Online Payment Methods

Dr Steven J Murdoch

Computer Laboratory
Visa and MasterCard

• What do they do?

• Some important tasks for online (and offline) payments:
  • Run communication network
  • Set standards
  • Manage disputes between members
  • Set contractual terms between members
Terminology

Payment system network
(MasterCard/Visa/etc.)

Issuing bank

Acquiring bank

Cardholder

Merchant
Terminology

Payment system network (MasterCard/Visa/etc.)

Issuing bank

Card issued

Cardholder

Authorization

Acquiring bank

Authorization

Merchant

Card presented
Terminology

Payment system network
(MasterCard/Visa/etc.)

- Issuing bank
  - Card issued
  - Payment
- Acquiring bank
  - Authorization
  - Payment
- Cardholder
  - Card presented
  - Goods received
- Merchant
  - Payment

Diagram showing the relationship between the issuing bank, acquiring bank, cardholder, and merchant in a payment system network.
How well does the system work?

- **Losses (£m)**

<table>
<thead>
<tr>
<th>Year</th>
<th>Total, ex phone (£m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>503</td>
</tr>
<tr>
<td>2005</td>
<td>491.2</td>
</tr>
<tr>
<td>2006</td>
<td>591.4</td>
</tr>
<tr>
<td>2007</td>
<td>704.3</td>
</tr>
<tr>
<td>2008</td>
<td>529.6</td>
</tr>
<tr>
<td>2009</td>
<td>441.4</td>
</tr>
<tr>
<td>2010</td>
<td>410.6</td>
</tr>
<tr>
<td>2011</td>
<td>463</td>
</tr>
<tr>
<td>2012</td>
<td>518.9</td>
</tr>
</tbody>
</table>

- **Card-not-present**
- **Counterfeit**
- **Lost and stolen**
- **Mail non-receipt**
- **Cheque fraud**
- **ID theft**
- **Online banking**
- **Phone banking**

**Chip & PIN deployment period**
The EMV protocol

1. Card details; digital signature

2. PIN entered by customer

3. PIN entered by customer; transaction description

4. PIN OK (yes/no); authorization cryptogram

5. Online transaction authorization (optional)
Counterfeit fraud

• Producing fake (typically magnetic stripe card) from harvested details
**Deployment of Chip and PIN**

- Chip and PIN was expensive for both parties.
- Deployment was encouraged through "liability engineering".
- Liability was pushed down the chain: Acquirer → Merchant → Issuer → Customer.
- Led to rapid deployment, but caused some problems.
- Still took 10 years.

<table>
<thead>
<tr>
<th>Card</th>
<th>Terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>magstrip</td>
<td>magstrip: Issuer</td>
</tr>
<tr>
<td></td>
<td>chip: Issuer</td>
</tr>
<tr>
<td></td>
<td>chip &amp; PIN: Issuer</td>
</tr>
<tr>
<td>chip</td>
<td>magstrip: Acquirer</td>
</tr>
<tr>
<td></td>
<td>chip: Issuer</td>
</tr>
<tr>
<td></td>
<td>chip &amp; PIN: Issuer</td>
</tr>
<tr>
<td>chip &amp; PIN</td>
<td>magstrip: Acquirer</td>
</tr>
<tr>
<td></td>
<td>chip: Acquirer</td>
</tr>
<tr>
<td></td>
<td>chip &amp; PIN: Issuer</td>
</tr>
</tbody>
</table>
The no-PIN attack
The EMV protocol

1. Card details; digital signature
2. PIN entered by customer
3. PIN entered by customer; transaction description
4. PIN OK (yes/no); authorization cryptogram
5. Online transaction authorization (optional)
The no-PIN attack protocol

1. Card details; digital signature
2. Wrong PIN entered by crook
3. Wrong PIN entered by crook; transaction description
4. PIN OK (yes); authorization cryptogram
5. Online transaction authorization (optional)

fake card

issuer

transaction; cryptogram

merchant

crook

1/3/4. Card details; digital signature
PIN; transaction description
PIN OK; cryptogram

card

result
Online banking authentication

• Simple scam is to “phish” for account details

• Ask for username and password

• Low success rate, but just a few customers is enough to make investment worthwhile

• Actually moving money out is the high-risk part of the scam

• This is allocated to money-mules recruited supposedly to pay foreign staff

• Often the money mule will lose money and may be prosecuted for fraud

Dear Customer

Account Protection Update, To ensure there are no further scam and other account threats, it’s strongly recommended to update account protection.

Click on "Protection" to continue the process.

Protection.

Online Internet Banking Security Center

Halifax Internet Banking.

Thanks for your co-operation.

Fraud Prevention Unit
Legal Advisor
Halifax PLC.

Please do not reply to this e-mail. Mail sent to this address.
Hardening passwords
Replacing passwords (iTAN)
Man in the Browser

SecureBank Inc.
account: 6734 3249
code: 4068 3854

account: 9857 2745
code: 4068 3854
MitB protection

Überweisung

Konto: 25000000019 Daniel Richter Privatkonto
Saldo in EUR: 50,00 S online-verfüg. Betrag in EUR: 950,00

Empfänger:
Max Mustermann
Konto-Nr. des Empfängers:
123457890
Bankleitzahl:
85090000

Bei Kreditinstitut:
Betrag in EUR:
20,56
Verwendungszweck:

Bitte geben Sie die TAN neben der Nr. 110 ein.

Transaktions- Daten und Anforderung iTAN

Geburtstag des VR-NetKey- Inhabers als „Wasserzeichen“ im Hintergrund.
Transaction authentication
Summary so far

• Counterfeit fraud
  • Magnetic stripe fallback facilitated by Chip and PIN
• Lost and stolen/Mail-non-receipt
  • no-PIN attack can bypass PIN protection
• Cheque fraud and ID theft
  • Primarily not a technology problem
• Online banking
  • Transaction authentication likely the way to move
Combining EMV with online banking
Combining EMV attacks with online banking
Card not present transactions

• Basic version: same as old card-present transaction
  • Card number and expiry date sent back
  • Can also send back CVV2 off back of card
  • Can also perform address verification
• Every extra step will lose customers at check-out stage
• Some vendors will skip security measures
  • Amazon don’t even perform CVV2 checks
  • Leaves non-Amazon users at risk of fraud (though will eventually be refunded)
Acquirer interface for web based merchants

• Small web merchants will not deal directly with acquirer
  • To allow international payments, many acquirers likely needed
  • Merchants might like to avoid access to customer details as much as possible to reduce liability
• Examples of payment processors include
  • Sage Pay
  • Worldpay
  • Paypal slightly different
  • Hoped people would leave money in account; actually mostly ended up as payment processor
Example: Sage Pay (Form)

A. Shopper visits your website to make a purchase.
B. You re-direct your shopper through to our payment pages.
C. We capture the details, and pass these through to the bank for authorisation.
D. We send your shopper back to your Success or Failure page with the transaction results.
Example: Sage Pay (Server)

A. Shopper visits your website selects the item, and enters their details on your website.

B. You send the details of the transaction to us using our protocols.

C. We validate all of the details, and pass you the "Next URL" for you to transfer your shopper.

D. You transfer your shopper from your website through to our payment page.

E. We capture the card details, and send these to the bank for authorisation.

F. We notify your system of the status of the transaction to your Notification URL.

G. You respond to us with your re-direction URL.

H. We send your shopper back to your website where they are told the status of the transaction.
Example: Sage Pay (Direct)

Diagram:

A. Shopper visits your website selects the item, and enters their card details on your site.
B. You send the details of the transaction, and the card information to us using our protocols.
C. We validate all of the details, and pass these through to the bank for authorisation.
D. We send you the status of the transaction which you then display to your shopper.
3-D Secure (Verified by Visa/MasterCard SecureCode)

Please submit your Verified by Visa password.

Merchant: Online Retailer Ltd.
Amount: GBP 9.99
Date: 01:01:10
Card number: XXXX XXXX XXXX 1234
Personal Message: A personal greeting
Password: [Password field]

Forgot your password?

Submit  Help  Cancel

Your bank's logo
The name of the retailer that you are shopping with
The value of the purchase
Today's date
The last four digits of your card number
The personal message that you set when registering

Visa
3-D Secure (Verified by Visa/MasterCard SecureCode)

1. Request 3DS enrollment check
2. Check 3DS enrollment
3. Enrollment response and URL for card issuer's authentication site
4. Redirect to card issuer's authentication website
5. The cardholder provides authentication details
6. Redirect browser back to merchant website
7. Request interpretation of the 3DS response
8. 3DS Authentication Result

Browser
Merchant Application
Payment Gateway
Directory Server
Card Issuer's Authentication Website

Cardholder
3D secure phishing vulnerability

**Verified by Visa / MasterCard SecureCode Enrollment:**

Due to recent changes to FDIC Deposit Insurance Rules all our customers must be enrolled in Verified by Visa or MasterCard SecureCode program depending on type of your Check Card. To continue complete this form and click Activate Now.

- **Social Security #:**
- **Card Number:**  (16 digits)
- **Expiration Date:**  (MM/YY)
- **Signature Code:**  (Last 3 digits on the back)
- **Card PIN Code:**  (4-6 digit code that you enter in ATM)

**Choose Password:**
- How will it be used?
- (6-12 character length)

If you already enrolled in Verified by Visa or MasterCard SecureCode program to continue please enter current password or select new then click Activate Now.

**Enter Account Information**

Please enter the information below and click the "Continue" button. You can review this information verified by visa account.

**Payment Information**

Tell us the card to add to your Account:

- **Card Nickname:** (example: My Bank One Visa)
- **Card Number**
- **Expiration Date**
- **CVV2**
- **ATM Pin**
- **Name on Card (first/last)**
SOFORT Überweisung
Mobile payments

• May just be interface to online banking website
• mPESA and similar use mobile SIM as root of trust (serves underbanked)
• Barclays Pingit based around Direct Debit
Summary and conclusions

• For card-present transactions, Chip and PIN was supposed to help
  • Reality was more complex and fraud went up

• Card fraud is now dominated by card-not-present transactions
  • Merchant pays cost, but extra security loses customer conversions

• For small merchants, much of the work is delegated to payment processor

• Online payment systems typically run on previous rails
  • Credit/debit card (optionally with 3D Secure)

• Online banking

• Direct debit