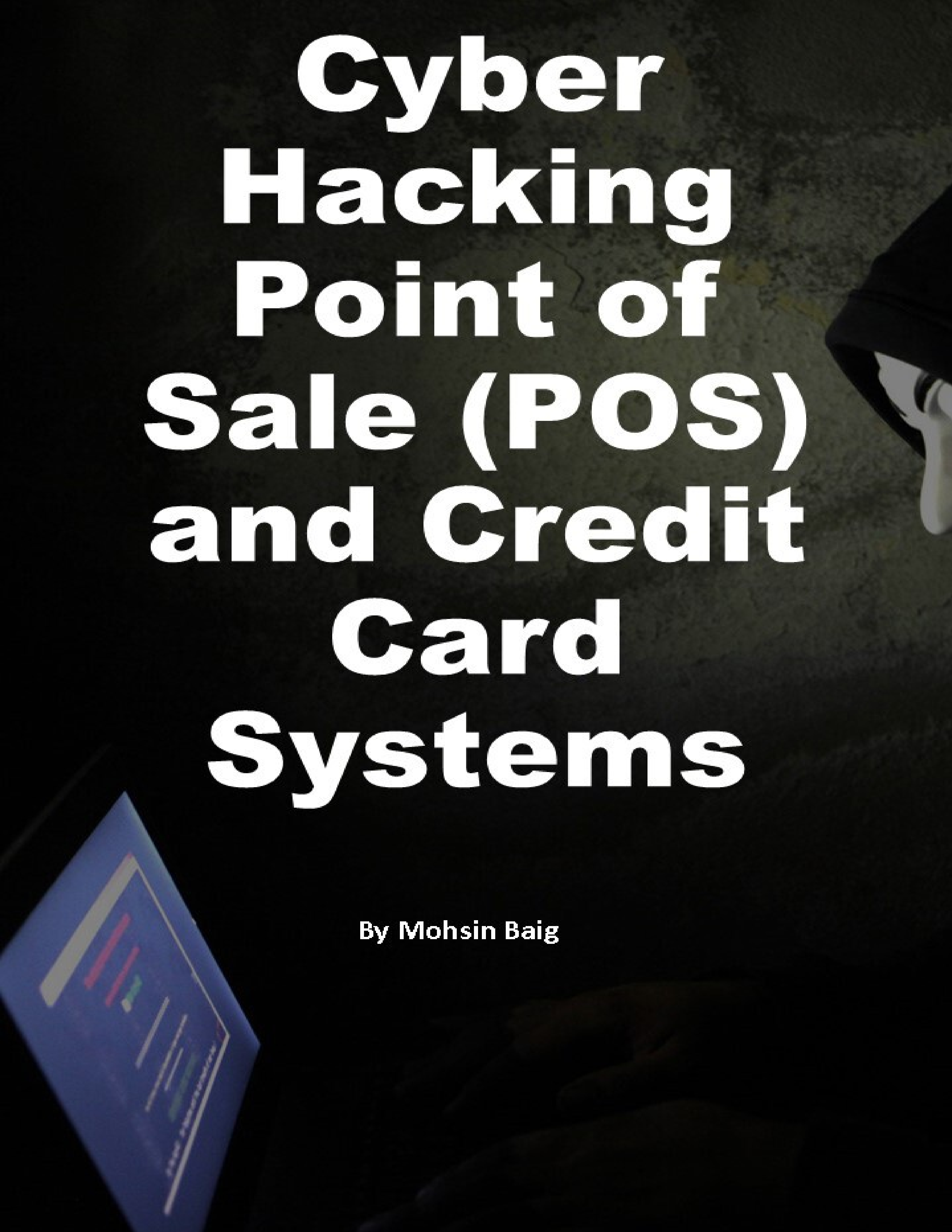


Cyber Hacking Point of Sale (POS) and Credit Card Systems

By Mohsin Baig

Cyber Hacking Point of Sale and Credit Card Payments (POS)

Author: Mohsin Baig

Our Group

Mastering Core Essentials Book series is part of the Defence Cyber School that is a Online training school based in the UK. Our mission is knowledge sharing and our objectives are to empower those who seek IT knowledge from all IT and Cyber security professional communities globally.

Book Structure

The Mastering Core Essentials books are an IT series of concise books where the books are written in a unique detailed summarised format covering all the essential elements of the relevant domain. Our books will provide you fast track knowledge and information about the relevant topics and are highly suitable for experienced IT professionals, IT Contractors and IT Consultants that perform in a project environment. Many of our books also support our Consultancy Level and Professional Training online learning courses that are available from: https://defencecyberschool.thinkific.com/

Our Professional Reader

Our books are designed for the fast track readers who want to sponge a lot of information in the shortest time possible about the relevant topics. You could be a Consultant or a Contractor or a highly experienced Business Transformation professional who has secured a new project role or consultancy assignment where you want to grasp the fundamentals and essentials of the relevant domain areas of the subject on the fly and hit the ground running.

UK Series Founder

The Mastering Core Essentials series was established in 2016 and most of our books are written by the Author: Mohsin Baig, who is a Self-Book Publisher based in the United Kingdom and also hails from an IT Professional Project Consultancy and Cyber Security Training Background.

Mohsin was born and raised in Scotland and currently resides in England. Mohsin is also the start-up founder of the UK Defence Cyber School that started in 2019: https://www.defencecyberschool.com

Global Book Distribution

Our Kindle and paperback books are available from Amazon and within the following Amazon based countries

UK, USA, France, India, Canada, Japan, Australia, Mexico, Spain, Netherlands, Italy

Online Training Courses

Our Books support Individual and Corporate Online Training courses that are delivered by the Defence Cyber School in the UK.

Currently we offer the following Professional Consulting global online training programmes to IT professionals:

1. Professional Consulting Certificate in Cyber Security and Digital Financial Services Transformation
2. Digital Transformation Consulting Certificate in Software System Architecture with Cyber Security
3. Digital Transformation Consulting Certificate in Enterprise Architecture Strategy with Cyber Security
4. Professional Consulting Certificate in Cyber Security Architecture with IT System Consultancy
5. Professional Consulting Certificate in Cyber Security Strategy with Cloud Architecture

For more information on Individual and Corporate Training visit us on : https://defencecyberschool.thinkific.com/

Global Dawah Project

The mission of the Mastering Core Essentials Book series is to spread and share professional knowledge equally amongst all global professional communities and empower IT professionals from all global backgrounds.

"My Lord! Enrich me with knowledge." (Quran, 20:114)

Contents Page

Learning Objectives

Develop deep understanding about the payment processing landscape and about the building blocks of the payment application architecture

Develop broad understanding about the payment card industry security standards

Understand about the techniques and major attack vendors used by malicious attackers to attack the point of sale systems

Develop understanding about the payment security industry standards such as PCI DSS, PA DSS, PTS and P2PE,

Learn why security fails on payment cards with regards to PAN, CVV2, Magnetic stripes, and the types of counterfeit cards produced by threat actors

Learn about the major payment application attack vectors: POS memory scraping and local network sniffing and how malicious hackers break into protected PCI protected areas

Benefit Realization

Gain detailed insight about vulnerability areas such as data at rest, data in transit and application code and configuration and the associated PCI requirements.

Understand cryptographic standards and cryptography in payment applications with regards to symmetric encryption, algorithms, asymmetric encryption, public key encryption,

Learn how to protect cardholder data through technologies such as .NET Securestring class, implementing SSL, certificate authority, installing root certificates, client certificate, implementing encrypted tunnels, secure key management, KEK and DEK, point to point encryption, EMV,

Learn the fundamentals of securing application code during all stages of the application life cycle.

Chapter 1: Introduction to Credit Cards

1.1 Introduction – Payment Cards

The following are the main types of cards which exist that can be used for payments:

- Credit card
- Debit cards (ATMs)
- Gift cards
- Fleet (proprietary) card

1.2 Card Entry Methods

- Main methods of entering card data into POS to execute payment transaction is by the following: swipe and manual entry.

1.3 Magnetic Stripe Reader

- Magnetic Stripe Reader (MSR) device that reads magnetic strip on cards.
- MSR devices possess encryption capabilities and can be used in point to point encryption (P2PE).
- Card data entered in MSR is via physical swiping the card.
- Customer also has option of manually entering account number and expiration date details if magnetic stripe is damaged.
- Some MSR devices very similar to a keyboard input.
- Threat Actors can steal card data by installing a keystroke logger on MSR devices.

1.4 Pin-pad

- Built with MSR, sophisticated device that enables custom protection of all sensitive card data.
- Also maintain hardware encryption capabilities implemented as TRSM (Tamper- Resistant Security Module.)

1.5
Key Players – Payment Processing Landscape

- Consumers
- Merchants
- Acquirers
- Issuers
- Card Brands
- Gateways
- Processors
- Software Vendors
- Hardware Manufactures

1.6 Consumers

- Customers who use debit cards and credit cards to make payments in store when purchasing goods or services.

1.7 Merchants

- Merchants such as Hotels, Supermarkets, Retail stores etc. maintain decisions such as what cards to accept, such as credit or debit or both, and which bank to hold a merchant account with.

- Maintain POS, Payment Hardware and Software that will process the card information and send it to the payment processor in order to receive funds into their merchant account.
- Maintain security policy and processes how to protect customer card data.

1.8 Acquirer

- Authorize payment transactions and settles them with the card issuers.
- Payment processors route all transactions based on card type to corresponding acquirer for authorization and settlement.
- Regulate the merchant discount rates (fees merchant pays every payment transaction processed).

1.9 Issuer

- Issuer banks maintain customer accounts and give cards to customers
- Bill customers for the transactions
- Send money to the acquirers so that the merchants can be paid
- Develop the card maintain responsibility of physical security

features on the card

1.10 Card Brands

- Facilitate end to end process payment authorization and settlement.
- Connectivity between acquirers and issues is maintained by networks such as Visa net.
- Some Brands such as Visa, Mastercard etc do not directly participate in the roles of acquiring, issuing, but instead outsource the functions to third parties.
- Brands such as American Express participate directly undertake the roe of issuing cards and acquire payment transactions.
- PCI Security Standards Council (PCI SSC) creates and maintains security standards for merchants, found by various card brands.

1.11 Payment Processor

- Manages payment between merchant and multiple acquirers
- Maintain merchant accounts which receive money for goods and services purchased by cardholders
- Perform the role of routing payment transactions to the relevant issuer based on payment and card brand type such as credit, debit cards issued by visa, Mastercard etc.
- Publish financial transaction reports for merchants

- Not limited to debit and credit cards also process gift cards, fleet cards, Electronic Benefit Transfers (EBTs)

1.12 Payment Gateway

- Known as "Man in the middle" and reside between the merchant and payment processor
- Main role is the provision of routing services to merchants but could also provide additional services such as point to point encryption, centralized reporting, POI Device Management, tokenization etc.

1.13 Payment Software Vendors

- Develop POS and payment applications for merchants.
- Payment applications perform the role of processing, transmitting and storing sensitive card data during the payment lifecycle.
- Merchants depend on third party software to protect cardholder data, though merchants are the main target of hacker attackers.

- Payment applications must conform to PCI PA-DSS (Payment Application Data Security Standard).

1.14 Hardware Manufacturing

- Develop the devices such as MSR, Pin pads etc. essential for payment processing.
- Devices transmit, process and store sensitive data and must be compliant to PCI PIN Transaction Security (PTS) compliant.

Chapter 2
Card Payment Application Architecture

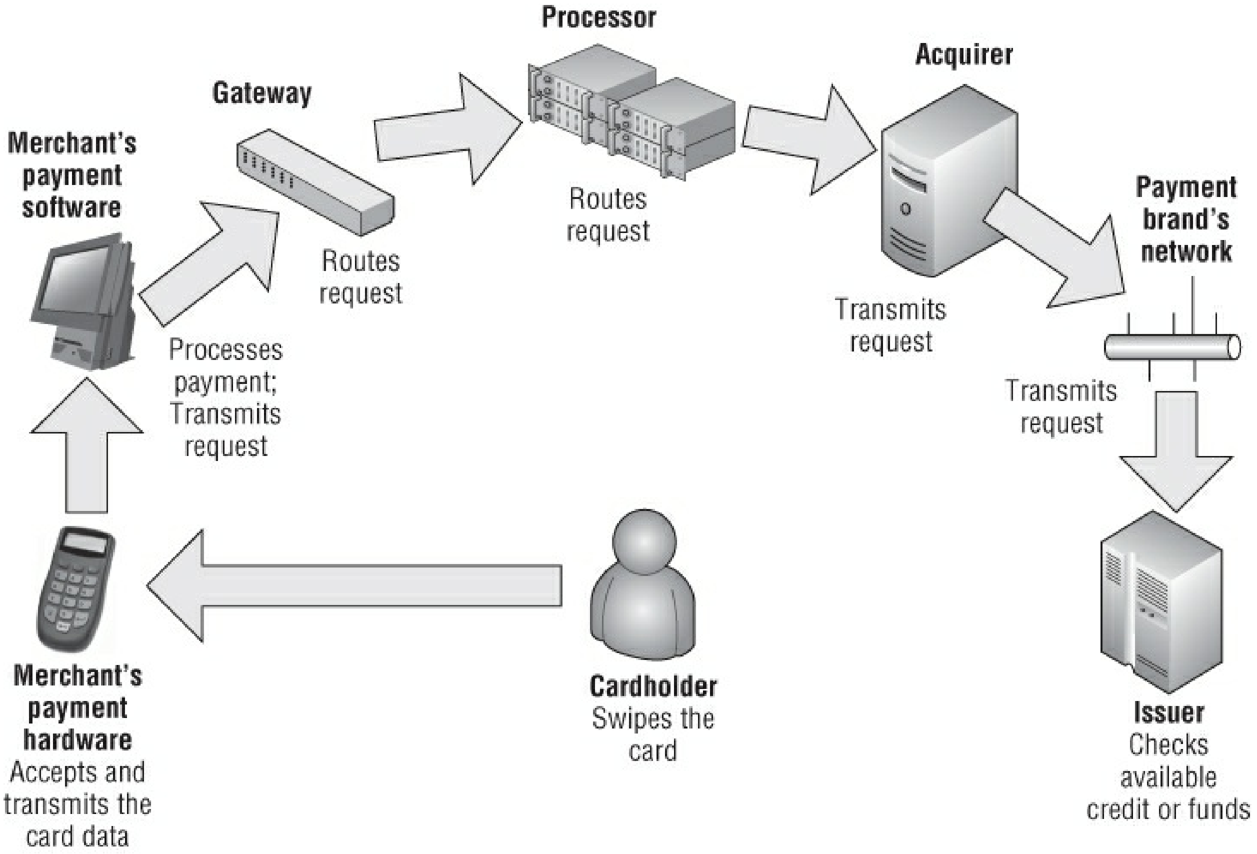
2.1 POS Payment Stages

- Payment processing comprises of the Authorization and Settlement phases.

2.1 Authorization Stage

- In the authorization phase it is essential to validate and ensure that the customer has enough credit or funds in their bank account to pay for the purchase.
- Authorization stage is most important from a data security viewpoint since all sensitive authentication data from the POS to the acquirer.
- Threat actors pursue most attacks on card data in the authorization stage.

Example of Authorization flow


Processor
Gateway
Acquirer
Merchant's payment software
Routes request
Routes request
Payment brand's network
Transmits request
Processes payment; Transmits request
Transmits request
Merchant's payment hardware
Accepts and transmits the card data
Cardholder
Swipes the card
Issuer
Checks available credit or funds

Analysis of Example: Authorization flow

- Customer selects payment of method as credit or debit or gift or EBT card.
- Customer swipes the card in the card reader in MSR or POI device
- Payment application performs validation of the card data and initiates payment transaction based on card type and Bank Identification Number (BIN) range.
- Payment transaction routes via payment gateway or via payment processor
- Transaction data is routed to the relevant acquirer which then is communicated to the issuer to gain authorization.

Notes:

- If the payment transaction is based on a credit transaction, the issuer will perform validation to ensure customer has enough credit to pay the transaction amount.

- If sufficient credit is available, the issuer will send approval message to the acquirer who further sends it to the payment processor who sends approval to the POS device.

- In the event of a debit card, the issuer will perform validation with the customer bank account to ensure that customer has enough funds in their account.

2.2 Settlement Phase

- After authorization is obtained via the POS system, the payment must be settled.

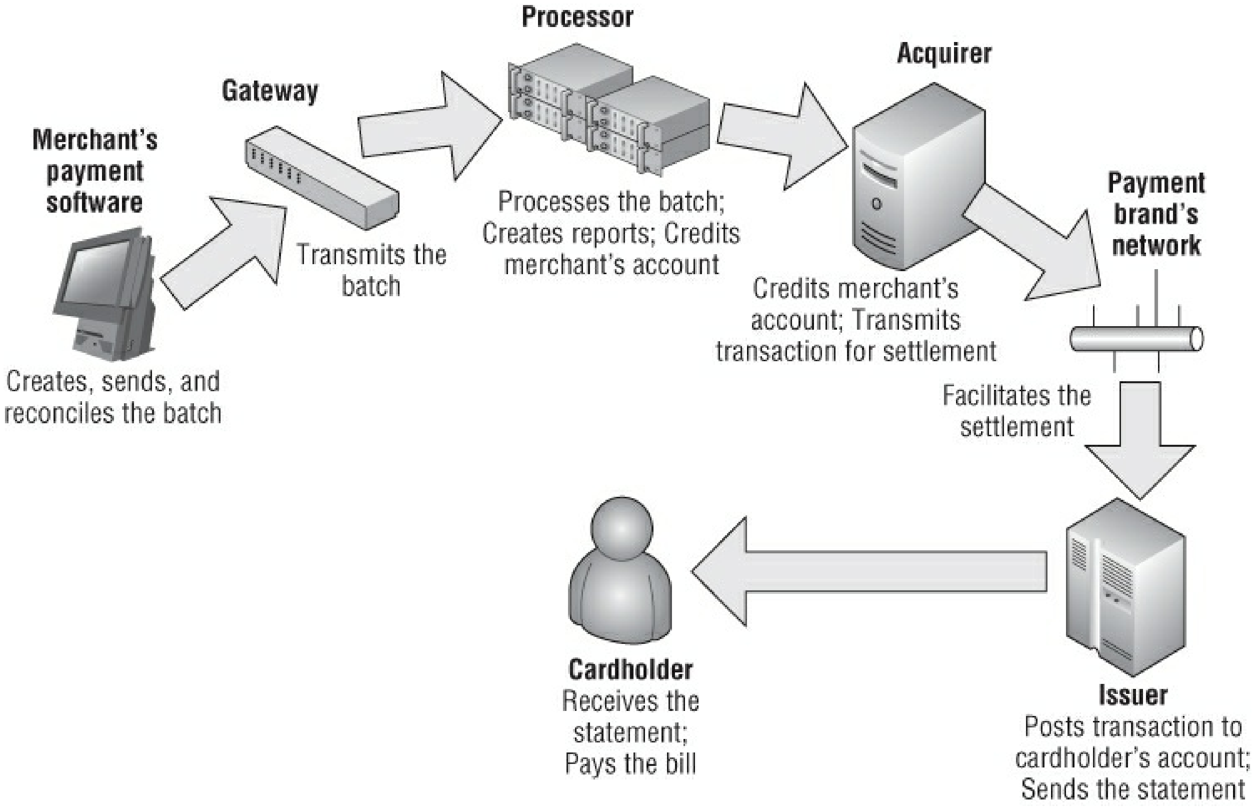
- Payment is reconciled between the merchant, its acquirer and the issuer.

- Settlement phase is less vulnerable than the authorization phase for attacks since it doesn ’ t entail sensitive authentication data.

- Settlement phase comprises of the Primary Account Number (PAN) which refers to the multiple transaction held in batches is vulnerable to attack by threat actors.

- All authorization data is destroyed by POS as soon as it is received.

Example of Settlement Flow


Merchant's payment software
Creates, sends, and reconciles the batch
Gateway
Transmits the batch
Processor
Processes the batch; Creates reports; Credits merchant's account
Acquirer
Credits merchant's account; Transmits transaction for settlement
Payment brand's network
Facilitates the settlement
Issuer
Posts transaction to cardholder's account; Sends the statement
Cardholder
Receives the statement; Pays the bill

Analysis of Settlement Flow Example

- Merchant sends transaction data to the processor who further sends it to the acquirer.
- Acquirer or Processor credits the merchant account and forwards data to the issuer who publishes the transaction to the customer account.

2.4 Payment Transactions

- Comprises of authorization amount and transaction amount
- Acquirer sends approval to merchant to charge cardholder the authorized amount.
- Once payment is made merchant sends acquirer the transaction amount which equals the authorized amount.

2.5 Void and Return

- If a cardholder wants to return goods, the merchant can initiate a return or void transaction.
- The return transaction is only initiated if the cardholder seeks a partial refund for returned goods and not for the entire payment amount.
- Threat actors are more likely to attack the return transaction process as they could route the funds from the merchant account.
- Sensitive data is not contained in the void transaction process

2.6 Fallback Processing

- Also referred as Stand-In, or Store & Forward, or Offline Authorization

- Enables Merchants to accept card payments during offline network connectivity when payment host are down.

- Permits internal approval of transactions by backup host if acquirer online authorization cannot be obtained due to network connectivity.

- Offline internal approval can take longer due to waiting time for "response timeout" protocol defined by the payment processor.

- Sensitive cardholder data is stored on POS disk for the duration of the network outrage that can be exploited by threat actors.

2.7 Timeout Reversals

- Prevents duplicate charges

- Sensitive authentication information is stored locally in the POS device that can be exploited by threat actors

2.8 Special Transaction Types

Comprise of the following POS transaction types:

- Balance Enquiry to verify remaining balance
- Recharges add funds to a gift card using different payment method

2.9 Payment Application Vulnerabilities

- Methods known as Attack Vectors can be employed by threat actors to attack a POS system in order to elicit authenticated card data

- Attack vectors can be used by threat actors in order to gain illicit access to network or severs to deliver a payload or malicious outcomes.

- Attack vectors typically entail viruses, e-mail attachments, web pages, pop-up windows, instant messages.

- Most common payloads in financial services are trojan horses, worms and spyware.

Payment data in the payment application is vulnerable in the following states:

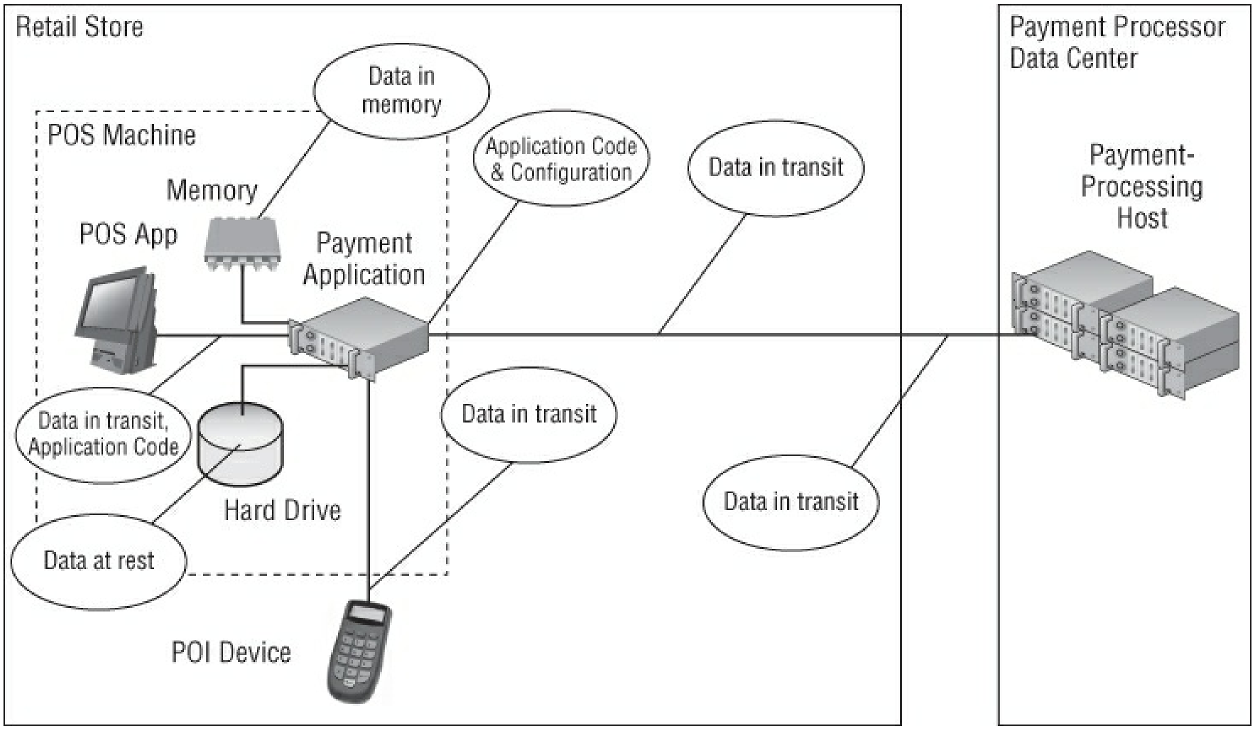
- **Data in Memory**: data maintained in the RAM of the POS machine that is utilized in various manipulations integral for payment authorization or settlement.

- **Data at Rest: Stored in** the hard drive of the POS machine on a temporary basis

- **Data in Transit**: data sent and received to third party applications and devices

- Application code and config can also be baselined as a vulnerability area since threat actors are able to tamper with them in order to gain access towards other vulnerability areas.

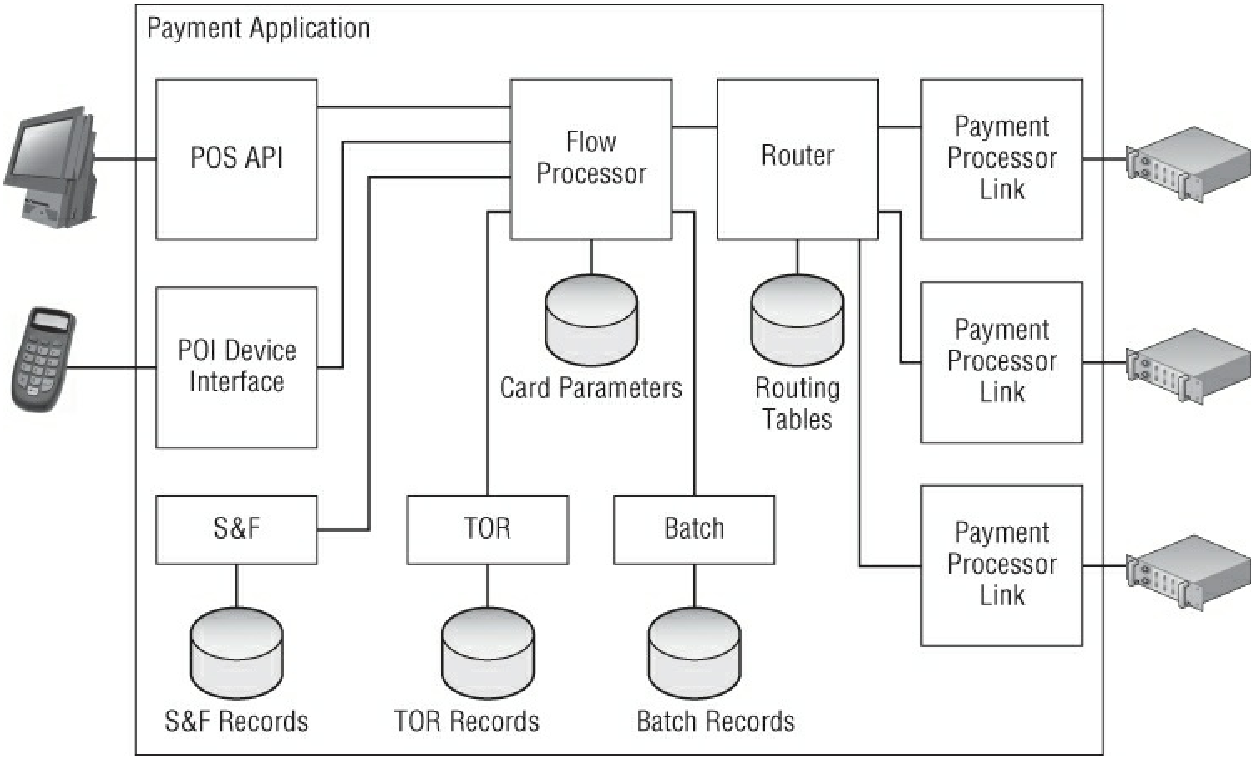
Example of Key Vulnerability Areas



2.10 Payment Application Architecture

- Design principles for the payment landscape typically comprise of external interfaces and modules irrespectively of the vendor

Example of building blocks in payment architecture



2.11Interfaces

Three types of external interfaces which enable connectivity of payment applications with devices and applications:

- POI device interface
- POS API
- Payment processor link

2.12 POI Device Interface

- Perform the role of exchanging data with the pin pad and or MSR devices

- Though message protocols vary due to different vendors type often communication is based on serial (COM) or via TCP/IP/LAN
- Modern interfaces incorporate encryption methods such as Secure Socket Layer (SSL), data payload encryption and authentication with certificates.
- Default communication of sensitive data within POI devices don ’ t have encryption methods and are vulnerable to eavesdropping.

2.13 POS API

- Performs communication responsibility with POS application to manage all payment transactions
- Communication can be done via TCP/IP or HTTP largely dependent on the application design of POS and PA
- Lack of standard security mechanism

2.14 Payment Processor Link

- Converts application transaction format to the appropriate format which conforms to the payment processor message protocol.
- Delivers communication with authorization host based on a communication protocol largely supported by the payment processor
- Hardcoded to communicate with a processor

2.15 Processing Modules

- Triggers the payment process from the step when cardholder swipes the card to the step to the process when merchant bank paid, and the customer account debited.

- Process modules comprise of the following:

1) Router
2) S& F (Store and Forward)
3) TOR
4) Batch

2.16 Router

- Routes the payment transaction for authorization, completion, or settlement to the relevant payment processor link underpinned by the card BIN range, card type, transaction type

- Payment application (PA) can typically have a design where more than one payment processor link is deployed various levels such as the POS, Store, data center switch

- Routing tables are used by the router which enable the router to route based on PAN range records to the relevant to the payment processor link.

Example of PAN Routing Table

PAN From	**PAN To**	**Link ID**

9000000000000000	4999999999999989	BOA
540000000000000	349999999999999	AMEX
370000000000000	979999999999999	AMEX

2.17
S & F: Store and Forward

- Module exercises a critical *fallback process* that permits merchants to support business continuity by the uninterrupted acceptance of electronic payments.

- Generates offline approval and stores transactional data in the S & F database.

- Stored transactional data is sent to relevant host when networks become available and is online or sent as batch to the host

- Security vulnerability exists when transactional data is stored on POS and can be exploited by threat actors.

- PCI DSS and PA DSS standards stipulates sensitive data must not be stored after authorization.

2.18
TOR: Timeout Reversal

- Error control mechanism which performs the role of ensuring duplicate charges are not imposed on the cardholder account.

- Duplicate charges typically occur when an authorization timeout response isn't received from the host, but the transaction is not only recoded but approved by the processor.

- Timeout reversal message is generated by payment application instructing the host to cancel the transaction if it was approved or not.

- In the event the network is down, and the TOR module is unable to communicate with the host all TOR messages and maintained in the TOR database and sends them to the server when the network becomes available again.
- Security concerns are about the sensitive authentication data storage

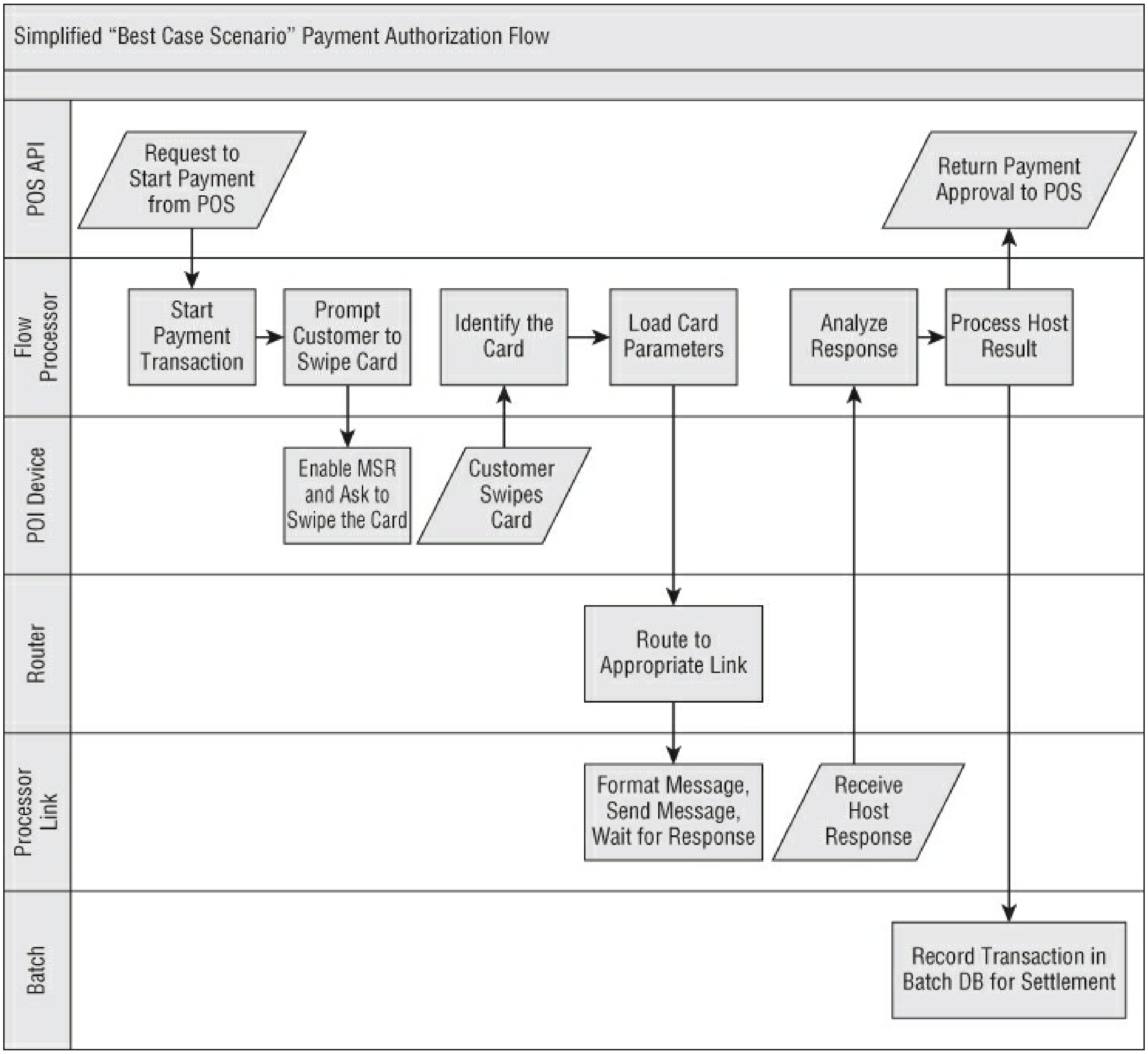
2.19 BATCH

- Also known as Close Batch, Close Shift, End of Day, or Settlement Module.
- Functionally performs responsibilities for the recording and settlement of all payment transactions processed in a specific period.

2.20 Data Storage: Data at rest

- Data at rest is used to describe any form of hard drive storage such as database, flat data file or log file.
- No standards or standard approach exist for payment application data storage with regards to encryption schemes.
- Using multiple data storage technologies may require the use of different cryptographic protection mechanisms, which increases application vulnerability.

Example of Payment Transaction Flow


Simplified "Best Case Scenario" Payment Authorization Flow
POS API
Flow Processor
POI Device
Router
Processor Link
Batch
Request to Start Payment from POS
Return Payment Approval to POS
Start Payment Transaction
Prompt Customer to Swipe Card
Identify the Card
Load Card Parameters
Analyze Response
Process Host Result
Enable MSR and Ask to Swipe the Card
Customer Swipes Card
Route to Appropriate Link
Format Message, Send Message, Wait for Response
Receive Host Response
Record Transaction in Batch DB for Settlement

2.21 Communication Between Modules

- Modules are vulnerable to sniffing and tampering by threat actors if they reside in different PCs and have their own unique APIs.

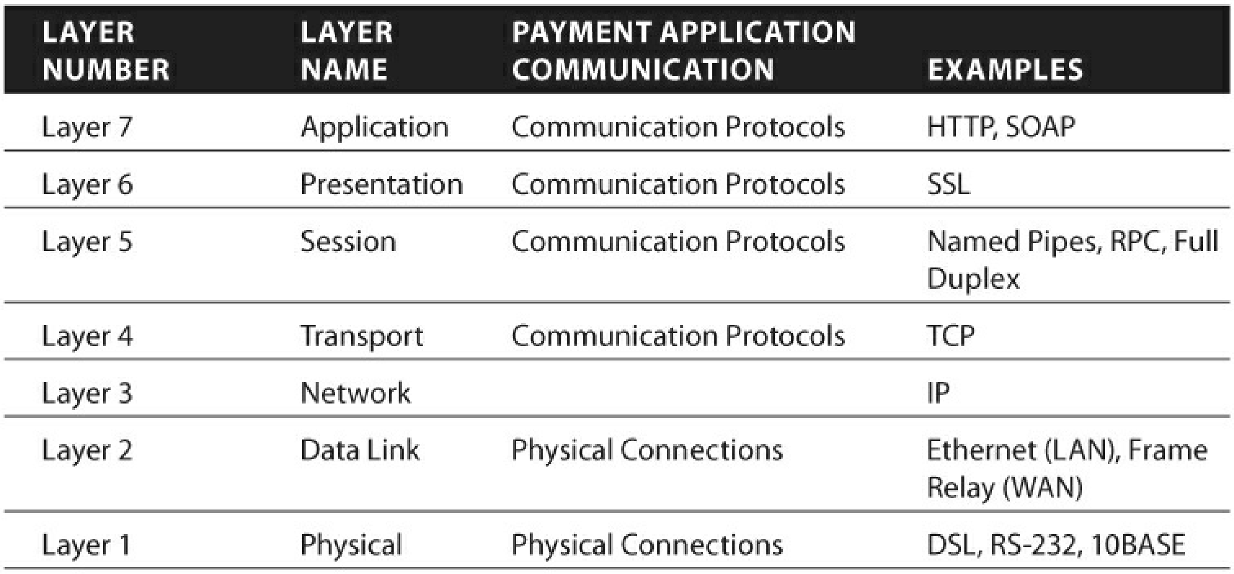
2.22
Communication Protocols

- Message exchange between sender and receiver is established via communication protocols that reside in the high level of the Open System Interconnect (OSI) stack.

- Payment application implementing the communication protocol maintains the function role of establishing the connection, ensuring error control and message bits from the sender to the recipient are sent.

- High level communication protocols can implement numerous OSI stack levels.

Example of Payment Application Communication and OSI Stack



LAYER NUMBER	LAYER NAME	PAYMENT APPLICATION COMMUNICATION	EXAMPLES
Layer 7	Application	Communication Protocols	HTTP, SOAP
Layer 6	Presentation	Communication Protocols	SSL
Layer 5	Session	Communication Protocols	Named Pipes, RPC, Full Duplex
Layer 4	Transport	Communication Protocols	TCP
Layer 3	Network		IP
Layer 2	Data Link	Physical Connections	Ethernet (LAN), Frame Relay (WAN)
Layer 1	Physical	Physical Connections	DSL, RS-232, 10BASE

2.23
Local Communication

- Communication protocols such as DLL API or Windows COM are implemented by internal interfaces and POS APIs

- DLL APIs and In-Process COM calls are used if both client (for example, POS application) and server (EPS) are running under the same OS process (in the same *address space*).

- Out-of-Process COM can be used for communication between different processes when the POS and EPS (or two internal PA modules) are separate executable applications.

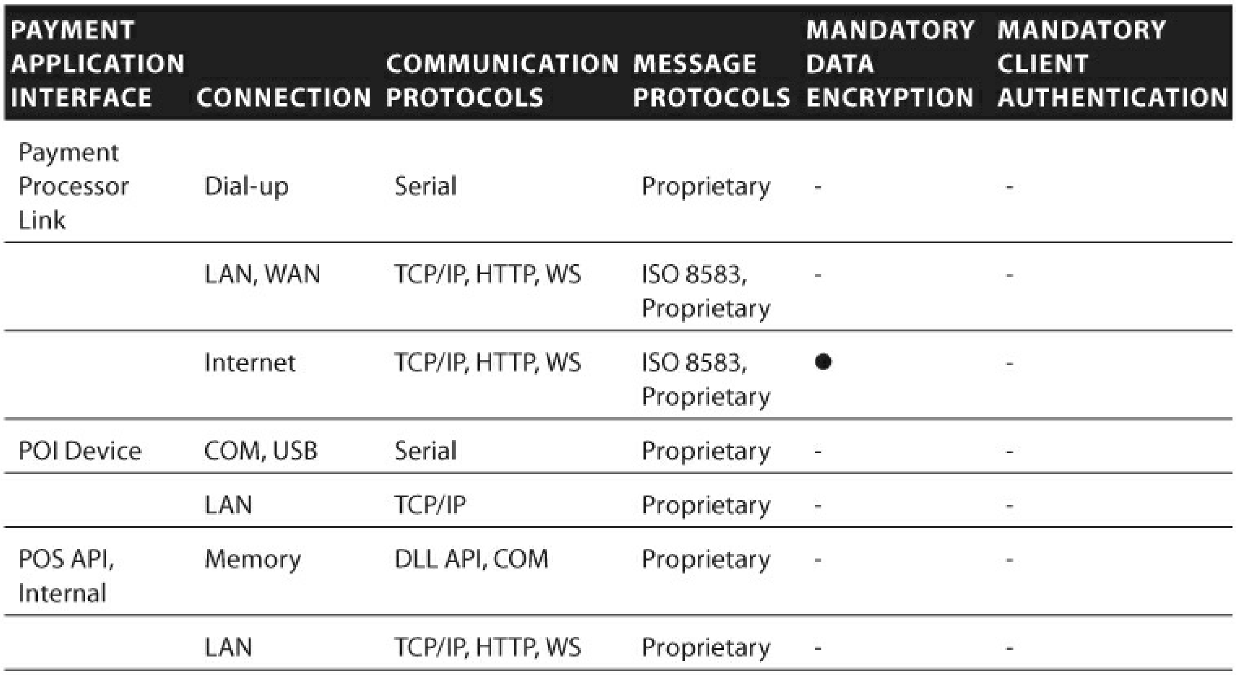
2.24
Message and Communication Protocols

- Payment application communication comprises of message and communication protocols which are uniquely different types of protocols from a security viewpoint.

- *Message protocols* work on the application software level above the OSI stack.

- Message protocols provide the following functions: Conversion of message format which can be understood by other communication channels.

Example of different types of PA interfaces using different types of connectivity, communication and message protocols



PAYMENT APPLICATION INTERFACE	CONNECTION	COMMUNICATION PROTOCOLS	MESSAGE PROTOCOLS	MANDATORY DATA ENCRYPTION	MANDATORY CLIENT AUTHENTICATION
Payment Processor Link	Dial-up	Serial	Proprietary	-	-
	LAN, WAN	TCP/IP, HTTP, WS	ISO 8583, Proprietary	-	-
	Internet	TCP/IP, HTTP, WS	ISO 8583, Proprietary	●	-
POI Device	COM, USB	Serial	Proprietary	-	-
	LAN	TCP/IP	Proprietary	-	-
POS API, Internal	Memory	DLL API, COM	Proprietary	-	-
	LAN	TCP/IP, HTTP, WS	Proprietary	-	-

2.25 Deployment of Payment Applications

- Prominent payment application deployment models comprise of the following:

1) Store EPS
2) POS EPS
3) Hybrid Store/POS

2.26 Store EPS Deployment Model

- EPS stands for Electronic Payment Systems

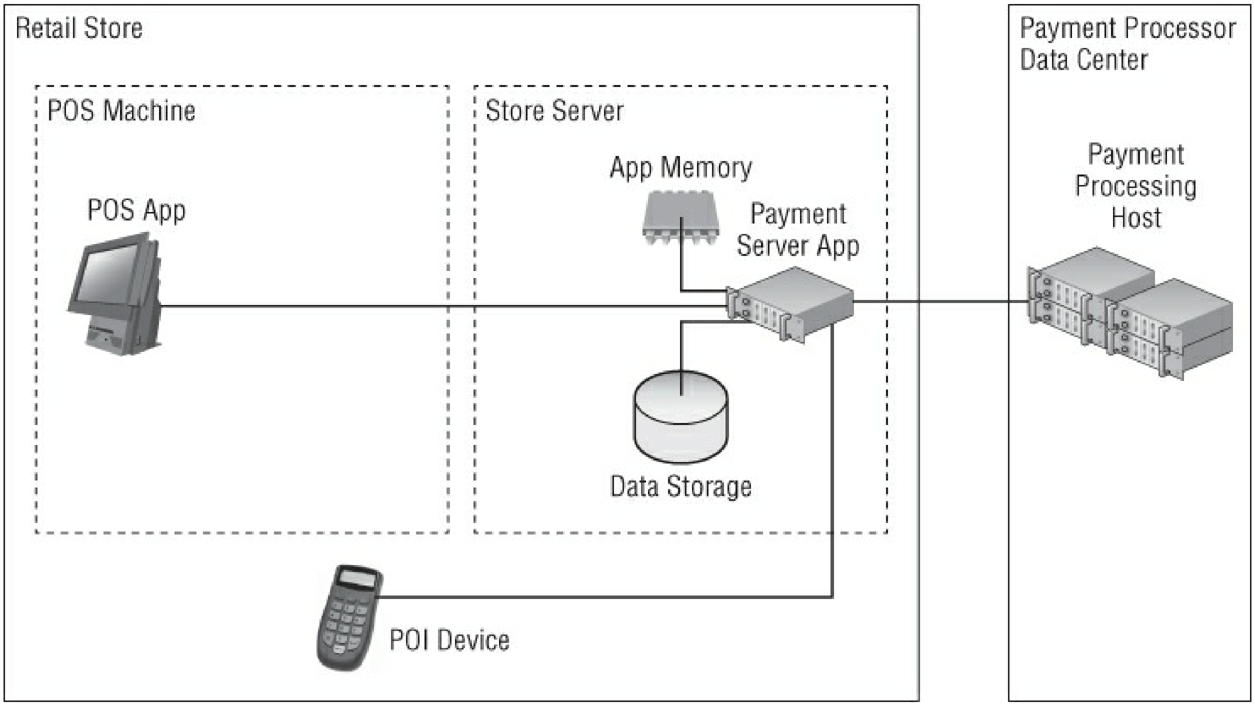
- Payment processing is performed by EPS in a central location at the store server

- EPS in this architecture design maintains all forms of communication with all POS and POI devices.

- EPS maintains diverse responsibilities from card entry flow, to processing payment transactions

- No card sensitive data is transferred between the POS and the EPS.
- Encryption isn't required since the POS machine and store server doesn't contain sensitive data.

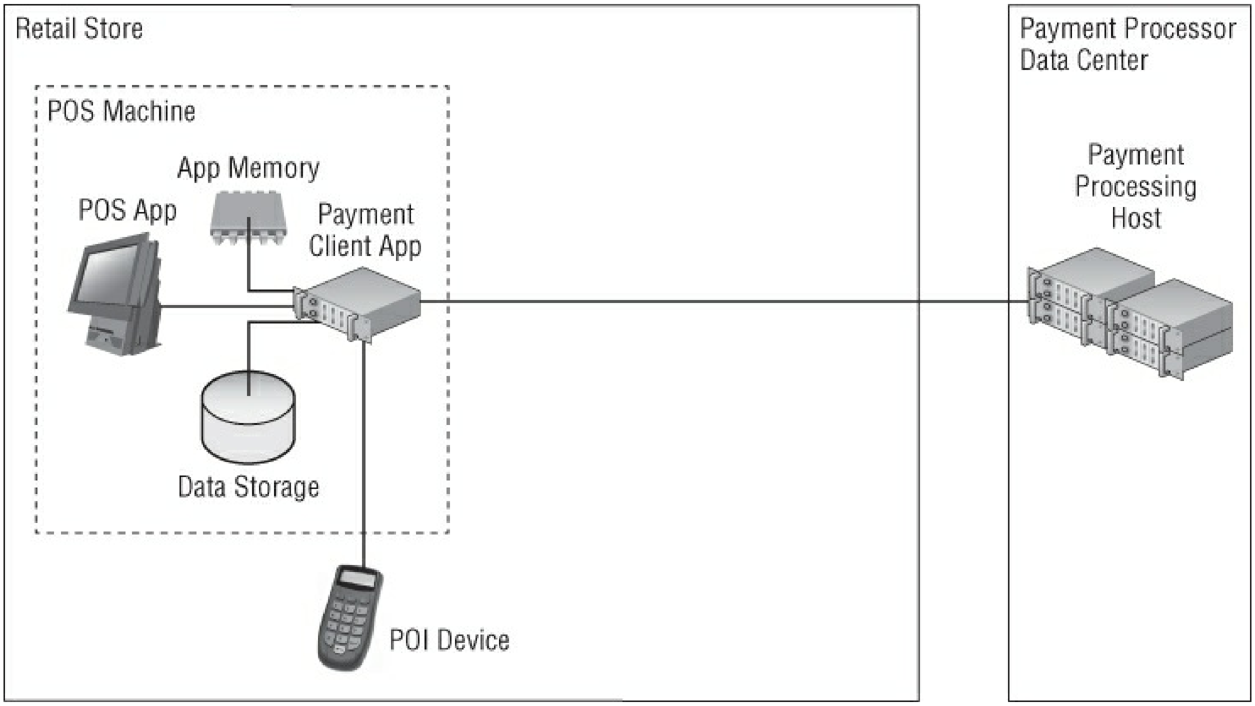
Example of Store EPS Deployment Model



2.27
POS EPS Deployment Model

- Payment processing conducted by an EPS is located at each POS machine.
- EPS maintains direct communication with POS and POI devices exercises responsibilities from card entry flow to processing payment applications.
- No sensitive data is exchanged between the POS and the EPS
- EPS maintains a direct connection with the payment processor switch resided outside the store.
- In the security viewpoint all POS Machines (memory, data storage) within the store are highly exposed to sensitive data as well as communication between the POS machine and the payment host.

Example of POS EPS Deployment Model

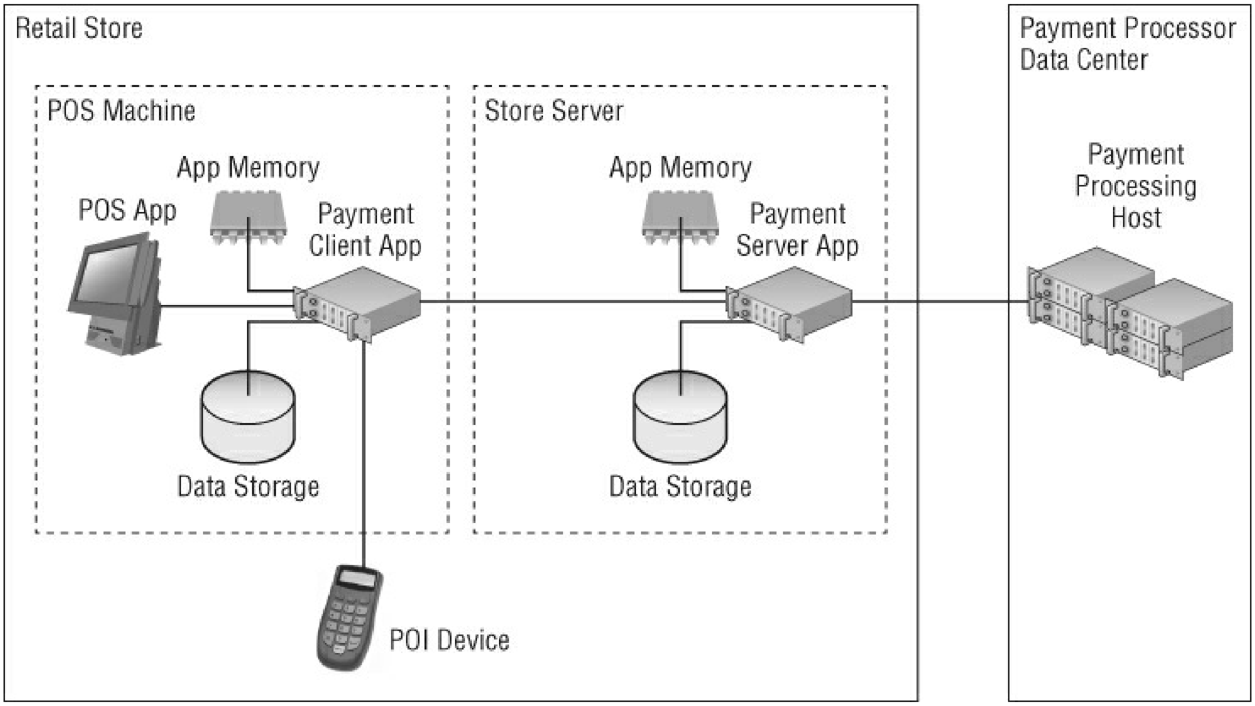


2.28
Hybrid POS/Store Deployment Model

- Most vulnerable design solution due to the PA modules are deployed across the different physical machines.
- Initial payment processing is implemented at the POS machine, which also establishes communication with the server module at the store level.
- Links to the payment switch or processors are implemented from the store server.

- In the security viewpoint both the POS and store server machines and all components -memory, data, application code and communication lines are all vulnerable.

Example of Hybrid POS /Store Deployment Model



2.29 Mobile Payments

- Many payment processors, payment software vendors, cellular communication providers, banks, payment brands, startup companies, Internet search engines etc. are competing to become the industry standard for mobile payments.

- Two main types of mobile payment technology

1) Near Field Communication (NFC)
2) Anything else

2.30
Near Field Communication (NFC)

- Enables electronic devices to exchange information using high frequency (13.56MHZ) radio communication.

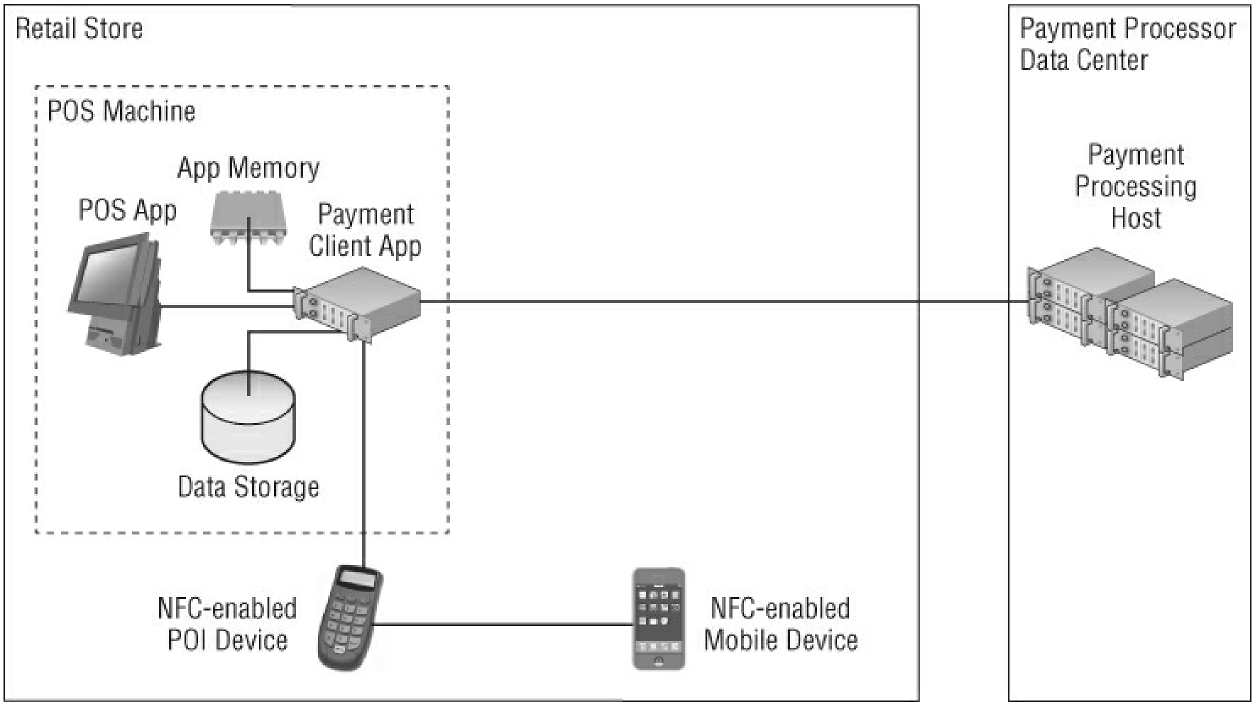
- Cohort of diverse protocols and standards; - implemented by a wide array of applications such as proximity cards, NFC tags, mobile payments (google wallet) etc.

- Potential for attacks increase when sensitive data is transmitted from the mobile to the POI device to implement payment transaction.

- Payment card authentication data (the content of plastic cards' magnetic stripes) can either be stored on the mobile device or downloaded from the cloud

- NFC-based applications are potentially more vulnerable because they store and/or transmit sensitive cardholder data.

Example of architecture and deployment of an NFC based payment solution



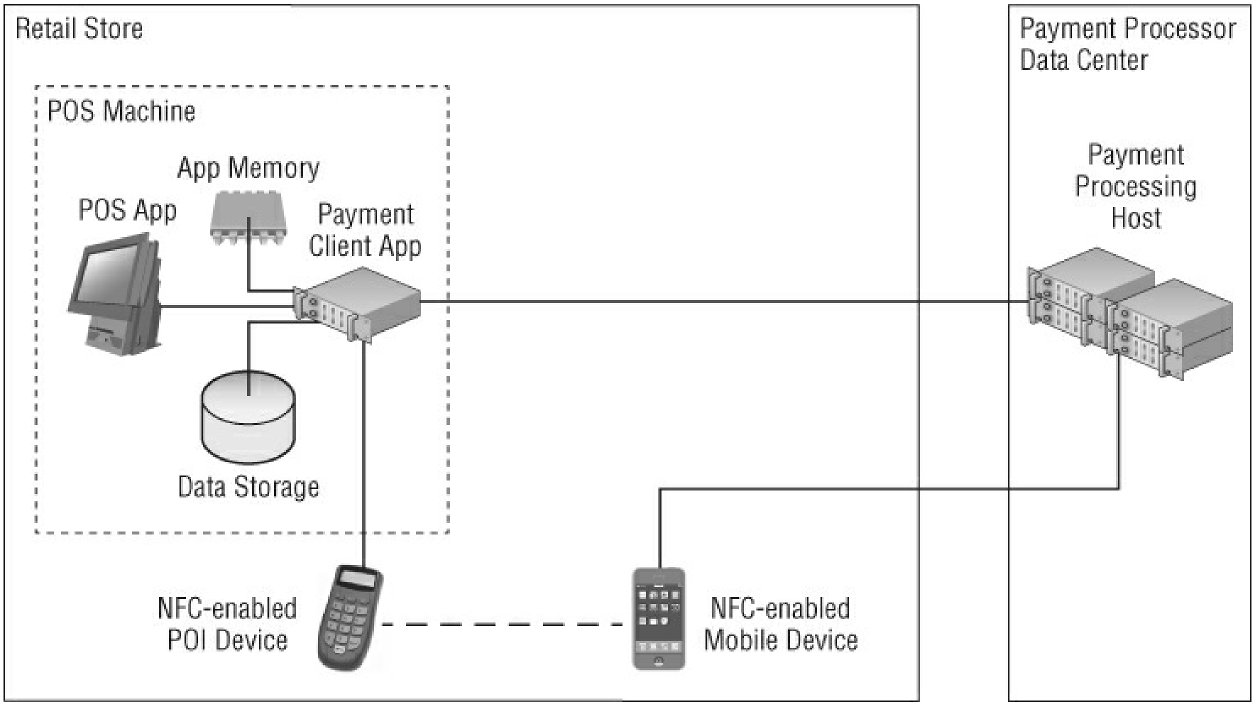
2.31 Non-NFC Mobile Payment Solutions

- Many mobile payment solutions not based on NFC
- Mobile phones such as iphone don ’ t have NFC transmitters
- Limited merchants have deployed POI devices with NFC equipment
- Example of Non-NFC mobile payment applications is Starbucks' Mobile App which depicts the card number and a barcode on the phone's display. To initiate payment the card number is manually

keyed or scanned and payment is processed as a typical card.

- More secure than applications based on NFC since sensitive authentication data never touches the mobile device and POS payment application, which is a huge security benefit compared to contactless/NFC models which require transmission of actual card data through the mobile device to the POS.

Example of Secure architecture and deployment of mobile payments without NFC



Chapter 3 Payment Card

Industry (PCI)

3.0 Payment Card Industry (PCI)

- PCI standards are designed to make payment systems more secure and address many different aspects of the electronic payment life cycle.

- PCI Data Security Standard (PCI DSS) provides a baseline to service providers such as payment processors, gateways etc. in how to protect sensitive cardholder information.

- Payment Application Data Security Standard (PA-DSS) provides a baseline to payment software vendors how developers should structure the design of their products to be compliant with PCI DSS
- PTS: - which takes care of hardware devices, such as POI and HSM (hardware security modules), and their cryptographic modules and firmware.

3.1 PA DSS

- Payment Application Data Security Standard (PA DSS)
- Established as a validation program for POS software vendors who sell products to various clients
- Demonstrates confidence and assurance to buyers that their purchase from the vendors will not violate the PCI DSS rules
- Only standard within PCI DSS that focuses on payment application security

Scope of PA DSS requirements and Payment Application Key Vulnerability Areas

	PA-DSS REQUIREMENT	DATA IN MEMORY	DATA IN TRANSIT	DATA AT REST	PA CODE & CONFIG
1	Do not retain full magnetic stripe, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data	-	-	○	-
2	Protect stored cardholder data	-	-	●	-
3	Provide secure authentication features	-	-	-	-
4	Log payment application activity	-	-	-	-
5	Develop secure payment applications	-	-	-	○
6	Protect wireless transmissions	-	○	-	-
7	Test payment applications to address vulnerabilities	-	-	-	○
8	Facilitate secure network implementation	-	-	-	-
9	Cardholder data must never be stored on a server connected to the Internet	-	-	-	-
10	Facilitate secure remote access to payment application	-	-	-	-
11	Encrypt sensitive traffic over public networks	-	○	-	-
12	Encrypt all non-console administrative access	-	-	-	-
13	Maintain instructional documentation and training programs for customers, resellers, and integrators	-	-	-	-

● – provides an adequate, full protection if implemented correctly

○– provides only limited or selective protection

- – provides no direct protection

	PCI DSS REQUIREMENT	DATA IN MEMORY	DATA IN TRANSIT	DATA AT REST	PA CODE & CONFIG
1	Install and maintain a firewall configuration to protect cardholder data	○	○	○	○
2	Do not use vendor-supplied defaults for system passwords and other security parameters	-	○	○	-
3	Protect stored cardholder data	-	-	●	-
4	Encrypt transmission of cardholder data across open, public networks	-	○	-	-
5	Use and regularly update antivirus software or programs	○	-	○	○
6	Develop and maintain secure systems and applications	○	○	○	○
7	Restrict access to cardholder data by business' need to know	-	-	-	-
8	Assign a unique ID to each person with computer access	○	○	○	○
9	Restrict physical access to cardholder data	-	-	-	-
10	Track and monitor all access to network resources and cardholder data	-	-	-	-
11	Regularly test security systems and processes	-	-	-	-
12	Maintain a policy that addresses information security for all personnel	-	-	-	-

● – provides an adequate, full protection if implemented correctly

○ – provides only limited or selective protection

- – provides no direct protection

PA-DSS REQUIREMENT	PCI DSS REQUIREMENT	GUARANTEES STRONG PROTECTION OF:	FACILITATES CASUAL PROTECTION OF:
9. Cardholder data must never be stored on a server connected to the Internet	1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks	None	Data at rest
10. Facilitate secure remote access to payment application	8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties	None	None
11. Encrypt sensitive traffic over public networks	4. Encrypt transmission of cardholder data across open, public networks	None	Data in transit
12. Encrypt all non-console administrative access	2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access	None	Data in transit, Data at rest
13. Maintain instructional documentation and training programs for customers, resellers, and integrators		None	None
	5. Use and regularly update antivirus software or programs	None	Data at rest, Data in memory, Application code
	7. Restrict access to cardholder data by business need to know	None	None

3.2 PIN Transaction Security

- Essential for payment vendors if payment application operates on a pinpad device
- Integrated POS Solutions such as POS devices or PIN Entry Devices (PED), PIN security is maintained via implementation of triple DES encryption and DUKPT key management mechanisms.

3.3 PCI – P2PE

- Initial attempt to establish a secure single system built from the pin-pad device to the POS to the bulletproof (from the merchant's store environment perspective) data center of a payment gateway or processor

- Security of P2PE systems is designed to be solely dependent on strong cryptography protected by hardware

- More robust and comprehensive than PCI domains thus comprising of 6 domains that stipulate 491 requirements and 648 testing procedures.

3.4 P2PE: Domain 1: Encryption Device Management

- Largely focused on the security of the devices

- Validates and ensures devices conform to PCI PTTS standards

3.5
P2PE: Domain 2: Application Security

- Only in scope for solutions where POI devices is largely executing all key management and cryptographic operations, and transmitting data to the PA hosted by POS

3.6
P2PE: Domain 3: Encryption Environment

- Scope is to address POI deployment and issues relating to the environment encompassing maintenance, secure transportation procedures and key injections.

3.7 P2PE: Domain 4: Segmentation between Encryption and Decryption Environments,

- According to PCI P2PE, “ has no applicable requirements for hardware/hardware solutions since the account data is encrypted for transmission by the PCI-approved POI device before the data leaves the device, and the merchant has no access to the decryption environment or the cryptographic keys. ”

3.8 P2PE: Domain 5: Decryption Environment and Device Management

- Scope of the domain focuses on security of the payment processor data center environment to ensure all aspects of the environment are PCI DSS compliant.

- Stipulates and enforces all key management and decryption operations must be done in HSM certified with FIPS 140-2 and/or PCI PTS.

3.9

P2PE: Domain 6: P2PE Cryptographic Key Operations

- Scope of the domain focuses on cryptographic keys encompassing secure generation, rotation and injection.

Chapter 4 Attacks on POS Systems

4.1 Physical Structure and Security Features

- Payment credit cards can be distinguished from fake payment credit cards based on the following criteria:

- Payment Brand Logo, background, Colour and Image
- *Embossed Primary Account Number (PAN), expiration date,* and *cardholder name*
- *Card Verification Value (CVV2)*
- *Ultraviolet (UV) marks,*
- *Customer service phone numbers*
- *Metallic tipping (optional)*
- *Cardholder Signature (optional)*
- *Cardholder photo (optional),*
- *Hologram (optional)*
- *Holographic magnetic stripe (optional)*

4.2 Why Security Features Fail

- Lack of standardization in the protection standards such as many cards validation code exists with different names: CSC, CVV, CAV, CID, CAV2, etc. with different lengths (3 or 4 digits) and locations (front or back end of the card)

- Payment cards don ’ t inherit any physical security controls so unattended ATMs, Kiosk etc. are vulnerable to fraud targets

4.3 The Magnetic Stripe

- Located in the back of the plastic card
- Magnetic strip stores cardholder data
- 2 magnetic tracks: (track 1 and track 2) used for processing electronic payments
- Track 3 also exists but not implemented for POS processing
- All Data format for credit cards, debit cards, EBS etc. within the magnetic tracks is based on the ISO 7813 standard
- Magnetic stripe contains PAN, expiration date, service code which is send to the payment processing system when card with magnetic stripe is swiped in the MSR device

4.4 Security vulnerabilities – Magnetic Stripe

- Can be duplicated on a blank plastic card using a magnetic stripe encoder device
- Magnetic stripe encoder devices are cheap to buy and accessible

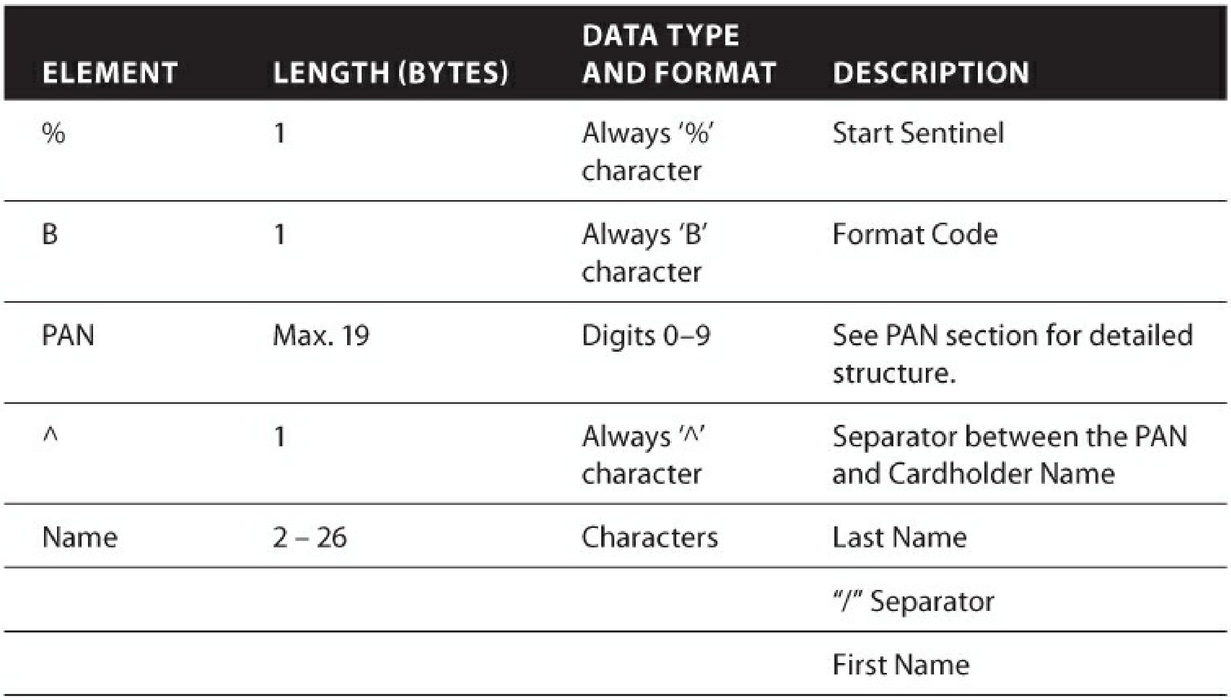
4.5: Track 1

- Comprises of cardholder first name and last name
- Maximum length of track is 79 bytes
- First bytes are the PAN, then the cardholder name which is separated by a “ ^ ” character from the PAN on the left and Expiration Date on the right
- Data is not encrypted or protected in any form but stored in clear text

Field	Data
PAN	4005554444444403
Expiration Date	1512 (December 2015)
Cardholder's first name	SLAVA
Cardholder's last name	GOMZIN
Service Code	101
CVV	123

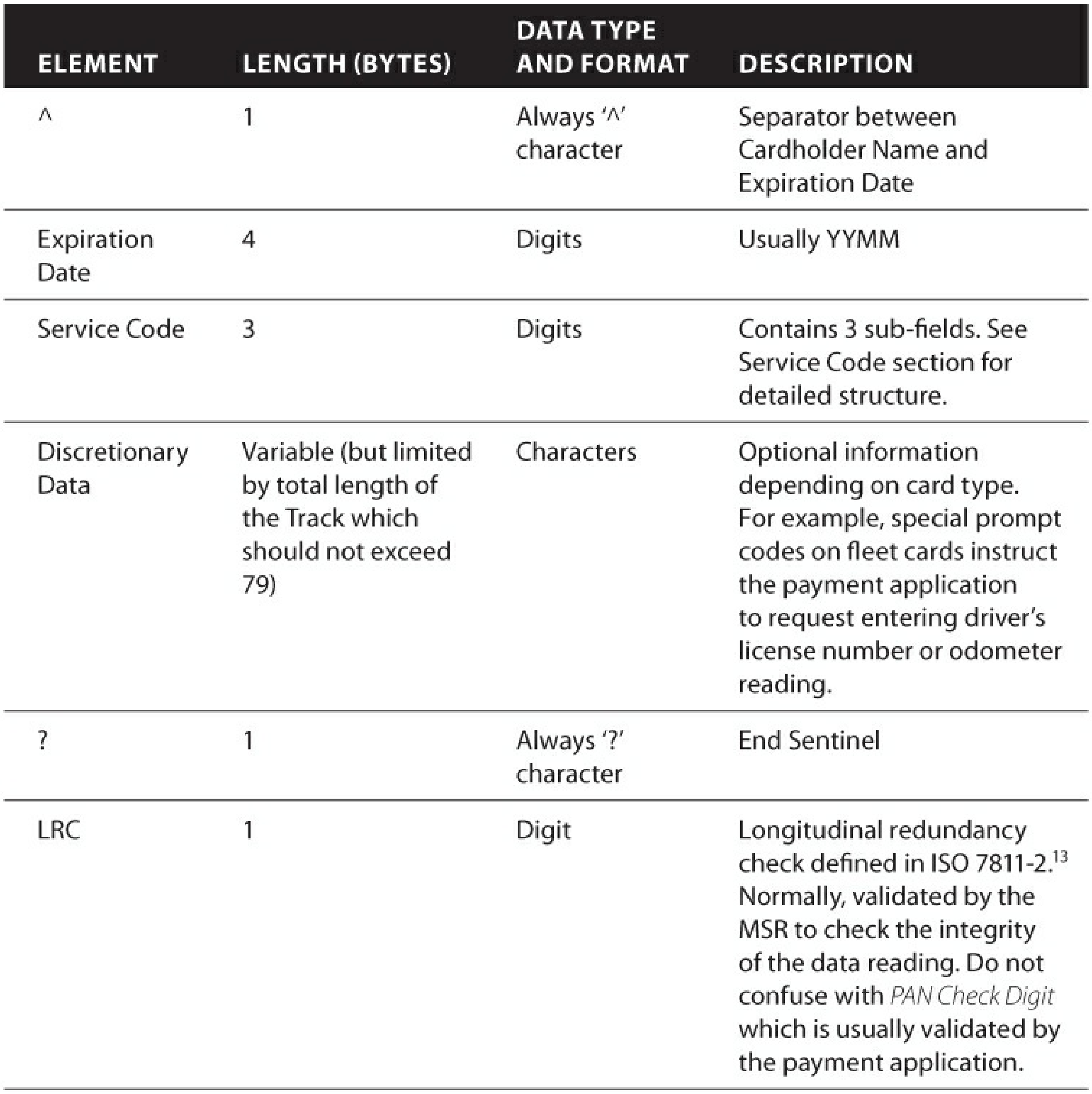
Example of components of Track 1

Detailed Track 1 Structure



ELEMENT	LENGTH (BYTES)	DATA TYPE AND FORMAT	DESCRIPTION
%	1	Always '%' character	Start Sentinel
B	1	Always 'B' character	Format Code
PAN	Max. 19	Digits 0–9	See PAN section for detailed structure.
^	1	Always '^' character	Separator between the PAN and Cardholder Name
Name	2 – 26	Characters	Last Name
			"/" Separator
			First Name

Detailed Track 1 Structure (2/2)



ELEMENT	LENGTH (BYTES)	DATA TYPE AND FORMAT	DESCRIPTION
^	1	Always '^' character	Separator between Cardholder Name and Expiration Date
Expiration Date	4	Digits	Usually YYMM
Service Code	3	Digits	Contains 3 sub-fields. See Service Code section for detailed structure.
Discretionary Data	Variable (but limited by total length of the Track which should not exceed 79)	Characters	Optional information depending on card type. For example, special prompt codes on fleet cards instruct the payment application to request entering driver's license number or odometer reading.
?	1	Always '?' character	End Sentinel
LRC	1	Digit	Longitudinal redundancy check defined in ISO 7811-2.[13] Normally, validated by the MSR to check the integrity of the data reading. Do not confuse with *PAN Check Digit* which is usually validated by the payment application.

4.6 Magnetic Stripe: Track 2

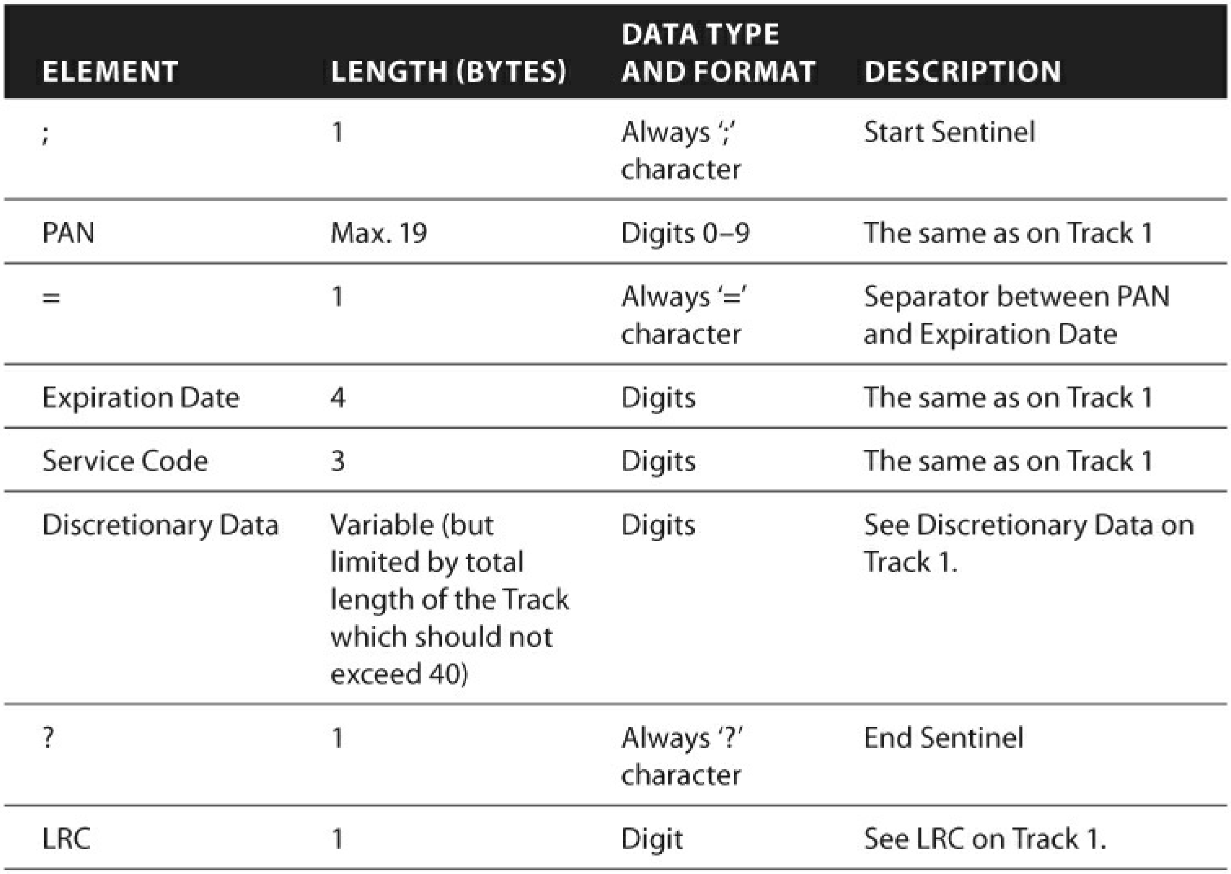
- Contains the following data: PAN, expiration date, service code, card issuer and card type
- Sufficient for payment processing
- Track 1 is optional
- Was released to shorter version of Track 1 in order to improve performance of old dial up payment terminals which were using ground phone lines for communication with the authorizers

- The standard length of Track 2 is 40 ASCII characters
- First digits (usually 16 but vary from 15 to maximum 19) are reserved for the PAN.
- The ‘ = ’ character separates the PAN from the 4 bytes of Expiration Date followed by additional discretional data.

Components of Track 2

Field	**Data**
PAN	4005554444444403
Expiration Date	1512 (December 2015)
Service Code	101
CVV	123

Detailed Track 2 Structure



ELEMENT	LENGTH (BYTES)	DATA TYPE AND FORMAT	DESCRIPTION
;	1	Always ';' character	Start Sentinel
PAN	Max. 19	Digits 0–9	The same as on Track 1
=	1	Always '=' character	Separator between PAN and Expiration Date
Expiration Date	4	Digits	The same as on Track 1
Service Code	3	Digits	The same as on Track 1
Discretionary Data	Variable (but limited by total length of the Track which should not exceed 40)	Digits	See Discretionary Data on Track 1.
?	1	Always '?' character	End Sentinel
LRC	1	Digit	See LRC on Track 1.

4.7 Primary Account Number (PAN)

- Comprises of 16 digits, maximum length is 19 digits
- Incorporated in the front of the payment card
- In the event magnetic stripe, can be used manually for electronic processing at the POS
- Track 1 and Track 2 contain the same PAN, which is also constructed from several elements: ISO Prefix, account number, and check digit

PAN Location On the Magnetic

Tracks

Track	Data
1	%B4005554444444403^GOMZIN/SLAVA^1512101000000012300
2	;4005554444444403=1512101000000012300?

4.8 Expiration Date

- Encoded as four digits: two digits each for month and year.
- Track 1 and 2 contain expiration date which follows the = PAN separator on Track 2 and the second cardholder name separator “ ^ ” on Track 1
- Order of month and year is defined by the ISO standard: first are the last two digits of the year and then the two digits representing the month (YYMM)
- Expiration date is also embossed on the front of the card.
- Payment applications and most payment processors and acquirers do not check the expiration date.
- No verification of the authenticity of the expiration date,

Expiration Date Location on the Magnetic Tracks

Track	Data
1	%B4005554444444403^GOMZIN/SLAVA^1512101000000012300
2	;4005554444444403=1512101000000012300?

4.9 ISO Prefix and BIN Ranges

- First 6 digits of the PAN are called the ISO Prefix, also known as *BIN* or *IIN Prefix* which is the official name.
- ISO Prefix is not part of the account number because it contains generic information about the card issuer

4.10 PCI Disclosure of the PAN - Reasons

- ISO prefix does not contain any cardholder sensitive information
- Cardholders by large often have similar ISO prefix numbers.
- ISO prefix data is known.
- Client payments systems use the ISO only to route the transaction to the relevant processor

4.11 PAN Check Digit

- Last digit of any PAN is referred to as a check digit.
- Check digit enables essential distinction between real card account numbers and and random sequences of digits when looking for PANs in memory or in files.
- Not part of any account number.
- Check digit is determined by a special Mod 10 (Modulus 10) calculation, also known as the Luhn formula invented by Hans Peter Luhn - first information scientists in America.
- Official Mod 10 algorithm for payment cards is defined in Annex B of ISO 7812-1

PAN Check Digit Location on Magnetic Tracks

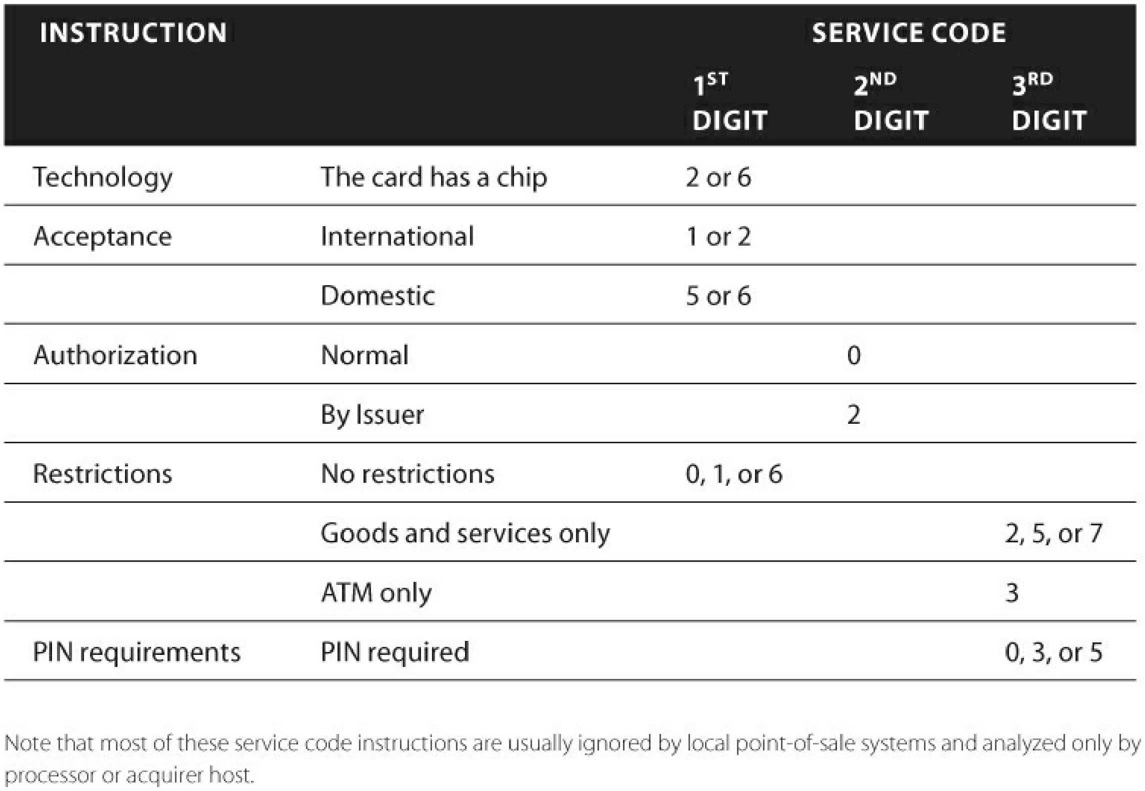
Track	**Data**
1	%B4005554444444403^GOMZIN/SLAVA^1512101000000012300?
2	;4005554444444403=1512101000000012300?

4.12 Service Code

- Instructs the payment application and payment processor how to handle the card during payment acceptance
- Typically consists of 31-byte subfields.
- Most common service codes are 101 and 201, where 101

are simple magnetic stripe cards and 201 are cards which contain chips and have limitations.

Service Code Instructions



INSTRUCTION		SERVICE CODE		
		1ST DIGIT	2ND DIGIT	3RD DIGIT
Technology	The card has a chip	2 or 6		
Acceptance	International	1 or 2		
	Domestic	5 or 6		
Authorization	Normal		0	
	By Issuer		2	
Restrictions	No restrictions	0, 1, or 6		
	Goods and services only			2, 5, or 7
	ATM only			3
PIN requirements	PIN required			0, 3, or 5

Note that most of these service code instructions are usually ignored by local point-of-sale systems and analyzed only by processor or acquirer host.

4.13 Card Verification Values (CVV)

- Established by payment brands in order to address credit card fraud
- Every payment brand has their own unique naming convention

4.14 CVV ENCODED ON MAGNETIC TRACKS

- Depending on payment brand also referred to as CSC, CVC and CAV
- Encoded in track 1 and track 2 areas
- Elicited from the track data elements using a special cryptographic function.
- CVV is verified by the acquirer's host during the authorization phase when the POS sends full Track 1 or 2 data, or both

CVV Location on Magnetic Tracks

Track	**Data**
1	%B4005554444444403^GOMZIN/SLAVA^1512101000000012300?
2	;4005554444444403=1512101000000012300?

4.15
CVV2 PRINTED ON PLASTIC

- Also known as CAD, CAV2, and CVC2 depending on payment brand
- Validation is optional since cardholder is physically present
- CVV2 is not present on the magnetic stripe but only printed on the front or back of the plastic card,
- Card data held in tracks 1 and 2 do not contain any CVV2

4.16 Regular Expressions

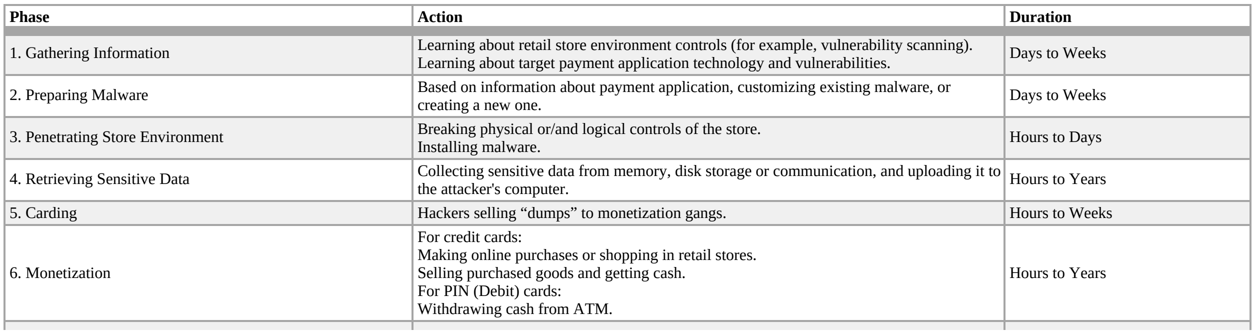
- Programming technique called *regular expressions* (or *regex*) is employed by malware to find Track 1, Track 2, and PAN components in computer memory or disk files.

4.17 Security Breach

- Term largely implemented in the payment industry refer to events related to leak and or fraudulent usage of customer cardholder data.

Carding refers to the “ the practice of buying or selling stolen or hacked credit-card details ”
Hackers typically make money from selling batches of stolen records to individuals or groups

Phases of Typical Card Data Breach



Phase	Action	Duration
1. Gathering Information	Learning about retail store environment controls (for example, vulnerability scanning). Learning about target payment application technology and vulnerabilities.	Days to Weeks
2. Preparing Malware	Based on information about payment application, customizing existing malware, or creating a new one.	Days to Weeks
3. Penetrating Store Environment	Breaking physical or/and logical controls of the store. Installing malware.	Hours to Days
4. Retrieving Sensitive Data	Collecting sensitive data from memory, disk storage or communication, and uploading it to the attacker's computer.	Hours to Years
5. Carding	Hackers selling “dumps” to monetization gangs.	Hours to Weeks
6. Monetization	For credit cards: Making online purchases or shopping in retail stores. Selling purchased goods and getting cash. For PIN (Debit) cards: Withdrawing cash from ATM.	Hours to Years

7. Disclosure	Internal discovery (abnormal system behavior) of public disclosure (customers reporting about fraudulent transactions). Investigation and mitigation.	Days to Months

End