Information Systems and Network Security

Chapter 16

- **E-Commerce Security**

-Sanket Mohan Pandhare

E-Commerce

- E-commerce
  - Use of the internet to transact business.
  - Many parties are involved in online business like banks, payment gateways, sellers, transport companies, currier companies, etc.
  - Chain of People to deliver the product from Manufacturer to the Buyer.
  - B2B, B2C, C2C and etc.

E-Commerce: Challenges

- Trusting others electronically
  - E-Commerce infrastructure
- Security threats – the real threats and the perceptions
- Network connectivity and availability issues
  - Better architecture and planning
- Global economy issues
  - Flexible solutions

E-Commerce: Challenges

- Trusting others electronically
  - Authentication
  - Handling of private information
  - Message integrity
  - Digital signatures and non-repudiation
  - Access to timely information

Three components to security

- Three perspectives
  - User’s point of view
  - Server’s point of view
  - Both parties
- Three parts
  - Client-side security
  - Server-side security
  - Document confidentiality

Electronic Commerce Threats

- Client Threats
  - Active Content
    - Java applets, Active X controls, JavaScript, and VBScript
    - Programs that interpret or execute instructions embedded in downloaded objects
    - Malicious active content can be embedded into seemingly innocuous Web pages
    - Cookies remember user names, passwords, and other commonly referenced information

Client Side Security

- Client-side security deals with the security from the customer's desktop system to the e-commerce server.
- This part of the system includes the customer's computer and browser software and the communications link to the server
- Within this part of the system, there are several issues:
  - The protection of information in transit between the customer's system and the server
  - The protection of information that is saved to the customer's system
  - The protection of the fact that a particular customer made a particular order

Communications Security

- Communications security for e-commerce applications covers the security of information that is sent between the customer's system and the e-commerce server.
- EXAMPLE
  - sensitive information such as credit card numbers or site passwords.
  - confidential information that is sent from the server to the customer's system, such as customer files.

Saving Information on the Client System

Why so Important

- In order to conduct commerce across the Internet using Web browsers and Web servers, the servers must remember what the consumer is doing (this includes information about the consumer, what they are ordering, and any passwords the consumer may have used to access secured pages).
- One way (and the most common way) that a Web server can do this is to usercookies

Internet Cookie

- A *cookie* is a small amount of information that is stored on the client system by the Web server.
- Only the Web server that placed the cookie is supposed to retrieve it, and the cookie should expire after some period of time (usually less than a year).
- A cookie is a piece of text that a Web server can store on a user's hard disk.
- Cookies allow a Web site to store information on a user's machine and later retrieve it. The pieces of information are stored as **name-value pairs**.
- Cookies can be in clear text or they can be encrypted.
- Cookies can be used to track anything for the Web server.

- •Example:
  - UserID A9A3BECE0563982D www.goto.com/

Security Threats in the E-commerce Environment

- **Three key points of vulnerability**:
  - Client
  - Server
  - Communications channel

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

Reasons for E-Commerce Crimes

- Six major reasons why is it difficult for e-tailers to stop cyber criminals and fraudsters:
  1. Strong EC security makes online shopping inconvenient for customers
  2. Lack of cooperation from credit card issuers and foreign ISPs
  3. Online shoppers do not take necessary precautions to avoid becoming a victim
  4. IS design and security architecture are vulnerable to attack
  5. Software vulnerabilities (bugs) are a huge security problem
  6. Managers sometimes ignore due standards of care

Stopping E-Commerce Crimes

- **Information assurance (IA)**

  The protection of information systems against unauthorized access to or modification of information whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats

- **Human firewalls**

  Methods that filter or limit people's access to critical business documents

Stopping E-Commerce Crimes

- **Application firewalls**

  Specialized tools designed to increase the security of Web applications

- **Common (security) vulnerabilities and exposures (CVE)**

  Publicly known computer security risks, which are collected, listed, and shared by a board of security-related organizations (cve.mitre.org)

Stopping E-Commerce Crimes

- **Vulnerability**

  Weakness in software or other mechanism that threatens the confidentiality, integrity, or availability of an asset (recall the CIA model). It can be directly used by a hacker to gain access to a system or network

- **Risk**

  The probability that a vulnerability will be known and used.

Stopping E-Commerce Crimes

- **Exposure**

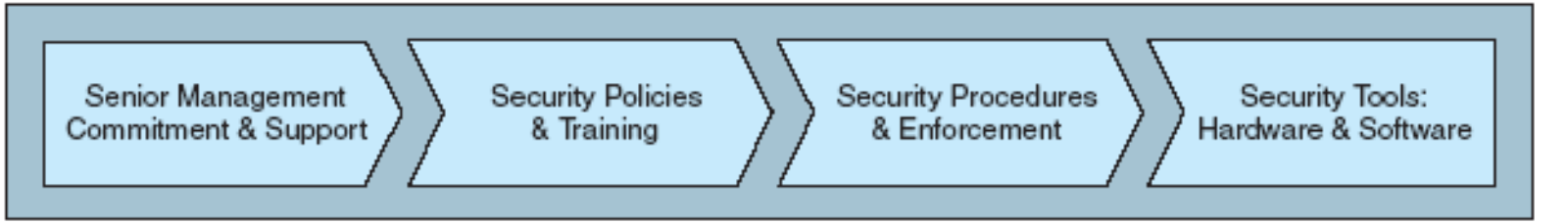
  The estimated cost, loss, or damage that can result if a threat exploits a vulnerability

- **Standard of due care**

  Care that a company is reasonably expected to take based on the risks affecting its EC business and online transactions

Enterprisewide E-Commerce Security and Privacy Model

EXHIBIT 11.6 Enterprisewide EC Security and Privacy Model



Enterprisewide E-Commerce Security and Privacy Model

- **Senior Management Commitment and Support**
- **EC Security Policies and Training**
  - To avoid violating privacy legislation when collecting confidential data, policies need to specify that customers:
    - Know they are being collected
    - Give permission, or “opt in,” for them to be collected
    - Have some control over how the information is used
    - Know they will be used in a reasonable and ethical manner
  - **Acceptable use policy (AUP)**

    Policy that informs users of their responsibilities when using company networks, wireless devices, customer data, and so forth

Enterprisewide E-Commerce Security and Privacy Model

- **EC Security Procedures and Enforcement**
  - **Business Impact Analysis (BIA)**

    An exercise that determines the impact of losing the support of an EC resource to an organization and establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems
- **Security Tools: Hardware and Software**

Securing E-Commerce Networks

- The selection and operation of technologies that ensure network security should be based on:
  - Defense in depth
  - Need-to-access basis
    - **policy of least privilege (POLP)**

      Policy of blocking access to network resources unless access is required to conduct business
  - Role-specific security
  - Monitoring
  - Patch management
  - Incident response team (IRT)

Securing E-Commerce Networks

- **FIREWALLS**
  - **Firewall**

    A single point between two or more networks where all traffic must pass (choke point); the device authenticates, controls, and logs all traffic
  - Firewalls can be designed to protect against:
    - Remote login
    - Application backdoors
    - SMTP session hijacking
    - Viruses
    - Spam

Securing E-Commerce Networks

- **Packet-filtering routers**

  Firewalls that filter data and requests moving from the public Internet to a private network based on the network addresses of the computer sending or receiving the request

- **Packet filters**

  Rules that can accept or reject incoming packets based on source and destination addresses and the other identifying information

Securing E-Commerce Networks

- **Demilitarized Zone (DMZ)**

  Network area that sits between an organization's internal network and an external network (Internet), providing physical isolation between the two networks that is controlled by rules enforced by a firewall

- **Personal firewall**

  A network node designed to protect an individual user's desktop system from the public network by monitoring all the traffic that passes through the computer's network interface card

Securing E-Commerce Networks

- **Virtual private network (VPN)**

  A network that uses the public Internet to carry information but remains private by using encryption to scramble the communications, authentication to ensure that information has not been tampered with, and access control to verify the identity of anyone using the network

- **Protocol tunneling**

  Method used to ensure confidentiality and integrity of data transmitted over the Internet, by encrypting data packets, sending them in packets across the Internet, and decrypting them at the destination address

Securing E-Commerce Networks

- **Intrusion Detection Systems (IDSs)**

  A special category of software that can monitor activity across a network or on a host computer, watch for suspicious activity, and take automated action based on what it sees

- **Honeynet**

  A network of honeypots

- **Honeypot**

  Production system (e.g., firewalls, routers, Web servers, database servers) that looks like it does real work, but which acts as a decoy and is watched to study how network intrusions occur

Summary

- Businesses are growing exponentially
- E-Commerce is dependency between multiple servers, payment gateways and many more.
- Once you secure every end the infringement is quiet impossible.
- Enterprisewide E-Commerce Security and Privacy Model
- Network is most critical part
- Securing eCommerce Network