Safe payments on the Net

Chris Mitchell

Information Security Group

Royal Holloway, University of London

http://www.isg.rhul.ac.uk/~cjm

Internet e-commerce

- Focus of this talk is security issues for e-commerce payments made across the Internet.
- In other words the talk focuses on security issues for b2c (business to consumer) e-commerce.
- This is a rapidly growing method for buying goods and services, despite end of ‘dot com’ boom.

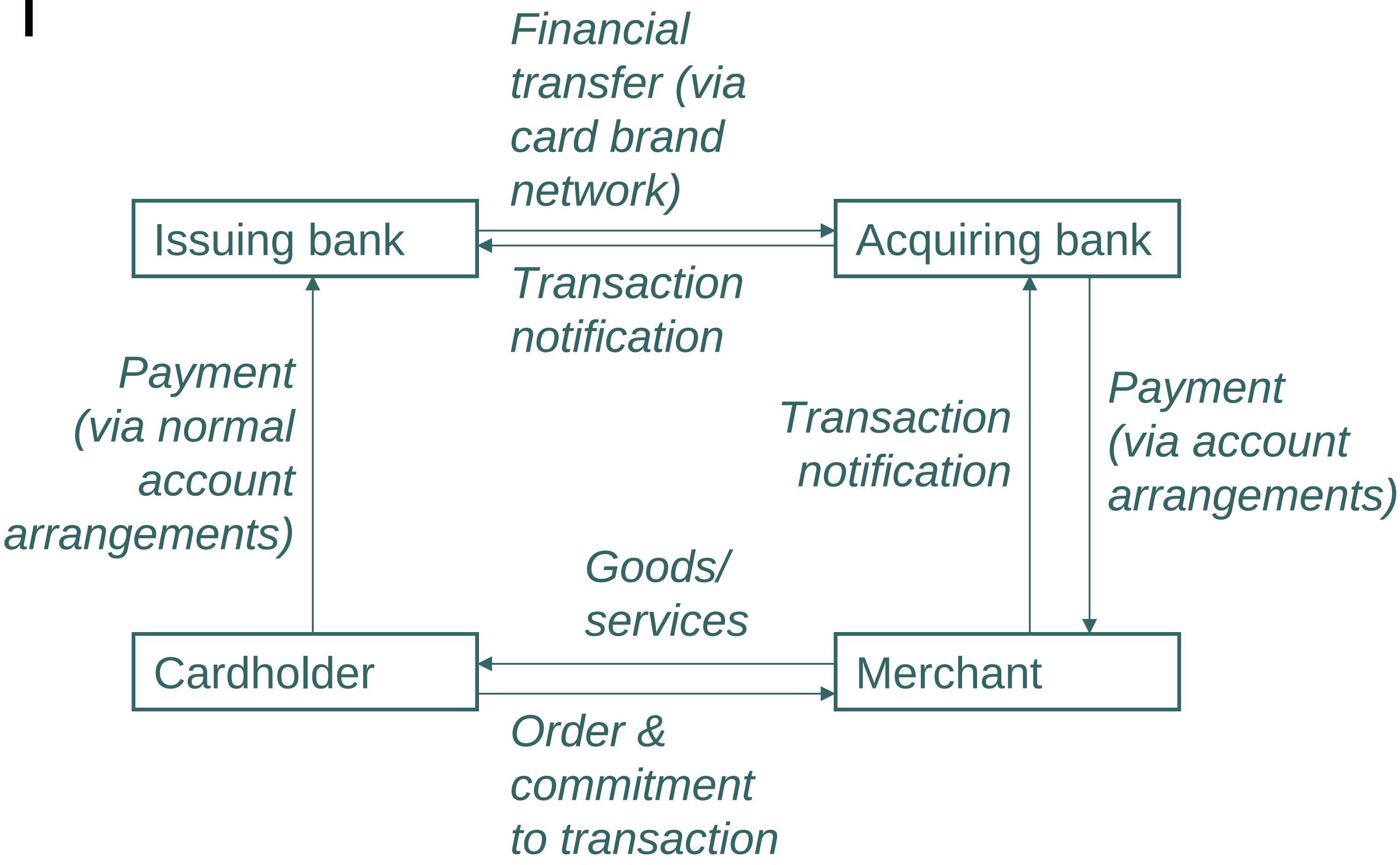
Payment methods

- There are a variety of possible methods for making payments across the Internet.
- Methods include:
  - debit/credit cards;
  - bank transfers/cheques;
  - third party payment services (e.g. Paypal).

Credit card payments

- The ‘standard’ payment model for credit card payments involves four parties:
  - Cardholder;
  - Merchant;
  - Issuing bank (issuer of card);
  - Acquiring bank (relationship with merchant).

Payment model


Financial transfer (via card brand network)
Issuing bank
Acquiring bank
Transaction notification
Payment (via normal account arrangements)
Transaction notification
Payment (via account arrangements)
Goods/ services
Cardholder
Merchant
Order & commitment to transaction

Royal Holloway University of London

Security threats

- Number of security threats to this payment model when merchant & cardholder interact via the Internet, including:
  - impersonation of cardholder using stolen credit card details;
  - theft of credit card details when sent via Internet;
  - theft of credit card details at merchant;
  - manipulation of transaction details during transmission across Internet;
  - manipulation of transaction details at Merchant.

Security techniques – what we have today

- On-line transaction authorisation at merchant (prevents use of stolen cards);
- CVC value printed on card (designed to make use of stolen card details harder);
- Use of SSL/TLS to protect cardholder/merchant link (and authenticate merchant).

Areas not covered

- Credit card details held in cleartext on merchant server.
- No cardholder authentication – hence if cardholder repudiates transaction then merchant loses (no cover for ‘cardholder not present’ transactions).
- No protection for transaction details except on cardholder/merchant link.

EMV

- EMV (for Europay-MasterCard-Visa) is a set of specifications for smart card/terminal interactions.
- EMV-compliant credit cards now being rolled out in UK.
- EMV not really designed to protect e-commerce.
- Designed to reduce fraud and reduce number of online authorisations (expensive).

SSL/TLS

- Secure Sockets Layer (SSL) – and the similar Transport Layer Security (TLS) – provide security for an Internet communications link.
- TLS is commonly used to protect e-commerce transactions against Internet eavesdroppers.

Residual security risks

- SSL/TLS does not protect data once it reaches the merchant server.
- SSL/TLS does not provide cardholder authentication.
- Although SSL/TLS provides merchant authentication, this is not foolproof, as it relies on the cardholder checking displayed web pages.

SET – a complete solution?

- In mid-1990s, Visa and MasterCard agreed on SET (Secure Electronic Transaction) specifications.
- SET provides ‘complete’ protection for e-commerce transactions.
- Bidirectional authentication, encryption of card details at merchant server, privacy of transaction details from acquirer bank, transaction integrity protection, …
- SET transactions regarded as ‘cardholder present’ transactions.

Why has SET failed?

- Despite dealing with all security threats, and protecting merchants against losses, SET has not been adopted to any significant extent.
- Number of reasons:
  - Cost for merchants;
  - Complexity of cardholder initialisation;
  - Lack of cardholder mobility, …

SET extensions

- Various SET ‘extensions’ have been introduced to try to promote SET adoption.
- PIN extensions allow cardholder authentication via a card PIN.
- Chip extensions allow use of an EMV card to avoid need for SET initialisation process.

Other solutions

- Despite the best efforts of Visa and MasterCard, SET now seems doomed to failure.
- Other approaches to the enhancement of e-commerce security being tried.
- Still not clear what will happen in long run.

3-D Secure

- One recently devised approach being promoted by Visa.
- One of a number of ‘3 domain’ solutions.
- Instead of requiring cardholder and merchant to provide secure payment functionality, servers provided by issuer and acquirer perform functions on behalf of end-players.
- Servers interact with interoperability (brand) server – hence ‘3 domains’.

M-commerce solutions

- Other possible approaches to secure Internet payments operate via mobile networks (or with support of mobile networks).
- Promising because mobile networks already have means for end-user authentication, and mobiles rapidly becoming ubiquitous.

Electronic cash

- Other solutions rely on payment methods other than credit card.
- One family of solutions involves storing value on smart cards.
- Such e-cash already in use in variety of countries, and can also potentially be used for e-commerce transactions.

Where next?

- Long term solution to security for b2c e-commerce still very unclear.
- Probably will involve a combination of different payment models.
- 3-D solutions seem promising for debit/credit payments.
- M-commerce solutions also appear likely.