



E-Commerce Course Review

Michael O’Herlihy



Agenda

- Course Review
- Individual Assignments
- Exam Questions



E-Commerce Introduction

- E-Commerce Definition
- E-Commerce versus E-Business
- Pure Versus Partial EC
- EC Organisations
 - Bricks and Mortar
 - Bricks and Clicks
 - Clicks Only
- EC Domains
 - B2B, B2C, C2C, C2B

Traditional Payment Methods

- Cash
- Check
- Credit Card
- Stored Value
- Accumulating Balance

Desirable Properties of Digital Money

- Universally accepted
- Transferable electronically
- Divisible
- Cant be stolen or forged
- Private (no one except parties know the amount)
- Anonymous (no one can identify the payer)
- Work off-line (no online verification needed)

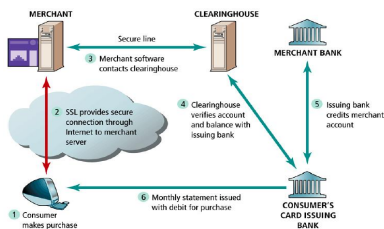
Accepting Credit Cards Online

- Merchant Account
- Third Party Services Providers
- Virtual Malls
- Person to Person (P2P) Payment Systems

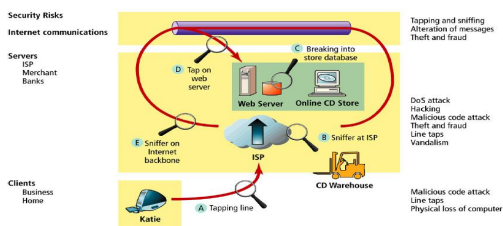
How an Online Credit Card Transaction Works

- Processed in much the same way that in-store purchases are
- Major difference is that online merchants do not see or take impression of card, and no signature is available - Card Not Present (CNP) transactions
- CNP transactions incur a higher fee
- Participants include consumer, merchant, clearinghouse, merchant bank (acquiring bank) and consumer's card issuing bank

Typical E-Commerce Transaction



Vulnerable Points in an E-Commerce Transaction



Most Common Threats

- Most common threats:
 - Malicious code
 - Hacking and cyber vandalism
 - Credit card fraud/theft
 - Spoofing
 - Denial of service attacks
 - Sniffing
 - Insider jobs

Dimensions of E-Commerce Security

- **Confidentiality:** ability to ensure that messages and data are available only to those authorised to view them
- **Integrity:** ability to ensure that information being displayed on a Web site or transmitted/received over the Internet has not been altered in any way by an unauthorised party
- **Availability:** ability to ensure that an e-commerce site continues to function as intended
- **Non-repudiation:** ability to ensure that e-commerce participants do not deny (repudiate) online actions
- **Authenticity:** ability to identify the identity of a person or entity with whom you are dealing on the Internet
- **Privacy:** ability to control use of information a customer provides about himself or herself to merchant

The Tension between Security and Other Values

- Security vs. ease of use: the more security measures that are added, the more difficult a site is to use, and the slower the process becomes
- Security vs. desire of individuals to act anonymously

SPAM

- *“Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups”*
- Directive 2002/58/EC, implemented as:
European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003
(SI 535/2003)
in force 6 November 2003

Irish Legislation

- The new Irish laws also place restrictions on direct marketing via telephone, fax, automated calling system and, importantly, SMS and MMS, or mobile spam
- Positives
 - It's opt-in, rather than opt-out
 - Each spam counts as a separate offence
 - Forging / disguising of originating header info is prohibited
- Negatives
 - No private right of action
 - Spamming to mailing lists is not prohibited
 - No good against non European based spammers

Encryption

- The translation of data into a secret code
- To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it
- Unencrypted data is referred to as plain text
- Encrypted data is referred to as cipher text
- Two Types of Encryption
 - Symmetric
 - Asymmetric (public-key)

Major problems of Symmetric Encryption

- **Data Integrity:** Receiver can not verify the that a message has not been altered
- **Repudiation:** Receiver can not make sure that the message has been sent by the claimed sender
- **Scalable Key Distribution**

Asymmetric – Public Key Encryption

- An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them
- It is virtually impossible to deduce the private key if you know the public key

Individual Assignments

Exam Questions

- 6 Questions Do 4
- 2 Questions on this Module
- Two Parts to each question
 - A Part worth 15 Marks, B Part worth 5 Marks
- “Identify, explain and give examples”

Last Years Exam Question

- Traditional payment systems were never designed for use in the digital world. As the Internet has expanded and more consumers make online purchases, the weaknesses of cash, cheques, and credit and debit cards become more apparent.

a) Describe a typical online credit card transaction. In your answer you must detail the roles played by each of the five parties involved.

15 Points Available: 1 point for mentioning each of the 5 parties and 2 additional points for describing the process that party plays.

b) List five desirable properties of “digital money”.

- 5 Points Available: 1 point for listing each property.

Contact Details

- Michael O’Herlihy
- Email: michael@websteps.ie
- Course Site: <http://www.websteps.ie/tcd>
- Telephone: 01 440 3868
- Mobile: 086 600 8710
