E-commerce
Security

Threats and Protection Mechanisms. This lecture covers internet security issues and discusses their impact on an e-commerce.

Learning objectives

You will learn about:

- Internet security issues
- Security for client computers
- Security for the communication channels between computers
- Security for server computers
- Organizations that promote computer, network, and Internet security

Internet Security Issues:
Overview

- **Computer security**: The protection of assets from unauthorized access, use, alteration, or destruction
- **Physical security**: Includes tangible protection devices
- **Logical security**: Protection of assets using nonphysical means
- **Threat**: Any act or object that poses a danger to computer assets

Managing Risk

- **Countermeasure**: General name for a procedure that recognises, reduces, or eliminates a threat
- **Eavesdropper**: Person or device that can listen in on and copy Internet transmissions
- **Crackers or hackers**: Write programs or manipulate technologies to obtain unauthorized access to computers and networks

Computer Security Classifications

- **Secrecy**: Protecting against unauthorized data disclosure and ensuring the authenticity of data source
- **Integrity**: Refers to preventing unauthorized data modification
- **Necessity**: Refers to preventing data delays or denials (removal)
Security Policy and Integrated Security-1

- A written statement describing
  - Which assets to protect and why they are being protected
  - Who is responsible for that protection
  - Which behaviors are acceptable and which are not
- First step in creating a security policy
  - Determine which assets to protect from which threats
  - Define minimum level of acceptable security

Security Policy and Integrated Security-2:
Requirements for Secure Electronic Commerce

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secrecy</td>
<td>Prevent unauthorized persons from reading messages and business data, unauthorized trial or audit, or unauthorized access to resources.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Ensures information is a digital envelope so that the computer can automatically detect messages that have been altered in transit.</td>
</tr>
<tr>
<td>Availability</td>
<td>Provide delivery assurance for each message segment so that messages or message segments cannot be lost undetectable.</td>
</tr>
<tr>
<td>Key management</td>
<td>Provide secure distribution and management of keys needed to provide secure communications.</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>Provides undeletable, tamper-proof of each messages’s origin and recipient.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Securely identify clients and servers with digital signatures and certificates.</td>
</tr>
</tbody>
</table>

Security Policy and Integrated Security-3

Elements that a security policy should address:

- Authentication: who is trying to access?
- Access control: who is allowed to log on and access?
- Secrecy: who is permitted to view selected info?
- Data integrity: who is allowed to change data?
- Audit: who or what causes specific events to occur and when?


- **Active content**: Programs embedded transparently in Web pages and cause action to occur
- **Scripting languages**: Provide scripts, or commands, that are executed (JavaScript; VBScript)
- **Applet**: Small application program (Java Applets)


- **Trojan horse**: Program hidden inside another program or Web page that masks its true purpose
- **Zombie**: Program that secretly takes over another computer to launch attacks on other computers
  - Attacks can be very difficult to trace to their creators

Example: Dialog box asking for Permission to Open a Java Applet

Figure 11-3: Dialog box asking for permission to execute a Java applet
Security for Client Computers-

Cookies

- **Cookie Central**: Web site devoted to Internet cookies
- **Session cookies**: Exist until the Web client ends connection
- **Persistent cookies**: Remain on client computer indefinitely

Example: Information Stored in a Cookie on a Client Computer

Security for Client Computers-

Cookies2

- **First-party** cookies: Cookies placed on client computer by Web server site
- **Third-party** cookies: Cookies placed on client computer by different Web site
- **Web bug**: Tiny graphic that a third-party Web site places on another site’s Web page

Security for Client Computers-

Java Applets

- **Java**: High-level programming language developed by Sun Microsystems
- **Java sandbox**: Confines Java applet actions to a set of rules defined by the security model
- **Untrusted Java applets**: Applets not established as secure

Security for Client Computers-

JavaScript

- **JavaScript**: Scripting language developed by Netscape to enable Web page designers to build active content
- Can be used for attacks by
  - Executing code that destroys client’s hard disk
  - Disclosing e-mail stored in client mailboxes
  - Sending sensitive information to attacker’s Web server

Security for Client Computers-

ActiveX Controls

- **ActiveX Controls**: Object containing programs and properties that Web designers place on Web pages
  - Common programming languages used
    - C++ and Visual Basic
  - Actions cannot be halted once they begin execution
Example: Internet Explorer ActiveX Control Warning Message

Security for Client Computers- Viruses, Worms, and Antivirus Software

- **Virus**: Software that attaches itself to another program and can cause damage when host program is activated
- **Worm**: Virus that replicates itself on the computer that it infects
- **Macro virus**: Type of virus coded as a small program (macro) and is embedded in a file
- **Antivirus software**: Detects viruses and worms

Security for Client Computers- Steganography

- Describes process of hiding information within another piece of information
- Provides way of hiding an encrypted file within another file
- Messages hidden using steganography are difficult to detect

Protecting Client Computers- Digital Certificates 1

- A program embedded in a Web page that
  - Verifies that the sender or Web site is who or what it claims to be
- Signed code or messages
  - Provide proof that the holder is the person identified by the certificate
- Certification authority (CA)
  - Issues digital certificates

Example: Amazon.com’s Digital Certificate

Protecting Client Computers- Digital Certificates 2

- Main elements included:
  - Certificate owner’s identifying information
  - Certificate owner’s public key
  - Dates between which the certificate is valid
  - Serial number of the certificate
  - Name of the certificate issuer
  - Digital signature of the certificate issuer
Communication Channel Security

- Secrecy
  - Prevention of unauthorized information disclosure
  - Privacy is the protection of individual rights to nondisclosure
- Sniffer programs
  - Provide means to record information passing through a computer or router that is handling Internet traffic

Communication Channel Security - Integrity Threats

- Exists when an unauthorized party can alter a message stream of information
- Cybervandalism
  - Electronic defacing of an existing Web site’s page
- Masquerading or spoofing
  - Pretending to be someone you are not
- Domain name servers (DNSs)
  - Computers on the Internet that maintain directories that link domain names to IP addresses

Communication Channel Security - Necessity Threats

- Purpose is to disrupt or deny normal computer processing
- Denial of Service attacks
  - Remove information altogether or
  - Delete information from a transmission or file

Communication Channel Security - Threats to Wireless Networks

- Wardrivers
  - Attackers drive around using their wireless-equipped laptop computers to search for accessible networks
- Warchalking
  - When wardrivers find an open network they sometimes place a chalk mark on the building

Protecting Communication Channel - Encryption Solutions

- Encryption
  - Using a mathematically based program and a secret key to produce a string of characters that is unintelligible
- Cryptography
  - Science that studies encryption

Protecting Communication Channel - Encryption Algorithms

- Encryption
  - The coding of information by using a mathematically based program and secret key
- Encryption program
  - Program that transforms normal text into cipher text
- Decryption program
  - A type of encryption reversing procedure
**Protecting Communication Channel - Hash Coding**

- Process that uses a hash algorithm to calculate a number from a message of any length
- Good hash algorithms
  - Designed so that probability of two different messages resulting in same hash value is small
- Convenient way to tell whether a message has been altered in transit

**Protecting Communication Channel - Asymmetric Encryption1**

- Encodes messages by using two mathematically related numeric keys
  - Public key
    - Freely distributed to the public at large
  - Private key
    - Belongs to the key owner, who keeps the key secret

**Protecting Communication Channel - Asymmetric Encryption2**

- Pretty Good Privacy (PGP)
  - One of the most popular technologies used to implement public-key encryption
  - Set of software tools that
    - Can use several different encryption algorithms to perform public-key encryption
    - Can be used to encrypt their e-mail messages

**Protecting Communication Channel - Symmetric Encryption**

- Encodes message with one of several available algorithms that use a single numeric key
  - Data Encryption Standard (DES): Set of encryption algorithms adopted by the U.S. government for encrypting sensitive information
  - Triple Data Encryption Standard
    - Offers good protection
    - Cannot be cracked even with today’s supercomputers

**Comparing Asymmetric and Symmetric Encryption Systems**

- Public-key (asymmetric): Systems provide several advantages over private-key (symmetric) encryption methods
- Secure Sockets Layer (SSL): protocol that provides secure information transfer through the Internet. SSL secures connections between two Computers
- S-HTTP: Sends individual messages securely. Extension of “http”

**Protecting Communication Channel - Public-key Encryption**

- Diagram illustrating the process of public-key encryption.
Ensuring Transaction Integrity with Hash Functions

- Integrity violation
  - Occurs whenever a message is altered while in transit between the sender and receiver
- Hash algorithms are **one-way functions**
  - There is no way to transform the hash value back to original message
- Message digest
  - Small integer number that summarizes the encrypted information

Ensuring Transaction Integrity with Digital Signatures

- Hash algorithm
  - Anyone could
    - Intercept a purchase order
    - Alter the shipping address and quantity ordered
    - Re-create the message digest
    - Send the message and new message digest on to the merchant
- Digital signature
  - An encrypted message digest

Sending and Receiving a Digitally Signed Message

Security for Server Computers

- Web server
  - Can compromise secrecy if it allows automatic directory listings
  - Can compromise security by requiring users to enter a username and password
- Dictionary attack programs
  - Cycle through an electronic dictionary, trying every word in the book as a password

Other Programming Threats

- Buffer
  - An area of memory set aside to hold data read from a file or database
- Buffer overrun
  - Occurs because the program contains an error or bug that causes the overflow
- Mail bomb
  - Occurs when hundreds or even thousands of people each send a message to a particular address

Protecting the web server—Firewalls

- Computer and software combination installed at the Internet entry point of a networked system
- Provides a defense between
  - Network to be protected and the Internet, or other network that could pose a threat
- All corporate communication to and from Internet flows through firewalls
Protecting the web server - Firewalls2

- Characteristics
  - All traffic from inside to outside and from outside to inside the network must pass through firewall
  - Only authorized traffic is allowed to pass
  - Firewall itself is immune to penetration
- Trusted
  - Networks inside the firewall
- Untrusted
  - Networks outside the firewall

Protecting the web server - Firewalls3

- Packet-filter firewalls: Examine data flowing back and forth between trusted network and the Internet
- Gateway servers: Firewalls that filter traffic based on the application requested
- Proxy server firewalls: Firewalls that communicate with the Internet on the private network’s behalf

Organizations that Promote Computer Security

- Computer Emergency Response Team
  - Responds to thousands of security incidents each year
  - Helps Internet users and companies become more knowledgeable about security risks
  - Posts alerts to inform Internet community about security events

Other Organizations

- SANS Institute
  - A cooperative research and educational organization
- Internet Storm Center
  - Web site that provides current information on the location and intensity of computer attacks
- Microsoft Security Research Group
  - Privately sponsored site that offers free information about computer security issues

Computer Forensics and Ethical Hacking

- Computer forensics experts
  - Hired to probe PCs and locate information that can be used in legal proceedings
- Computer forensics
  - The collection, preservation, and analysis of computer-related evidence

Summary

- Assets that companies must protect: Client computers; Computer communication channels; Web servers (susceptible to security threats)
- Communication channels, in general, and the Internet, in particular are especially vulnerable to attacks
- Encryption: Provides secrecy
Next week

User Experience in E-commerce
  • Personalisation
  • Usability