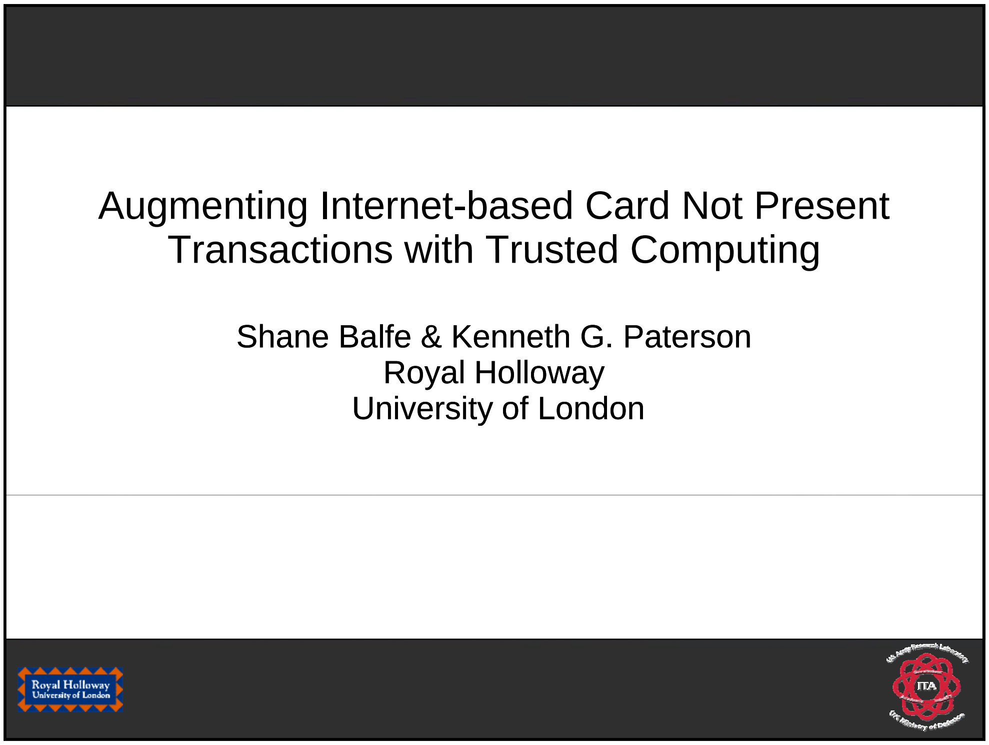
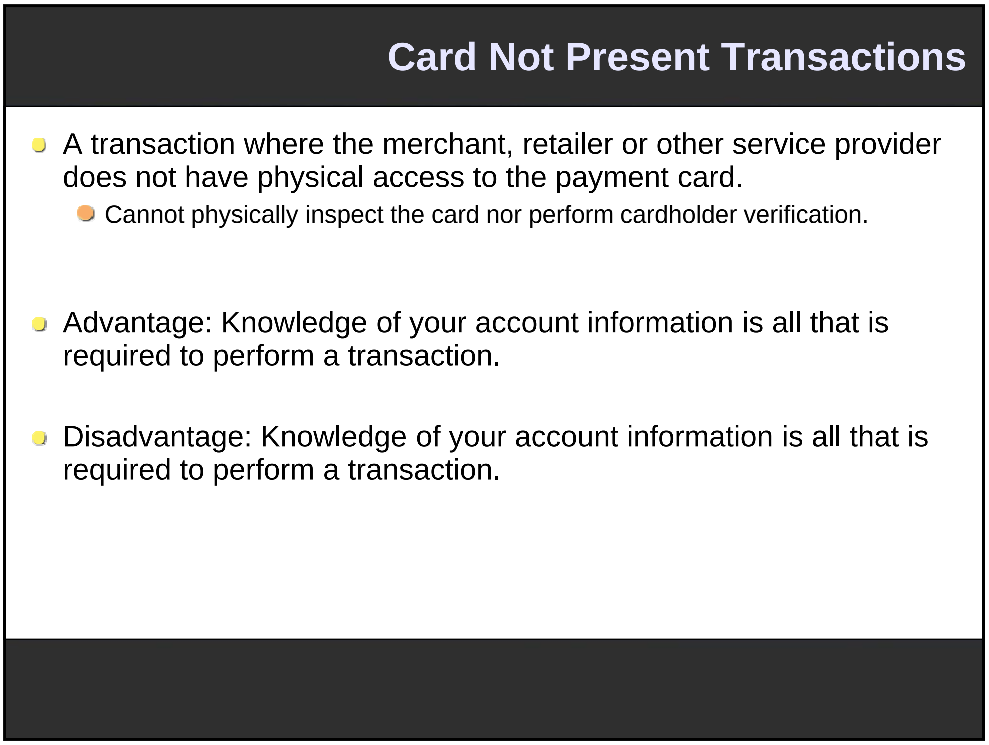


Augmenting Internet-based Card Not Present Transactions with Trusted Computing

Shane Balfe & Kenneth G. Paterson
Royal Holloway
University of London



Card Not Present Transactions

- A transaction where the merchant, retailer or other service provider does not have physical access to the payment card.
  - Cannot physically inspect the card nor perform cardholder verification.
- Advantage: Knowledge of your account information is all that is required to perform a transaction.
- Disadvantage: Knowledge of your account information is all that is required to perform a transaction.

What's the Problem?

- A report by the Association for Payment Clearing Services (APACS) on card fraud showed that Internet-based CNP transactions accounted for 36% of all card fraud perpetrated in 2006 in the UK.
  - This translated into £154.5 million in losses for card issuers and merchants.
- A report by Symantec highlighted that between the period July and December 2006, five of the top ten new malicious code families detected were trojans with keystroke logging capabilities.
  - Home users now account for 93 % of *all* targeted attacks.
  - It is predicted that mobile devices (such as smart phones and PDAs) will increasingly become targets of malware in the coming years.

Threats

- Phishing attacks
  - Attempt to fraudulently obtain sensitive information, such as usernames, passwords and credit-card details, by masquerading as a trustworthy entity.
- Spyware and Transaction Generators
  - Attempt to subvert platform and either extract credentials from a platform or locally instigate new transactions.

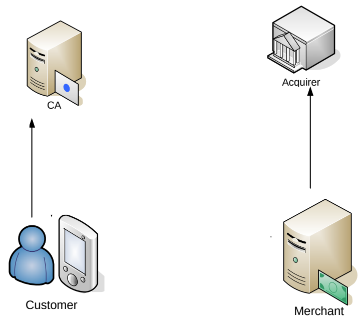
Preventing Online CNP Fraud

- SSL: Acts as a facilitator for the secure transfer of customer account details.
- 3-D Secure: An adjunct to SSL-based approach. Attempts to provide cardholder authorisation for Internet-based CNP transactions based on an additional password authentication.
- Given the increased threat from malware it is debatable how much of a barrier these protocols will be in preventing CNP fraud in the future.

Trusted Computing

- A Trusted System is one that will behave in a particular manner for a specific purpose.
- Trusted Computing has become synonymous with four fundamental concepts:
  - Integrity measurement and storage.
  - Attestation.
  - Protected storage.
  - Software Isolation.
- Physical Presence
  - Shows hardware manipulation of the platform.
  - “Depressing a key on the keyboard or some other such action” and should be “should be difficult or impossible to spoof by rogue software”.

Committing to a transaction



Our Work

- By tying payment authorisations to Trusted Computing hardware, in the form of a TPM, we provide similar benefits to those obtained with EMV (Chip and Pin).
- The use of client-side certification (where the private-key is non-migratable from tamper-resistant hardware) can defend against phishing attacks.
- The use of physical presence significantly reduces power of transaction generation attacks.
- In our full paper we describe how such a function may be integrated with SSL and 3-D Secure.

- Questions?