E-Commerce Strategies and Practices

Lesson 1: Electronic Commerce Foundations

- Inter-company commerce is business conducted between two different companies.
- Commerce is the exchange of goods and services for money.
- Electronic commerce is an integration of communication, transport, data management, and security capabilities that allow organizations to exchange information about the sale of goods and services.
  - Communication transport services support the transfer of information between the buyer and seller.
  - Data management services define the exchange format of the information.
  - Security mechanisms authenticate the source of information and guarantee its integrity and privacy.
- The two models of e-commerce are business-to-business and business-to-consumer.
  - Business-to-business (B2B) ecommerce is usually characterized by high-volume and low-price margins
  - Business-to-consumer (B2C) e-commerce is characterized by low-volume and high-prices
- Benefits of e-commerce:
  - Instant worldwide availability
  - Streamlined buyer to seller relationship
  - Reduced paperwork
  - Reduced errors, time, and overhead costs in information processing
  - Reduced time to complete transactions
  - Easier entry into new markets
  - New business opportunities
  - Improved market analysis
  - Wider access to assistance and advice
  - Improved product analysis
  - Ability to streamline and automate purchasing
- Disadvantages of e-commerce:
  - Increased vulnerability to fraud
  - Intellectual property
  - Confidentiality
  - Taxation
  - Customs
  - Regulations
  - Credit card fraud
  - Security
  - Trust
  - Availability 24/7
- Choices for an e-commerce site can be:
  - In-house: a Web business must buy or develop and integrate an e-commerce software package
    - Advantages: complete control of hardware and software infrastructure
    - Disadvantages: money; cost
  - Instant storefront: a software package from a vendor that provides the desired features at a lower cost
    - Online: the entire e-commerce package is on the service provider's infrastructure
    - Offline/Hybrid: requires installing software on the business's computing infrastructure

- Seven ingredients for success:
  - Generating demand
  - Ordering
  - Fulfillment
  - Processing payment
  - Service and support
  - Security
  - Community
- For the storefront to be effective, two situations must occur:
  - Traffic must be directed towards the storefront.
  - “Lookers” must be converted to buyers.
- When developing ordering infrastructure remember:
  - Be consistent
  - Eliminate redundant information
  - Make ordering easy
  - Accept substitutes
  - Include bailout mechanism
- Three models for payment in e-commerce:
  - Cash model: easiest to understand; hardest to implement
  - Check model: consumer presents a digital version of a check to the Web storefront
  - Credit model: works well because existing credit card processing already uses the same infrastructure needed for e-commerce
- Ways to provide service and support:
  - Automatic callback
  - Click-to-dial
  - Co-browsing
- Secure Sockets Layer (SSL) is an encryption protocol used to protect data transmitted between a client browser and a server.
- A Virtual Private Network (VPN) is an encrypted data stream that exists between two computers.
- The phased approach to a Web storefront:
  - Step 1: information only Web site
  - Step 2: limited transactions
  - Step 3: full transactions
  - Step 4: legacy system integration

Lesson 2: Law and the Internet

- Intellectual property is products such as written materials, musical compositions, and trademarks that are protected by copyright, trademark, or patent laws.
- Electronic publishing (EP) is the use of computers rather than traditional print mechanisms to distribute information.

- Two types of intellectual property:
  - Industrial property
    - Industrial designs
    - Inventions
    - Trademark and service marks
    - International protection
  - Copyrighted material
    - Protected works
      - Literary works
      - Musical works
      - Artistic works
      - Photographic works
      - Audiovisual works
      - Software
    - International protection
- EP laws of liability can be divided into the following categories, all of which affect the Internet and EP:
  - Copyright, trademark, and patent issues
  - Privacy and confidentiality issues
  - Jurisdictional issues
- Copyrights last for the life of the author plus fifty years.
- The Information Infrastructure Task Force (IITF) was formed in 1993 to examine the intellectual property implication of electronic publishing.
- Trademarks are property, and grant to the trader an exclusive right to use an individual mark.
- A patent is a document issued by the Government conferring some special right or privilege to the individual possessing the patent.
- The On-Line Copyright Infringement Liability Limitation Act amends the US Copyright law to exempt an online provider, from liability for direct infringement based on the intermediate storage and transmission of material over the provider's network.
- The No Electronic Theft (NET) Act amends US Copyright law so that "financial gain" includes the receipt of anything of value, including copyrighted works.
- The Digital Millennium Copyright Act (DMCA) was created to allow US Copyright laws to conform to World Intellectual Property Organization (WIPO) treaties for international copyright standards.
- Four main parts of the DMCA:
  - Anti-circumvention provision
  - Protect copyright management information (CMI)
  - Service provider liability
  - Web casting
- WIPO attempts to promote technology sharing among member countries. It also administers the Berne Treaty and the Paris Convention, both of which are multinational agreements governing the management of intellectual property.
- The Internet Tax Freedom Act was signed in 1998 and imposed a three-year moratorium on new Internet taxation.

Lesson 3: Web Marketing Goals

- Two ways to build a loyal following for a Web business:
  - Online communities
  - Directed or opt-in e-mail

- Online marketing strategies include many focus areas:
  - Web site design
  - Online promotion campaigns
  - Targeted marketing programs
  - Search engine placement methods
- Soft goods are software, music, news, and advice (digital).
- Hard goods are actual items such as computer hardware, clothes, and books.
- A product's appeal can be categorized in two ways:
  - Global or mass market
  - Niche or micro market
- Demographics is the study of groups of people based on common characteristics.
- Psychographics is the science used to help anticipate the specific positive, negative, or neutral psychological impact of words, symbols, shapes, textures, colors, fonts, or even scale on consumer target market groups.

Lesson 4: Online product promotion

- Common types of online promotions:
  - Banner ads
  - Banner exchange
  - Referrer sites
  - Search engine placement
  - Spam e-mail
  - Targeted e-mail
  - Opt-in e-mail
- A portal is a Web site that many people visit and use to explore and participate in activities on the Internet.
- A publisher site is a site whose primary focus is selling ad space as a means of revenue.
- A marketer site is a site whose primary focus is selling products or services for revenue.
- Banner advertising is one of the most common forms of online promotion.
  - Ad clicks: the number of times users click a banner ad
  - Banner: an ad on a Web page that links to the advertiser's site
  - CASIE: Coalition for Advertising Supported Information and Entertainment
  - Clickthrough: percentage of ad viewings that resulted in a user clicking the ad
  - CPC: cost per click
  - CPM: cost per thousand for an ad
  - Hit: each instance of a Web server sending a file to a browser
  - Impressions: number of times an ad banner is downloaded and presumably seen by visitors
  - Log file: file that tracks actions that have occurred
  - Page views: number of times a user requests a page containing an ad
  - Unique users: number of different users who visit a site within a time period
  - Visits: sequence of requests made by one user at one site
- Advertising representatives can help with decisions and placement choices for banner ads.
- The only way banner ads effectiveness can be understood is to track the process.
- A banner exchange program is a way to promote a site but keep costs down.
- Referrer sites or programs operate differently from banner exchange programs because they direct traffic in on direction.
- An evaluation of banner ad effectiveness can be done using several different software programs.
- Alternatives to banner ads:
  - E-pod
  - Bluestreak
- Becoming a partner with a well-known customer incentive program is a reliable method for generating sales.

- Only one of every 4 Web sites uses keyword and <META> tags.
  - Keywords: do not use excessively; maximum allowance is one thousand characters
  - Description: no more than twenty-five words
  - Robots: <NOINDEX>, <NOFOLLOW>, <NOIMAGECLICK>, <NOIMAGEINDEX>
- Search results are ranked according to relevance to given search criteria. A few common characteristics:
  - Titles
  - Beginning content
  - Frequency
- Spam e-mail is un-solicited e-mail.
- Targeted e-mail is spam that has been tailored for a particular customer base.
- Opt-in e-mail is the only legitimate form of e-mail marketing.

Lesson 5: Site Usability

- Usability is the measure of effectiveness users have with their Web site visit.
- The most traveled path of a Web site can be determined by click patterns.

Lesson 6: Customer Relationship Management (CRM) and E-Services

- E-service is online customer service.
- E-service methods can be solved synchronously, asynchronously, and by self-service.
  - Synchronous service allows the customer to communicate in real-time with the merchant.
    - Chat can allow immediate and specific information exchange.
    - Audio and voice connection is still developing but emerging as common forms of support.
      - Telephone: customer click's a hyperlink and call is made to support
      - Telephony: transmits voice over the Internet
    - Co-browsing allows a customer assistance center to control the customer's browsing during a live session.
  - Asynchronous service implies the steps in the process do not occur at the same time.
    - E-mail is the most common form of asynchronous service.
    - Web forms differ from e-mails in that questions will more likely be entered into a database.
  - Self-service is often faster than synchronous and asynchronous because the customer finds his or her own answers.
    - Client accounts and profiles
    - FAQs rank high as a form of customer service.
    - A knowledge database is similar to a FAQ but more customized.
    - HTML/Web-based help is relatively new because older browsers have difficulty supporting the technology.
    - Online communities allow customers to develop relationships with each other.
    - Surveys are an additional way to retrieve customer data to help gauge how customers perceive the level of customer service.
    - Customer service feedback must be easy to give, and responded to effectively.

- E-service action plan:
  - Identify the customer
  - Examine current Web traffic patterns
  - Use suppliers when appropriate
  - Use existing information
  - Analyze potential tools
  - Create a close relationship with the customer
  - Gather information for future planning
  - Remove the fear on online purchasing
  - Ensure privacy
  - Provide transaction incentives
  - Conduct service metrics
- Customer Relationship Management (CRM) is different from customer service because it deals with the management of customers from a business process viewpoint rather than that of the direct customer.
- Elements of CRM:
  - Establishing new customers is usually a major goal of most businesses.
  - Improving value to existing customers.
  - Generating repeat business
  - Data-mining is the use of consumer data to improve CRM
  - CRM incentives

Lesson 7: Business-to-Business Frameworks

- The business-to-consumer model is driven by many variables.
- The business-to-business model is driven by redundant high-volume transactions conducted between two companies.
- The most common form of data exchange is Electronic Data Interchange (EDI).
- EDI is a messaging protocol meant to ensure that data sent between normally incompatible computers retains its integrity and is formatted consistently.
- EDI is the inter-organizational exchange of documents in standardized electronic form directly between participating computers.
- EDI goals:
  - Enable easy and inexpensive communication of structured information throughout the lifetime of an electronic transaction.
  - Reduce the amount of data capture and number of transcriptions, in hopes of improving processes because of fewer errors, reduced time spent handling errors, and fewer delays due to incorrect or unformatted data.
  - To ensure faster handling of transactions to increase cash flow.
- The American National Standards Institute (ANSI) governs EDI encoding.
- A twofold benefit of Internet EDI is expected:
  - For established EDI users, new trading partners will have access to EDI.
  - Small to medium businesses will be able to compete for business with organizations that had previously been out of reach.
- Secure/Multipurpose Internet Mail Extensions (S/MIME) allows vendors to independently develop interoperable RSA-based security for their e-mail platforms.
- S/MIME uses enveloping.
- The XML/EDI combination will allow more flexibility than EDI on its own. It is also human and machine readable.
- Open Buying on the Internet (OBI) is an Internet e-commerce specification based on open technologies developed to target high-volume, low-cost transactions.

- Components of an OBI transaction:
  - Requisitioner: person or software that initiates the transaction to purchase
  - Buying organization: company that represents the requisitions and has an OBI server
  - Selling organization: company offering the product or service for sale and has an OBI server
  - Payment authority: organization that acts as a neutral third party to settle the final component of the transaction
- An OBI transaction undergoes a process of validation and authorization to ensure that the purchase is authentic and approved.
- OBI orders are formatted in ANSI EDI X12 850, meaning that companies that already have EDI can make their systems OBI-compliant.
- Open Trading Protocol (OTP) defines trading protocol options, which control how the trade occurs.
- OTP supports EDI for transaction processing.
- Three features of OTP:
  - Provides trading protocol options to control hw the trade occurs
  - Provides a record of the trade
  - Supports real and virtual delivery of goods and/or services
- Portals are short-term ways to conduct e-commerce, but cannot automate a B2B transaction from supplier to customer.
- E-business is defined as all forms of business conducted electronically including e-commerce.
- The Universal Description, Discovery, and Integration (UDDI) is an e-business industry initiative to help create platform-independent, open frameworks to allow companies to discover services and business rules that other businesses use and help them integrate their services using the Internet.
- A supply chain is the channel of getting raw materials needed to build a product from all sub-part manufacturers to the final assembly of a product, then to the end user.
- Supply chain management was controlled by EDI, but it is now controlled by the Internet and supply chain management software.
- Procurement is the process that companies use to buy items from suppliers.
- Automated procurement is also known as e-procurement.
- A vertical marketing system unites multiple manufacturers in the same industry to coordinate and streamline distribution channels and the supply chain.
- A horizontal marketing system is a venture between two or more companies, which do not compete, but instead compliment each other.
- Inventory is the amount of product held between the time the merchant produces or acquires that product and the time it is shipped to a customer.
- Allowing customers to track their orders is a valuable form of customer service.
- Localization is the process of translating material into a specific language or culture.
- Telecommuting is allowing messages to be sent wherever workers are located.
- Telephony is the technology in which telephone calls that would normally be routed via standard telecommunications means are instead sent over the Internet.
- Four types of Web conferencing:
  - Static
  - Static with presenter
  - Web-based conferencing service
  - Conferencing software

Lesson 8: Electronic Commerce Site Creation Packages-Outsourcing

Lesson 8.1: Outsourcing-The Online Instant Storefront

- Yahoo and other site servers allow small business owners to create an EC site that the site server administers at a fixed monthly cost.
- Online storefront packages separate into two subcategories:
  - Independent storefront: allows a business to be referenced by a fully qualified domain name
  - Portal/Community: create a new source of revenue and offer an entry-level EC business an inexpensive introduction to the marketplace; Independent domain names cannot be used.

Lesson 8.2: Outsourcing-The Mid-Level Offline Instant Storefront

- The mid-level online or offline instant storefront package offers the experienced EC marketer, established business owner, or the more developed business a more thoroughly customized, more personally administered, more expensive option for EC storefront creation and administration than the entry-level option.
- An efficient way of generating demand and building community is by using the customization features available with EC storefront packages.

Lesson 8.3: Outsourcing-The High-Level Offline Instant Storefront

- The high-end instant storefront offers the well-established, mid-size to large business a sophisticated software package for site creation, implementation, and administration.
- Another type of e-commerce is the auction site.
- By using a community auction site, an individual can conduct e-commerce without the need for an in-house, outsourced, online, or offline EC package.

Lesson 9: Electronic Commerce Site Creation Software

- A Web server commonly serves HTML and several image formats. It can also deliver program files of almost any type.
- A Web server uses the Hypertext Transfer Protocol (HTTP).
- Generally, a Web server runs as a daemon process on UNIX machines and as a service on Windows NT/2000 machines.
- You can extend the features of a Web server through additional programs and servers.
- Web servers often deploy client-side and server-side scripting.
- Apache Web server is a tested, open-source solution developed by Apache Software Foundation.
- Lotus Domino includes all most-used servers and has the ability to serve application over Intranets and the Internet.
- iPlanet is an alliance between Sun and Netscape that provides similar services to those of Lotus Domino and Apache.
- Internet Information Server (IIS) is integrated with Windows NT/2000 and provides two advantages:
  - IIS takes advantage of the Windows NT/2000 security structure.
  - IIS has a familiar interface.
- IIS allows the use of encryption of up to 128 bits for SSL services.
- Microsoft Active Server Pages allows you to create pages through client-side scripting.
- IIS has a built-in FTP feature.
- Because IIS is a Microsoft product, it integrates well with other Microsoft products.
- IIS allows the mapping of URLs to different physical locations on a hard drive. This is called a virtual directory.
- Virtual servers are similar to virtual directories in that several sites can run on one NT server.

- IIS supports all standard Web file formats.
- Additional IIS features:
  - Content management and site analysis
  - Ability to create multiple Web sites within on Web server
  - Automated management support
  - ASP script de-bugging
  - Built-in site search engine
  - Limited remote administration abilities
- The Microsoft Management Console (MMC) provides a framework for network administration programs for IIS, and other servers or services.
- The most important function of MMC is the ability to stop, start, and configure Internet-related services.
- You can view and customize IIS settings by highlighting a server in the MMC and right-clicking it.
  - The Web site tab allows you to customize IP addresses, port numbers, and server connections.
  - The Documents tab allows you to point the server toward a default document.
  - The Home Directory tab enables you to identify the default documents you will use.
  - The Directory Security tab allows you to control access and view and edit certificates.
  - The Operators tab determines who can administer the site.
  - The Performance tab optimizes the Web server for the expected number of hits.
  - The ISAPI Filters tab identifies ISAPI programs used as alternatives to CGI.
  - The HTTP Headers tab allows customization of headers sent from the server to a browser.
  - The Custom Errors tab sends a basic message whenever IIS cannot respond to a client or server request.
- Virtual directories and aliases are the flexible mapping of URL path names to local file names.
- Advantages of flexible mapping:
  - Ability to serve files that do no reside immediately beneath the Web server root directory
  - Simplified organizational structure
- Most enterprise-grade Web servers allow you to create multiple Web servers on the same machine.
- If you use multiple IP addresses, you can register each with a DNS server, allowing multiple companies or departments to use one system running multiple Web servers.
- When a service receives a request for a URL that refers to a directory, rather than a specified document, the server may:
  - Return a default document (index.htm, default.htm) present in that directory
  - Generate an error and refuse the request
  - Return a formatted directory listing to the browser

Lesson 10: Site Development Software Implementation-Microsoft Platform

- A database is a formally arranged set of persistent information stored by a computer program.
- A flat-file database is a file in which data is collected in lines of text, separated by a delimiter (usually a comma).
- A system catalog is a description of data in a database.
- A relational database is a body of data organized as a set of formally defined tables.
- Database Management System (DBMS) is software that supports the creation and management of databases.

- Some features of DBMS:
  - Can support a specific language to facilitate manipulation of data (SQL).
  - Allows users to retrieve, insert, update, and delete data in the database using Data Manipulation Language (DML).
  - Provides a security system, integrity system, concurrency control system, recovery system, and a system catalog
  - Provides a view mechanism used to create views particular to each set of users
- Structured Query Language (SQL) is commonly used to work with databases.
- Three types of SQL accounts:
  - Local system
  - Local user
  - Domain user-used for server-to-server activities such as Remote Procedure Call
- Remote Procedure Calls allow servers of different types to communicate across a dedicated network, accessing files, services and information.
- Commerce Server 2000 is Microsoft's package to create Internet commerce enabled Web applications.
- Commerce Server has three interfaces:
  - Biz Desk
    - Creating online catalogs
    - Managing user accounts
    - Analyzing applications
    - Managing campaigns and profiles
  - Commerce Server Manager
    - Administering multiple site resources and properties
  - Pipeline editor
    - Defining business processes and sequencing requirements
- Solution sites are pre-configured and defined e-commerce sites that help create a quick start for an e-commerce site. There are three types of solution sites:
  - Blank: provides an empty shell for development
  - Retail: provides a shell for an online catalog for a business-to-consumer site
  - Supplier: provides shell to support business-to-business application

Lesson 11: Developing an Electronic Commerce Site Using Commerce Server

- Solution sites are based heavily on ASP and server-side includes.
- Business Desk (BizDesk) is the Web interface for solution site administration.

Lesson 12: Online Catalog

- The term catalog implies a series of products grouped together that a customer can browse.
- The shopping cart is the component of an e-commerce site that helps users to keep track of the items they plan to buy.
- Commerce Server is concerned about four components in a catalog; property definitions, product definitions, category definitions, and catalog definitions.

Lesson 13: Using and Configuring Payment Gateways

- Three tasks must be accomplished to implement online transactions:
  - Prepare server and e-commerce site
  - Set up an online merchant account
  - Install payment software
- To use electronic cash, a consumer needs a wallet the same as the merchant.

- E-commerce myths:
  - Hackers can copy any credit card information transmitted across the Internet.
  - The encryption used on the Internet can be easily broken.
  - All that is needed to protect a Web site is to install a digital certificate and use SSL.
  - Securing a site is impossible.
- A payment gateway is the connection between the online catalog and a merchant bank.
- The process used to move a transaction onto the settlement stage is called batching.
- The Automated Clearing House (ACH) is a nationwide batch-oriented Electronic Funds Transfer (EFT) system governed in the United States by the National Automated Clearing House Association (NACHA) operating rules.
- ACH is not real time processing and usually needs twenty-four hours to complete a transaction.

Lesson 14: E-Services Support

- A knowledge base is a database that stores and retrieves information.
- To install Right Now Web a database management system must be installed.

Lesson 15: Transaction Security

- Cryptography protects against a wide variety of attacks on the communications between two parties.
- Security serves five purposes in e-commerce:
  - Authentication and identification
  - Access control
  - Data confidentiality
  - Data integrity
  - Non-repudiation
- Authentication is implemented by using digital certificates
- Access control governs the resources that a user may access on the network
- Data confidentiality deals with how secure data will remain and is provided by encryption.
- Data integrity ensures that information has not been modified en route to the destination and is provided by hashing.
- Properties of non-repudiation prevent merchants or customers from denying that they agreed to a sale or purchase. It is implemented with a digital signature.
- Cryptography is the science of encrypting and decrypting plaintext messages.
- Ciphertext is encrypted messages.
- A cipher is used to encrypt and decrypt plaintext messages.
- Encryption strength is based on three factors:
  - Strength of the algorithm
  - Secrecy of the key
  - Length of the key
- Three types of encryption standards are available today:
  - Symmetric: secret key, shared key, private key, or session key
  - Asymmetric: public key
  - One-way encryption
- In symmetric encryption, both parties possess a single secret key.

- Algorithms that use symmetric key:
  - Data Encryption Standard (DES): 56-bit key
  - Triple DES: Two 56-bit keys
  - Skipjack: 80-bit key and 64-bit 32-round cipher
  - International Data Encryption Algorithm (IDEA): 128-bit key on 64-bit plaintext blocks in eight iterations
  - Blowfish: variable key length, 448-bit maximum
  - RC2: Rivest Cipher Two is a 64-bit block cipher with variable key length
  - RC4: does not divide plaintext into blocks
  - RC5: totally parameterized system
- In asymmetric encryption, each person gets two pairs of keys: a private key and a public key. No secret key is ever shared or exchanged.
- Asymmetric key cryptosystems have the following properties:
  - Applying the algorithm with the encryption key on a plaintext message produces a ciphertext. Applying the algorithm with the decryption key on the ciphertext produces the original plaintext message.
  - Both public and private keys are easy to compute mathematically, but not easy to guess.
  - By publicly revealing his or her public key, the user does not reveal an easy way to compute the corresponding private key.
- One algorithm that uses asymmetric key encryption is RSA.
- One way encryption is used primarily for storing NT and UNIX passwords and ATM personal identification numbers.
- A message digest is a specific application of a one-way function.
- A good hash function has two properties:
  - It will be difficult to invert
  - It should be resistant to collisions
- Some well-known hash functions:
  - MD5: involves appending a length field to a message and padding it to a multiple of 512-bit blocks. Each 512-bit block is fed through a four-round process that results in 128-bit message digests.
  - Secure Hash Algorithm (SHA): developed by the National Institute of Standards and Technologies (NIST); the message is first padded with MD5, the fed through four-rounds, which are more complex than the ones used in MD5; the resulting message digest is 160-bits long.
- Authentication is the process by which the receiver of a digital message can be confident of the sender's identity.
- The following entities participate in e-commerce:
  - Customer: interested in initiating an electronic transaction
  - Merchant: Web storefront owner
  - Processing network: intermediary that facilitates transfer of financial data between Web storefront and bank
  - Card/check issuing bank: bank that issued customer's credit card or checking account
  - Merchant's bank: bank that holds the merchant's account
  - Trusted third party: usually a certifying authority that verifies the merchant's identity to the customer and vice-versa.
- Digital certificates are a standard file format for storing a user's or server's public key and related information.
- Certificate authorities are trusted third-parties that verify the identity of an individual.

- Four types of certificates are currently used:
  - A certificate authority certificate is used by organizations such as VeriSign to sign other certificates.
  - A server certificate is used on Web servers to identify the Web server and the company running it, and to allow for encrypted SSL sessions between the server and browsers.
  - A personal certificate allows individuals to strongly authenticate and to engage in S/MIME, SSL, and SET.
  - A software publisher certificate is used by software authors to sign and identify their released code so the author can be identified and the integrity of the code verified.
- Trusted third parties that issue certificates are called certifying authorities (CAs).
- All four certificate types use the X.509.3 standard, which established the format and contents of the physical certificate file.
- CAs maintain revocation lists, which identify certificates that have been revoked after their release.
- Reasons for revocation include private key compromise, wrong certificate issuance, issuance for an individual or service that is no longer valid, or the worst case scenario of CA compromise.
- The most widely accepted CA on the Internet is VeriSign.
- VeriSign is the first CA to specify a Certification Practice Statement (CPS), which sets the performance standards for a CA.
- VeriSign's digital IDs use the strongest available cryptographic techniques to ensure that IDs are not tampered with or forged.
- To ensure the integrity of the IDs issued, VeriSign uses comprehensive security systems, including multi-level physical access controls, biometric scanners, and sound firewall technology.
- VeriSign offers two types of personal certificates:
  - Level-one certificates use only e-mail verification.
  - Level-two certificates require you to supply significant information such as driver's license number, SSN, and so forth.
- The Secure Sockets Layer (SSL) is a security protocol that provides privacy over a network.
- SSL provides encryption and authentication.
- Port 443 is used for SSL.
- Certificates assist authentication but do not provide absolute proof.
- Secure Electronic Transactions (SET) is the de facto payment standard on the Internet.
- SET uses public-key and symmetric encryption techniques.
- To ensure maximum security, asymmetric cryptography is available.
- Hashing is used to insure payment information integrity.

Lesson 16: Web Site Management and Performance Testing

- The party responsible for the site content and integrity has three primary tasks:
  - Maintenance of the site and its contents, including updating the Web pages, maintaining the database, and checking for broken links.
  - Maintaining the security of the site.
  - Monitoring the performance of the site.
- If requests enter a queue until the queue has no more space, a bottleneck will result.
- System and service logs allow a user to determine a system's ability to meet demands.
- Logs can inform you of the following issues:
  - Server efficiency
  - Usage rate
  - Revenue generation
  - Security

- Priorities to log files should be set using the following criteria:
  - Mission criticality
  - Service type
  - Server location
  - Recent installations
- When evaluating log files, check for the following:
  - Peak usage rates
  - Error messages
  - Failed logon attempts
- The more events that are logged, the harder the system has to work.
- Server logs record the time of each HTTP transaction, along with the number of bytes transferred.
- The Access log contains information about URL fetches, including:
  - IP address of the client accessing the server
  - Time of the day the connection occurred
  - Name of the URL
  - HTTP request
- The Error log records:
  - Server startup and shutdown
  - Malformed URLs
  - Erroneous CGI scripts
- A Referrer log can show the number of files one page requires to render in a browser.
- The Agent log records the version of any user agent that accesses a site.
- The only way to measure performance is to test the working site.
- Performance Monitor is the primary tool for determining server bottlenecks and problems on that system.
- The three main resources for measuring the stream of server requests and responses are:
  - Server and service log files
  - Protocol analyzers
  - System performance tools
- Packet sniffers capture packets as they cross a network.
- Three methods for correcting bottlenecks:
  - Speed up the component causing the bottleneck by replacing it with an upgraded version
  - Replicate the component causing the bottleneck by distributing the demand for a service across multiple servers
  - Increase the capacity of queues in the system to tolerate more requests before turning away new ones
- Improving hardware will always improve Internet server performance.
- The most important factor when considering Web servers is the amount of RAM.
- You can adjust the amount of time a Web application will keep a connection by using Microsoft IIS and enabling session state.