

E-Commerce Security

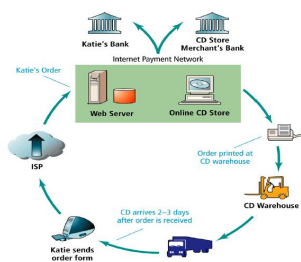
Michael O'Herlihy

23rd November 2006

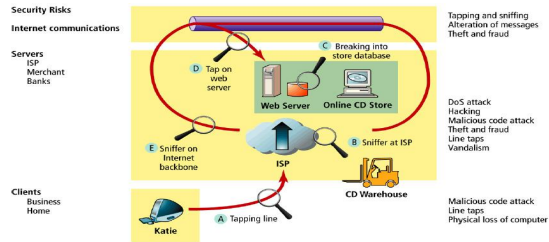
Agenda

- Typical E-Commerce Transaction
- Vulnerable Points
- Most Common Threats
- Technology Solutions

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

Malicious Code

- Includes a variety of threats such as viruses, worms, Trojan horses, and "bad applets"
- A virus is a computer program that has the ability to replicate or make copies of itself, and spread to other files
- A worm is a program that runs independently and consumes resources of the host computer from within and can propagate a complete working version of itself to another system
- Trojan horse takes the appearance of a friendly application, but performs some unwanted task in the background
- A logic bomb sits dormant until it is awakened by a particular event

Malicious Code

NAME	TYPE	DESCRIPTION
Melissa	Macro virus/worm	First spotted in March 1999. At the time, Melissa was the fastest spreading infectious program ever discovered. It attacked Microsoft Word's normal dot global template, ensuring infection of all newly created documents. It also mailed an infected Word file to the first 50 entries in each user's Microsoft Outlook address book.
Codified	worm	Appeared in 2001. It geared for hundreds of thousands of systems and tried to flood the White House IP address with bogus information requests.
Chernobyl	file infecting virus	First appeared in 1988. It is very destructive: It wipes out the first megabyte of data on a hard disk (making the rest useless) every April 26, the anniversary of the nuclear disaster at Chernobyl.
Klez	E-mail worm	Most prolific virus of 2002. Klez comes in an e-mail with a random subject line and message body. Once launched, the worm sends itself to all addresses in the Windows address book, the database of instant-messaging program ICQ, and local files. A file from the user's system is randomly selected and sent along with the message. Klez also attempts to disable anti-virus software and drops another virus in the user's system that tries to infect executable files there and across network filing systems.
Bugbear	Trojan horse/worm	Struck in 2002. It appeared as an e-mail attachment and random e-mail was infected in over 22,000 systems in 24 hours. It can intercept Web activity (i.e., credit card information) and can disable Windows and anti-virus software.

Hacking and Cyber Vandalism

- Hacker is an individual who intends to gain unauthorised access to a computer system
- Cracker is the term typically used within the hacking community to demote a hacker with criminal intent
- Cyber Vandalism is intentionally disrupting, defacing, or even destroying a site

Credit Card Fraud

- Fear that credit card information will be stolen deters online purchases
- Hackers target credit card files and other customer information files on merchant servers; use stolen data to establish credit under false identity
- One solution: New identity verification mechanisms

New identity verification mechanisms

- **Address verification service (AVS)** is an important fraud-prevention mechanism that verifies customer addresses within the United States. This ensures the identification of the cardholder and guarantees that you ship merchandise to a legitimate customer
- *Address Verification Service: To Catch a Thief* (<http://www.inc.com/articles/2000/06/19976.html>)

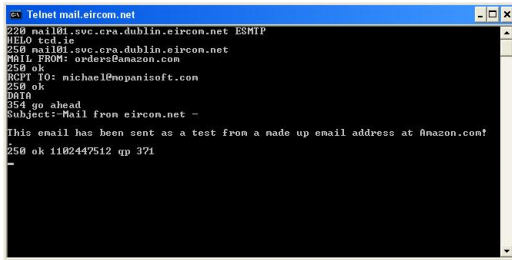
New identity verification mechanisms

- **Card validation code 2 (CVC2)** and **card verification value 2 (CVV2)** are important fraud-prevention mechanisms initiated by MasterCard and Visa to protect merchants
- MasterCard's CVC2 and Visa's CVV2 codes help merchants distinguish legitimate customers from those who try to commit fraud
- These codes are the three digits on the back of a MasterCard or Visa card that follow the cardholder's credit card number - they protect Internet merchants by helping to identify a cardholder in a non-face-to-face transaction
- An added layer of security for CNP transactions

Spoofing

- **Spoofing:** Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
- Can involve redirecting a web link to an address different from the intended one with the site masquerading as the intended one

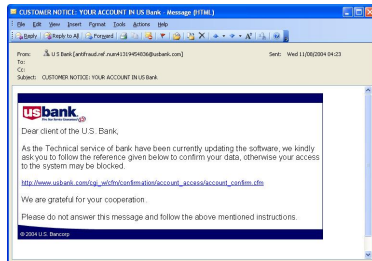
Spoofting



```
telnet mail.eircom.net
220 mail01.svc.cpa.dublin.eircom.net ESMT
HELO ted.ie
250 mail01.svc.cpa.dublin.eircom.net
MAIL FROM: orders@amazon.com
250 ok
RCPT TO: michael@mopanisoft.com
250 ok
3810
354 go ahead
Subject: Mail from eircom.net -
This email has been sent as a test from a made up email address at amazon.com!
250 ok 1402447512 qp 371
```

Email Relaying

Spoofting



That link does not go to <http://www.usbank.com/>, it actually goes to <http://80.239.36.118:87/cfm/index.htm>

DoS and dDoS Attacks

- Denial of service (DoS) attack: Hackers flood Web site with useless traffic to inundate and overwhelm network
- Distributed denial of service (DDoS) attack: hackers use numerous computers to attack target network from numerous launch points
- Do a Google search for Distributed Denial of Service attacks and you will be amazed at the number of results

ISPs raise the stakes on DDoS attacks
(<http://news.zdnet.co.uk/internet/security/0,39020375,39175485,00.htm>)

Sniffing

- Sniffing: type of eavesdropping program that monitors information travelling over a network; enables hackers to steal proprietary information from anywhere on a network

Insider Jobs

- Insider jobs: single largest financial threat
- IT systems administrators increasingly are seen as the most potentially dangerous insider threat
- Psychological profile
 - Likely to be seen in an insider threat:
 - Introvert; lives online
 - History of significant frustrations relating to family, peers, co-workers
 - Divorce or romantic discord
 - Propensity for anger toward authority
 - Grandiosity covers fragile ego
 - Extreme attachment to IT infrastructure

Source: George Washington University Political Psychology Program

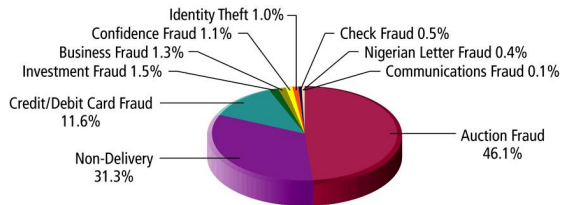
Technology Solutions

- Protecting Internet communications (encryption)
- Securing channels of communication
- Protecting networks (firewalls)
- Protecting servers and clients

Tools Available to Achieve Site Security



Internet Fraud Complaints (US)



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
