Topic 4

- Source: .ppt slides from instructor resources
  - Ch 4: Building an E-commerce Site
  - Ch 5: Security and Encryption

Right-Sizing a Web Site.

class Discussion

- What are the factors you should take into account when sizing a Web site’s infrastructure?
- How does OPERA use a queuing model?
- Why did eBay turn to IBM’s OPERA application?
- Why is peak usage an important factor to consider?
- What did eBay discover from its use of OPERA?

Building an E-commerce Site: A Systematic Approach

- Two most important management challenges in building a successful e-commerce site are:
  - Developing a clear understanding of business objectives
  - Knowing how to choose the right technology to achieve those objectives

Pieces of the Site-Building Puzzle

- Main areas where you will need to make decisions in building a site include:
  - Human resources and organizational capabilities—creating a team that has the skill set to build and manage a successful site
  - Hardware
  - Software
  - Telecommunications
  - Site design
Pieces of the E-commerce Site-Building Puzzle

Web Site Systems Development Life Cycle

The Systems Development Life Cycle

- Systems Development Life Cycle (SDLC) is a methodology for understanding the business objectives of a system and designing an appropriate solution.
- Five major steps in the SDLC are:
  - Systems analysis/planning
  - Systems design
  - Building the system
  - Testing
  - Implementation

System Analysis/Planning: Identifying Business Objectives, System Functionality, and Information Requirements

- Business objectives: a list of capabilities you want your site to have
- System functionalities: a list of the types of information system capabilities you will need to achieve your business objectives
- Information requirements: the information elements that the system must produce in order to achieve the business objectives

Systems Analysis: Business Objectives, System Functionality, and Information Requirements for a Typical E-commerce Site

<table>
<thead>
<tr>
<th>BUSINESS OBJECTIVE</th>
<th>SYSTEM FUNCTIONALITY</th>
<th>INFORMATION REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>List product details, prices</td>
<td>Product catalog</td>
<td>Product description, color, size, availability, price, and shipping information</td>
</tr>
<tr>
<td>Display product reviews</td>
<td>Product review system</td>
<td>Product review details, rating, and comments</td>
</tr>
<tr>
<td>Allow customers to track orders</td>
<td>Order tracking system</td>
<td>Order status, delivery date, and estimated time of arrival</td>
</tr>
<tr>
<td>Allow customers to communicate with support</td>
<td>Support chat system</td>
<td>Customer query details, response time, and satisfaction rating</td>
</tr>
<tr>
<td>Allow customers to change their payment information</td>
<td>Payment system</td>
<td>Payment method, card number, and expiration date</td>
</tr>
<tr>
<td>Allow customers to personalize their shopping experience</td>
<td>Personalization system</td>
<td>Customer preferences, recommended products, and personalized offers</td>
</tr>
<tr>
<td>Allow customers to search for products</td>
<td>Search system</td>
<td>Search terms, search results, and product categories</td>
</tr>
<tr>
<td>Allow customers to share their experiences with friends</td>
<td>Social sharing system</td>
<td>Share links, comments, and social media integration</td>
</tr>
</tbody>
</table>

Systems Design: Hardware and Software Platforms

- System design specification: a description of the main components of a system and their relationship to one another
- System design can be broken down into two parts:
  - Logical design
  - Physical design
Building the System: In-House versus Outsourcing

- Outsourcing: hiring an outside vendor to provide services involved in building the site
- The build your own versus outsourcing decision:
  - Build your own requires team with diverse skill set; choice of software tools; both risks and possible benefits
- Host your own versus outsourcing
  - Hosting: hosting company is responsible for ensuring site is accessible 24/7, for monthly fee
  - Co-location: firm purchases or leases a Web server (with control over its operation), but server is located in at vendor's physical facility

Insight on Business: Outsourcing Makes Sense When DIY Is No Bargain

Class Discussion

- What's wrong with building your own Web site?
- Why did Big Al's home-grown solution fail? Why didn’t they just fix it themselves?
- How systems are involved in Big Al's Web site?
- What are some of the risks of outsourcing your Web site?

Choices in Building and Hosting

Testing, Implementation, and Maintenance

- Testing: Includes unit testing, system testing, and acceptance testing
- Implementation and maintenance:
  - Maintenance is ongoing
  - Benchmarking: process by which site is compared to those of competitors in terms of response speed, quality of layout, and design
Factors in Web Site Optimization

Figure 4.7, Page 205

Page Delivery
- Content delivery networks
- Edge caching
- Bandwidth

Page Generation
- Server response time
- Device-based accelerators
- Efficient resource allocation
- Resource utilization thresholds
- Monitoring site performance

Page Content
- Optimize HTML
- Optimize images
- Site architecture
- Efficient page style

Simple versus Multi-tiered Web Site Architecture

- System architecture: refers to the arrangement of software, machinery, and tasks in an information system needed to achieve a specific functionality
- Two-tier architecture: Web server responds to requests for Web pages and a database server provides backend data storage
- Multi-tier architecture: Web server is linked to a middle-tier layer that typically includes a series of application servers that perform specific tasks, as well as to a backend layer of existing corporate systems

Two-Tier E-commerce Architecture

Figure 4.9(a), Page 207

User requests for pages → Web Server → Dynamic Content Database

(a) Two-tier Architecture
In a two-tier architecture, a Web server responds to requests for Web pages and a database server provides backend data storage.

Multi-tier E-commerce Architecture

Figure 4.9(b), Page 207

Web Server Layer
- Web servers

Middle-tier Layer
- E-commerce Servers
- Application Servers
- Database Servers
- Ad Servers
- Mail Servers

Backend Layer
- Corporate applications
- Financial applications
- Production MRP
- Enterprise systems
- HR systems

(b) Multi-tier Architecture
In a multi-tier architecture, a Web server is linked to a middle-tier layer that typically includes a series of application servers that perform specific tasks, as well as to a backend layer of existing corporate systems.

Web Server Software

- All e-commerce sites require basic Web server software to answer HTTP requests from customers
- Apache is the leading Web server software; works only with UNIX operating systems
- Microsoft’s Internet Information Server (IIS) is the second major Web server software

Basic Functionality Provided by Web Servers

Table 4.3, Page 209

<table>
<thead>
<tr>
<th>FUNCTIONALITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing of HTTP requests</td>
<td>Receive and respond to client requests for HTML pages.</td>
</tr>
<tr>
<td>Security services (SSL)</td>
<td>Verify username and password, process certificates and public/private key information.</td>
</tr>
<tr>
<td>File transfer protocol</td>
<td>Permit transfer of very large files from server to server.</td>
</tr>
<tr>
<td>Search engine</td>
<td>Search the site for specific keywords or search capabilities.</td>
</tr>
<tr>
<td>Data capture</td>
<td>Log file of all visits, time, duration, and referral source.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Ability to send, receive, and store e-mail messages.</td>
</tr>
<tr>
<td>Site management tools</td>
<td>Calculate and display key site statistics, such as unique visitors, page requests, and origin of requests.</td>
</tr>
</tbody>
</table>
Site Management Tools

- All Web servers contain basic site management tools that verify that links on pages are still valid and also identify orphan files.
- Additional site management software and services such as those provided by Webtrends can be purchased.

Dynamic Page Generation Tools

- Dynamic page generation: contents of Web page are stored as objects in a database rather than being hard-coded in HTML, and are fetched when needed from database.
- Tools include CGI (Common Gateway Interface), ASP (Active Server Pages), JSP (Java Server Pages), etc.
- Lowers menu costs, permits easy online marketing segmentation, and enables cost-free price discrimination.

Application Servers

- Web application servers: software programs that provide specific business functionality required of a Web site.
- Are an example of middleware software.
- A number of different types available, providing a variety of functionality.

Application Servers and Their Functions

<table>
<thead>
<tr>
<th>APPLICATION SERVER</th>
<th>FUNCTIONALITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog display</td>
<td>Provides a database for product descriptions and prices.</td>
</tr>
<tr>
<td>Transaction processing (shopping cart)</td>
<td>Accepts orders and credit payments.</td>
</tr>
<tr>
<td>User server</td>
<td>Creates and serves running lists and manages e-mail marketing campaigns.</td>
</tr>
<tr>
<td>Proxy server</td>
<td>Monitors and controls access to real-time server; implements firewall protection.</td>
</tr>
<tr>
<td>Mail server</td>
<td>Manages incoming and outgoing e-mail.</td>
</tr>
<tr>
<td>Authorized server</td>
<td>Stores and delivers streaming media content.</td>
</tr>
<tr>
<td>Cross server</td>
<td>Creates an environment for users to interact with each other.</td>
</tr>
<tr>
<td>News server</td>
<td>Provides connectivity and delivers Internet news feeds.</td>
</tr>
<tr>
<td>Fax server</td>
<td>Provides fax reception and sending using a Web server.</td>
</tr>
<tr>
<td>Groups server</td>
<td>Creates group-oriented environments for online collaboration.</td>
</tr>
<tr>
<td>Entitlement server</td>
<td>Stores customer's product, and price information.</td>
</tr>
<tr>
<td>Ad server</td>
<td>Maintains a Web-enabled database of advertising banners that permits customized and personalized display of advertisements based on user behavior and characteristics.</td>
</tr>
<tr>
<td>Auction server</td>
<td>Provides a transaction environment for conducting online auctions.</td>
</tr>
<tr>
<td>E2E Server</td>
<td>Implements buy, sell, and trade marketplaces for commercial transactions.</td>
</tr>
</tbody>
</table>

E-commerce Merchant Server Software Functionality

- Provides the basic functionality needed for online sales, including:
  - Online catalog
  - Shopping cart
  - Credit card processing

Merchant Server Software Packages (E-commerce Suites)

- Offer integrated environment that provides functionality and capabilities needed to develop sophisticated, customer-centric site.
- Key factors to consider in choosing include:
  - Functionality
  - Support for different business models
  - Business process modeling tools
  - Visual site management tools and reporting
  - Performance and scalability
  - Connectivity to existing business systems
  - Compliance with standards
  - Global and multicultural capability
  - Local sales tax and shipping rules.
Choosing the Hardware for an E-commerce Site

- Hardware platform: refers to all the underlying computing equipment that the system uses to achieve e-commerce functionality
- Objective to have enough platform capacity to meet peak demand but not so much that you are wasting money
- Important to understand the different factors that affect speed, capacity, and scalability of a site

Right-Sizing Your Hardware Platform: The Demand Side

- Demand that customers put on a site the most important factor affecting the speed of a site
- Factors involved in demand include:
  - Number of simultaneous users in peak periods
  - Nature of customer requests (user profile)
  - Type of content (dynamic versus static Web pages)
  - Required security
  - Number of items in inventory
  - Number of page requests
  - Speed of legacy applications

Factors in Right-sizing an E-commerce Platform

- Table 4.6, Page 217

Degradation in Performance as Number of Users Increases

- Figure 4.12 (a), Page 218

Degradation in Performance as Number of Users Increases

- Figure 4.12 (b), Page 218

The Relationship of Bandwidth to Hits

- Figure 4.14, Page 221

Right-Sizing Your Hardware Platform: The Supply Side

- Scalability: refers to the ability of a site to increase in size as demand warrants
- Ways to scale hardware:
  - Vertically: increase the processing power of individual components
  - Horizontally: employ multiple computers to share the workload
  - Improve processing architecture

Vertical and Horizontal Scaling Techniques

<table>
<thead>
<tr>
<th>TECHNIQUE</th>
<th>APPLICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a faster computer</td>
<td>Applies to edge servers, presentation servers, data servers, etc.</td>
</tr>
<tr>
<td>Create a cluster of computers</td>
<td>Use computers in parallel to balance loads</td>
</tr>
<tr>
<td>Use appliance servers</td>
<td>Special-purpose computers optimized for their task</td>
</tr>
<tr>
<td>Segment workload</td>
<td>Segment incoming work to specialized computers</td>
</tr>
<tr>
<td>Batch requests</td>
<td>Combine related requests for data into groups, process as a group</td>
</tr>
<tr>
<td>Manage connections</td>
<td>Reduce connections between processes and computers to a minimum</td>
</tr>
<tr>
<td>Aggregate user data</td>
<td>Aggregate user data from legacy applications in single data pools</td>
</tr>
<tr>
<td>Cache</td>
<td>Store frequently used data in cache rather than on the disk</td>
</tr>
</tbody>
</table>

Vertically Scaling a System

Figure 4.15, Page 222

Horizontally Scaling a System

Figure 4.16, Page 223

Improving the Processing Architecture of Your Site

<table>
<thead>
<tr>
<th>ARCHITECTURE IMPROVEMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separate static content from dynamic content.</td>
<td>Use specialized servers for each type of workload.</td>
</tr>
<tr>
<td>Cache static content.</td>
<td>Increase RAM to the gigabyte range and store static content in RAM.</td>
</tr>
<tr>
<td>Cache database lookup tables.</td>
<td>Cache tables used to look up database records.</td>
</tr>
<tr>
<td>Consolidate business logic on dedicated servers.</td>
<td>Put shopping cart, credit card processing, and other CPU-intensive activity on dedicated servers.</td>
</tr>
<tr>
<td>Optimize ASP code.</td>
<td>Examine your code to ensure it is operating efficiently.</td>
</tr>
<tr>
<td>Optimize the database schema.</td>
<td>Examine your database search times and take steps to reduce access times.</td>
</tr>
</tbody>
</table>

Web Site Design: Basic Business Considerations

- To achieve basic business functionality of a Web site, need to be aware of design guidelines and software tools that can build active content and functionality
- Poorly designed Web sites drive customers away
E-commerce Web Site Features that Annoy Customers

Figure 4.17, Page 225


<table>
<thead>
<tr>
<th>Feature</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requiring the installation of extra software to use the site</td>
<td>98.4%</td>
</tr>
<tr>
<td>Difficult to use</td>
<td>97.8%</td>
</tr>
<tr>
<td>Confusing navigation</td>
<td>97.4%</td>
</tr>
<tr>
<td>Requirement to register and log in before seeing the product</td>
<td>97.3%</td>
</tr>
<tr>
<td>Slow loading pages</td>
<td>96.3%</td>
</tr>
<tr>
<td>What customers said is out of date</td>
<td>93.4%</td>
</tr>
<tr>
<td>Ineffective site content test</td>
<td>90.3%</td>
</tr>
<tr>
<td>Inability to see tomorrow’s hours</td>
<td>87.4%</td>
</tr>
<tr>
<td>No contact information available (Privacy-only)</td>
<td>75.1%</td>
</tr>
<tr>
<td>Double-click unnecessary applauded or advertised</td>
<td>72.9%</td>
</tr>
<tr>
<td>Technical errors</td>
<td>55.9%</td>
</tr>
<tr>
<td>Poor appearance</td>
<td>54.8%</td>
</tr>
<tr>
<td>Miss or other ads that pop up automatically</td>
<td>52.3%</td>
</tr>
<tr>
<td>Delaying a sneeze for a link</td>
<td>26.4%</td>
</tr>
</tbody>
</table>

The Eight Most Important Factors in Successful E-commerce Site Design

Table 4.10, Page 226

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>Pages that work, load quickly, and point the customer toward your product offer</td>
</tr>
<tr>
<td>Informational</td>
<td>Links that customers can easily find to discover more about you and your products</td>
</tr>
<tr>
<td>Ease of use</td>
<td>Simple feel-proof navigation</td>
</tr>
<tr>
<td>Redundant navigation</td>
<td>Alternative navigation to the same content</td>
</tr>
<tr>
<td>Ease of purchase</td>
<td>One or two clicks to purchase</td>
</tr>
<tr>
<td>Multi-browser functionality</td>
<td>Site works with the most popular browsers</td>
</tr>
<tr>
<td>Simple graphics</td>
<td>Avoids distracting, obnoxious graphics and sounds that the user cannot control</td>
</tr>
<tr>
<td>Legible text</td>
<td>Avoids backgrounds that distort text or make it illegible</td>
</tr>
</tbody>
</table>

Tools for Interactivity and Active Content

- CGI (Common Gateway Interface): Set of standards for communication between a browser and a program running on a server that allows for interaction between the user and the server
- ASP (Active Server Pages): Enables programmers using Microsoft’s IIS package to build dynamic pages
- Java: Allows programmers to create interactivity and active content on the client computer

Tools for Interactivity and Active Content (cont’d)

- ActiveX: Programming language invented by Microsoft to compete with Java
- VBScript: Programming language invented by Microsoft to compete with JavaScript
- ColdFusion: An integrated server-side environment for developing interactive Web applications

Insight on Technology: Using Ajax and Flash For Fast Forms and High-Speed Interactivity

Class Discussion

- What is Ajax? How does it work?
- Compare Ajax to the traditional client/server Web model
- How does Google Maps use Ajax?
- What are some alternative ways to achieve the same results as Ajax?
Personalization Tools

- **Personalization**: Ability to treat people based on their personal qualities and prior history with your site
- **Customization**: Ability to change the product to better fit the needs of the customer
- Cookies the primary method for achieving personalization and customization

The Information Policy Set

- **Privacy policy**: Set of public statements declaring how site will treat customers' personal information that is gathered by site
- **Accessibility rules**: Set of design objectives that ensure disabled users can access site

Chapter 5: Security and Encryption

The E-commerce Security Environment: The Scope of the Problem

- Overall size of cybercrime unclear; amount of losses significant but stable; individuals face new risks of fraud that may involve substantial uninsured losses
  - Symantec: Over 50 overall attacks a day against business firms between July 2004–June 2005
  - 2005 Computer Security Institute survey
    - 56% of respondents had detected breaches of computer security within last 12 months and 91% of these suffered financial loss as a result
    - Over 35% experienced denial of service attacks
    - Over 75% detected virus attacks

The E-commerce Security Environment

**Dimensions of E-commerce Security**

- **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 unauthorized party
- **Nonrepudiation**: 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
- **Confidentiality**: ability to ensure that messages and data are available only to those authorized to view them
- **Privacy**: ability to control use of information a customer provides about himself or herself to merchant
- **Availability**: ability to ensure that an e-commerce site continues to function as intended
Customer and Merchant Perspectives on the Different Dimensions of E-commerce Security

<table>
<thead>
<tr>
<th>DIMENSIONS</th>
<th>CUSTOMER’S PERSPECTIVE</th>
<th>MERCHANT’S PERSPECTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>Has information I transmit or receive been altered?</td>
<td>Has data on the site been altered without authorization? Is data being removed from customers valid?</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>Can a party to an action be later denied taking the action?</td>
<td>Can a customer deny ordering products?</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Who am I dealing with? How can I be assured that the person or entity is who they claim to be?</td>
<td>What is the real identity of the customer?</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Can I control what is to be received by the intended recipient read my messages?</td>
<td>Are messages or confidential data accessible to anyone other than those authorized to see them?</td>
</tr>
<tr>
<td>Privacy</td>
<td>Can I control the use of information about myself transmitted to an e-commerce merchant?</td>
<td>What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers confidential?</td>
</tr>
<tr>
<td>Availability</td>
<td>Can I get access to the site?</td>
<td>Is the site operational?</td>
</tr>
</tbody>
</table>

Security Threats in the E-commerce Environment

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

Security Threats in the E-commerce Environment (cont’d)

- Most common threats:
  - Malicious code
  - Phishing
  - Hacking and cybervandalism
  - Credit card fraud/theft
  - Spoofing (pharming)
  - Denial of service attacks
  - Sniffing
  - Insider jobs
  - Poorly designed server and client software

A Typical E-commerce Transaction

Vulnerable Points in an E-commerce Environment
Malicious Code

- Viruses: computer program that has ability to replicate and spread to other files; most also deliver a "payload" of some sort (may be destructive or benign); include macro viruses, file-infecting viruses, and script viruses
- Worms: designed to spread from computer to computer
- Trojan horse: appears to be benign, but then does something other than expected
- Bots: can be covertly installed on computer; responds to external commands sent by the attacker

Phishing

- Any deceptive, online attempt by a third party to obtain confidential information for financial gain
  - Most popular type: e-mail scam letter
  - One of fastest growing forms of e-commerce crime

Hacking and Cybervandalism

- Hacker: Individual who intends to gain unauthorized access to computer systems
- Cracker: Used to denote hacker with criminal intent (two terms often used interchangeably)
- Cybervandalism: Intentionally disrupting, defacing or destroying a Web site
- Types of hackers include:
  - White hats
  - Black hats
  - Grey hats

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

Spoofing (Pharming)

- Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
- Threatens integrity of site; authenticity

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
Other Security Threats

- Sniffing: Type of eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network
- Insider jobs: Single largest financial threat
- Poorly designed server and client software: Increase in complexity of software programs has contributed to an increase in vulnerabilities that hackers can exploit

Technology Solutions

- Protecting Internet communications (encryption)
- Securing channels of communication (SSL, S-HTTP, VPNs)
- Protecting networks (firewalls)
- Protecting servers and clients

Tools Available to Achieve Site Security

Figure 5.7, Page 269

Protecting Internet Communications: Encryption

- Encryption: The process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and receiver
- Purpose: Secure stored information and information transmission
- Provides:
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality

Symmetric Key Encryption

- Also known as secret key encryption
- Both the sender and receiver use the same digital key to encrypt and decrypt message
- Requires a different set of keys for each transaction
- Data Encryption Standard (DES): Most widely used symmetric key encryption today; uses 56-bit encryption key; other types use 128-bit keys up through 2048 bits

Public Key Encryption

- Public key cryptography solves symmetric key encryption problem of having to exchange secret key
- Uses two mathematically related digital keys – public key (widely disseminated) and private key (kept secret by owner)
- Both keys are used to encrypt and decrypt message
- Once key is used to encrypt message, same key cannot be used to decrypt message
- For example, sender uses recipient’s public key to encrypt message; recipient uses his/her private key to decrypt it
Public Key Cryptography – A Simple Case

1. Original message
   Sender: Buy Cisco @ $25
2. Recipient receives public key
   Recipient: 10101011100001
3. Message encrypted in cipher text
   Internet
4. Recipient's private key
   Recipient: Buy Cisco @ $25

Public Key Encryption using Digital Signatures and Hash Digests

• Application of hash function (mathematical algorithm) by sender prior to encryption produces hash digest that recipient can use to verify integrity of data
• Double encryption with sender’s private key (digital signature) helps ensure authenticity and nonrepudiation

Digital Envelopes

• Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time) and symmetric key encryption (faster, but more secure)
• Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key

Digital Certificates and Public Key Infrastructure (PKI)

• Digital certificate: Digital document that includes:
  - Name of subject or company
  - Subject’s public key
  - Digital certificate serial number
  - Expiration date
  - Issuance date
  - Digital signature of certification authority (trusted third party institution) that issues certificate
  - Other identifying information
• Public Key Infrastructure (PKI): refers to the CAs and digital certificate procedures that are accepted by all parties
Digital Certificates and Certification Authorities

- PKI applies mainly to protecting messages in transit
- PKI is not effective against insiders
- Protection of private keys by individuals may be haphazard
- No guarantee that verifying computer of merchant is secure
- CAs are unregulated, self-selecting organizations

Insight on Technology: Advances in Quantum Cryptography May Lead to the Unbreakable Key

• Why are existing encryption systems over time more vulnerable?
• What is quantum encryption?
• What is the weakness of a symmetric key system (even one based on quantum techniques)?
• Would quantum-encrypted messages be immune to the growth in computing power?

Securing Channels of Communication

• Secure Sockets Layer (SSL): Most common form of securing channels of communication; used to establish a secure negotiated session (client-server session in which URL of requested document, along with contents, is encrypted)
• S-HTTP: Alternative method; provides a secure message-oriented communications protocol designed for use in conjunction with HTTP
• Virtual Private Networks (VPNs): Allow remote users to securely access internal networks via the Internet, using Point-to-Point Tunneling Protocol (PPTP)
### Firewalls and Proxy Servers

- **Figure 5.13, Page 283**

### Protecting Servers and Clients

- Operating system controls: Authentication and access control mechanisms
- Anti-virus software: Easiest and least expensive way to prevent threats to system integrity

### A Security Plan: Management Policies

- Steps in developing a security plan
  - Perform risk assessment: assessment of risks and points of vulnerability
  - Develop security policy: set of statements prioritizing information risks, identifying acceptable risk targets, and identifying mechanisms for achieving targets
  - Develop implementation plan: action steps needed to achieve security plan goals
  - Create security organization: in charge of security; educates and trains users, keeps management aware of security issues; administers access controls, authentication procedures and authorization policies
  - Perform security audit: review of security practices and procedures

### Developing an E-commerce Security Plan

- **Figure 5.14, Page 286**

### Insight on Business: Hiring Hackers to Locate Threats: Penetration Testing

- **Class Discussion**
  - Why would firms hire outsiders to crash its systems?
  - What are “grey” and “black” hats and why do firms avoid them as security testers?
  - Are penetration specialists like Johnny Long performing a public service or just making the situation worse?

### The Role of Laws and Public Policy

- New laws have granted local and national authorities new tools and mechanisms for identifying, tracing and prosecuting cybercriminals
  - National Infrastructure Protection Center – unit within National Cyber Security Division of Department of Homeland Security whose mission is to identify and combat threats against U.S. technology and telecommunications infrastructure
  - USA Patriot Act
  - Homeland Security Act
- Government policies and controls on encryption software
OECD Guidelines

- 2002 Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems and Networks has nine principles:
  - Awareness
  - Responsibility
  - Response
  - Ethics
  - Democracy
  - Risk assessment
  - Security design and implementation
  - Security management
  - Reassessment

ISO/IEC 17799:2005

- Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.
- The objectives outlined provide general guidance on the commonly accepted goals of information security management.
- ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:
  - Security policy;
  - Organization of information security;
  - Asset management;
  - Human resources security;
  - Physical and environmental security;
  - Communications and operations management;
  - Access control;
  - Information systems acquisition, development and maintenance;
  - Information security incident management;
  - Business continuity management;
  - Compliance.

Ref: http://www.computersecuritynow.com/presentation/
HISTORY 1

First published as DTI Code of Practice in UK
Re-branded and published as Version 1 of BS7799
published in Feb 1995

Not widely embraced - for various reasons, including:
- not flexible enough
- simplistic 'key control' approach
- other more pressing issues (eg: Y2K, EMU, etc)

HISTORY 2

- A major revision of BS7799 undertaken... Version TWO
  published in May 1999
- Formal certification and accreditation schemes are
  launched in the same year
- Supporting tools start to appear
- Fast track ISO initiative accelerated. First published as an
  ISO standard in Dec 2000
  in the same year.

WHAT IS HAPPENING NOW?

- Burst of activity in terms of uptake...
  - many organizations quote intent
  - same well on route to certification
  - some organizations already certified
  - significant worldwide take-up
  - massive increase in interest in general the issue itself
  - established as THE major standard for information security

WHY THE CHANGE?

- E-business... organizations seek security assurance in the new environment
- Major Consultancies... have invested very heavily... in the building of certified auditors...
- Potential major business processes is at risk
- The improved quality of the standard
- Y2K, EMU and other competing issues have been completed or scaled down

THE MARKET RISKS?

- What if your competitors are more advanced than you... consider what will happen if they become certified.
- They may then join the others in making certification a market differentiator. Obvious scenario of, for instance, a
  corporate customer choosing between two similar services (maybe e-business services) for which security
  is a concern...

YOUR OPTIONS

1) Ignore it
2) When creating a new policies/etc ensure they covers all ISO 17799 issues
3) Base all new policies and security directly on ISO 17799 and vigorously pursue compliance positioning
4) Press for full certification
ISO/IEC 27000 Series

• ISO has reserved the ISO/IEC 27000-series numbering for a range of information security management standards in similar fashion to the very successful ISO 9000-series quality assurance standards.

• ISO 27000 - vocabulary and definitions (terminology for all of these standards)
• ISO 27001 - the main Information Security Management System requirements standard (specification) against which organizations are formally certified
• ISO 27002 (currently known as ISO 17799 and formerly known as BS 7799 part 1) - this is the Code of Practice describing a comprehensive set of information security control objectives and a menu of best-practice security controls
• ISO 27003 - will be an implementation guide
• ISO 27004 - will be a new Information Security Management Metrics and Measurement standard to help measure the effectiveness of information security management system implementations.
• ISO 27005 - will be a new Information Security Risk Management standard (will replace the recently issued BS 7799 Part 3)
• ISO 27006 - will probably be a new standard: “Guidelines for information and communications technology disaster recovery services”