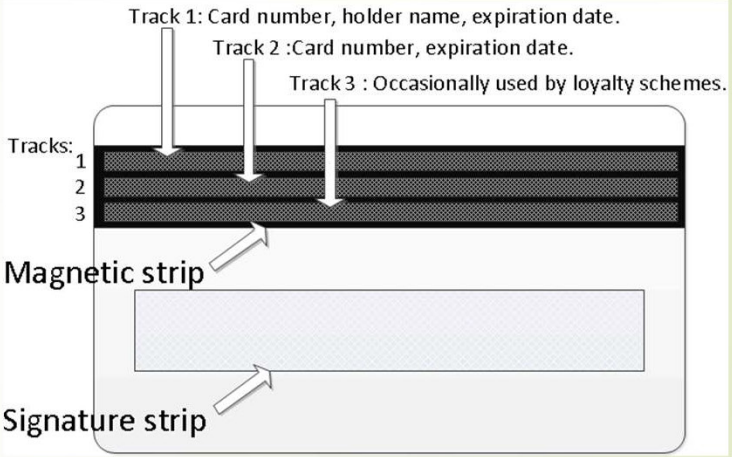
Type of Cards

- Magnetic Strip
- EMV Chip Based
- RFID

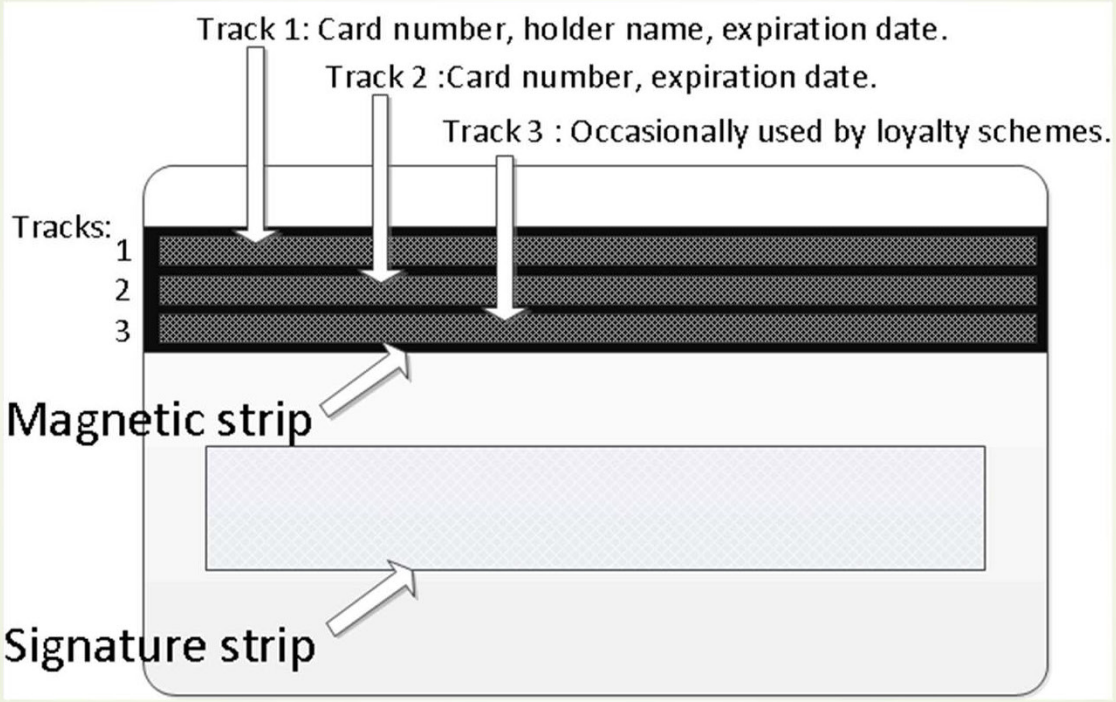
Magnetic Strip



Magnetic Strip



Point of sale (POS)


Track 1: Card number, holder name, expiration date.
Track 2 :Card number, expiration date.
Track 3 : Occasionally used by loyalty schemes.
Tracks:
1
2
3
Magnetic strip
Signature strip

EMV Chip Based

POS

RFID Cards


HANDS-FREE
PICKPOCKET

Payment Gateways and Processor

- What Is a Payment Gateway?
- What Is a Payment Processor?

- The merchant
- The customer
- The acquiring bank that provides the merchant's processing services
- The issuing bank that issued the customer's credit card or debit card

- What Is a Payment Gateway?
- What Is a Payment Processor?

PCI Compliance?

The Payment Card Industry Data Security Standard (PCI DSS) applies to companies of any size that accept credit card payments. If your company intends to accept card payment, and store, process and transmit cardholder data, you need to host your data securely with a PCI compliant hosting provider.

Goal: Building and maintaining a secure network

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.

Goal: Protect Cardholder Data

- Protect stored data.
- Encrypt transmission of cardholder data across open, public networks.

Goal: Maintain a Vulnerability Management Program.

- Use and regularly update anti-virus software.
- Develop and maintain secure systems and applications.

Goal: Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.

Goal: Implement Strong Access Control Measures

- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.

Goal: Maintain an Information Security Policy

- Maintain a policy that addresses information security.

Type of Payment gateways

- 3D secured
- 2D secured (non 3D secured)

Chargeback

- User
- Merchant
- Bank
- Payment processor

Carding

Conclusion

- Using EMV cards
- Don't give cards to any unknown or even known person
- Use only those sites that compilence with PCI-DSS
- Pay only on trusted sites
- Don't do carding
- File for chargeback as soon as you notice unusual transaction
- Don't perform transactions on open networks

Thank you

Conclusions are better than doubt…

Querries ?