INTERNET & WEB APPLICATION DEVELOPMENT SWE 444

Fall Semester 2008-2009 (081)

Module 9: e-Commerce and Web Security

Dr. El-Sayed El-Alfy
Computer Science Department
King Fahd University of Petroleum and Minerals
alfy@kfupm.edu.sa

Objectives/Outline

- Objectives
  - Describe the key dimensions of e-commerce security
  - Identify the key security threats in the e-commerce environment
  - Identify and describe various forms of encryption technology and security tools to protect e-commerce

- Outline
  - Introduction to e-Commerce
  - Dimensions of e-Commerce Security
  - Technology Solutions

Resources

- E-commerce: business, technology, society. 2nd Edition, Chapter 5. By Kenneth C. Laudon and Carol Guercio Traver
- Network Security Essentials: Standdards and Applications, 3rd Edition., Chapter 7 By William Stallings
- Some websites

Definition of e-Commerce

- E-commerce involves digitally-enabled commercial transactions between and among organizations and individuals
- Digitally enabled transactions include all transactions mediated by a digital technology
- Commercial transactions involve the exchange of value across organizational or individual boundaries in return for products or services
- e-Commerce vs. e-Business
  - E-Commerce: direct financial electronic transaction (e.g., ordering a book on Amazon.com)
  - E-Business: use of the Internet and the Web to better support any current manner (planning, sourcing, manufacturing, execution, selling) of doing business.

Unique Features of e-Commerce

- Ubiquitous
  - Available everywhere, all the time
  - Global reach (across cultural/national boundaries)
- Interactive (can simulate face-to-face experience, but on global scale)
- Operates according to universal standards
  - lowers market entry for merchants and search costs for consumers
- Provides information richness (amount and quality of information available to all market participants)
  - more powerful selling environment
- Permits personalization/customization

Types of e-Commerce

- Classified by nature of market relationship
  - Business-to-Consumer (B2C)
  - Business-to-Business (B2B)
  - Consumer-to-Consumer (C2C)
- Classified by type of technology used
  - Peer-to-Peer (P2P)
  - Mobile commerce (M-commerce)

Pros & Cons

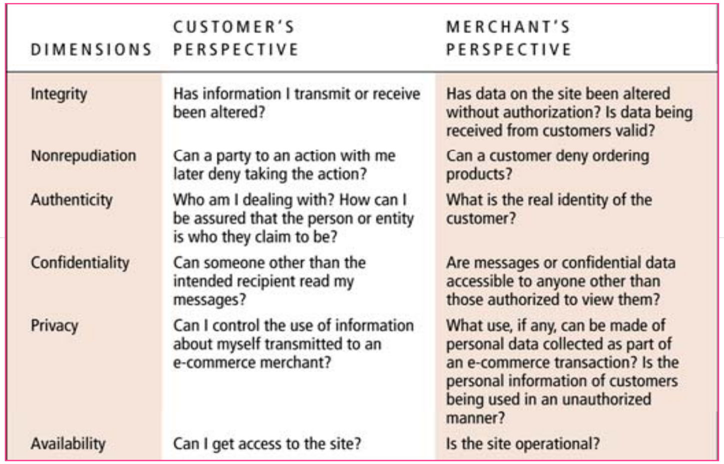
- Pros
  - Quick
  - Easy
  - Time saver
  - Variety of choices and comparison
- Cons/Concerns
  - Security --- very important
  - Speed of internet access
  - Malfunction of website
  - Physically touching the product
  - Shipping and handling
  - Who to deal with when customer is not satisfied

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

Dimensions of e-Commerce Security (cont.)

- Customer and merchant respective on the different dimensions of e-commerce security



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

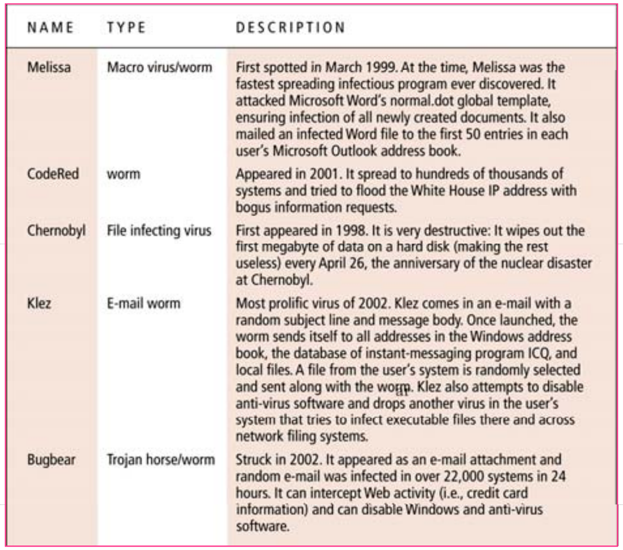
Security vs. Other Values

- Security vs. ease of use: the more security measures that are added, the more difficult a site is to use, and the slower it becomes
- Security vs. desire of individuals to act anonymously

Security Threats in the e-Commerce Environment

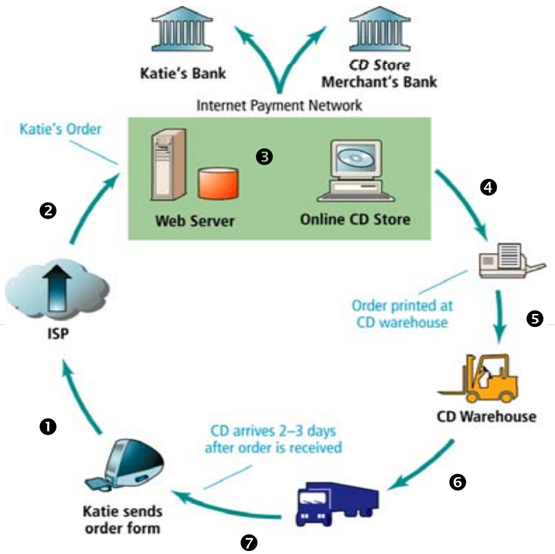
- Three key points of vulnerability:
  - Client
  - Server
  - Communications channel
- Most common threats:
  - Malicious code (code designed to cause harm in some way: viruses, worms, trojan horses, malicious java applets or ActiveX controls)
  - Hacking and cyber vandalism (To alter a computer program and/or gain access to computing resources illegally or without authorization)
  - Credit card fraud/theft
  - Spoofing (one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.)
  - Denial of service (DoS) and Distributed DoS (DDoS) attacks
  - Sniffing (using packet sniffer which is also known as network analyzer or protocol analyzer)

Examples of Malicious Codes

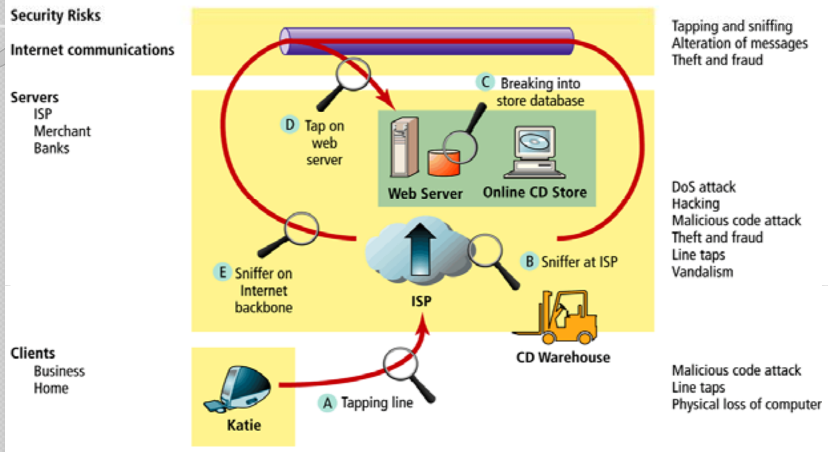


NAME	TYPE	DESCRIPTION
Melissa	Macro virus/worm	First spotted in March 1999. At the time, Melissa was the fastest spreading infectious program ever discovered. It attacked Microsoft Word's normal.dot global template, ensuring infection of all newly created documents. It also mailed an infected Word file to the first 50 entries in each user's Microsoft Outlook address book.
CodeRed	worm	Appeared in 2001. It spread to hundreds of thousands of systems and tried to flood the White House IP address with bogus information requests.
Chernobyl	File infecting virus	First appeared in 1998. It is very destructive: It wipes out the first megabyte of data on a hard disk (making the rest useless) every April 26, the anniversary of the nuclear disaster at Chernobyl.
Klez	E-mail worm	Most prolific virus of 2002. Klez comes in an e-mail with a random subject line and message body. Once launched, the worm sends itself to all addresses in the Windows address book, the database of instant-messaging program ICQ, and local files. A file from the user's system is randomly selected and sent along with the worm. Klez also attempts to disable anti-virus software and drops another virus in the user's system that tries to infect executable files there and across network filing systems.
Bugbear	Trojan horse/worm	Struck in 2002. It appeared as an e-mail attachment and random e-mail was infected in over 22,000 systems in 24 hours. It can intercept Web activity (i.e., credit card information) and can disable Windows and anti-virus software.

A Typical E-commerce Transaction



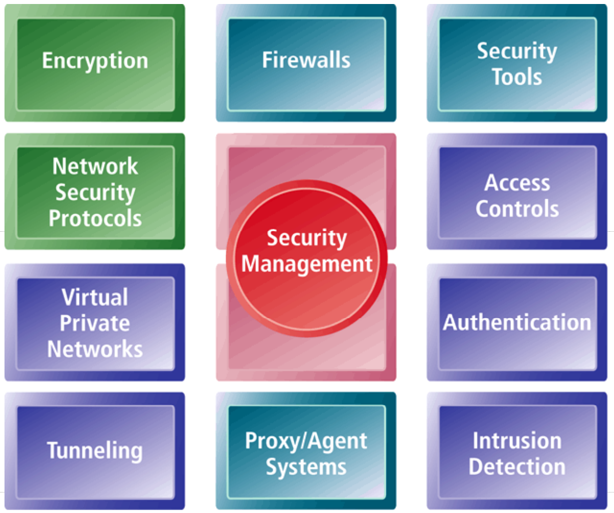
Vulnerable Points in an e-Commerce Environment



Technology Solutions

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

Site Security Management Tools



Encryption
Firewalls
Security Tools
Network Security Protocols
Security Management
Access Controls
Virtual Private Networks
Authentication
Tunneling
Proxy/Agent Systems
Intrusion Detection

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
  - Secure information transmission
- Provides:
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality

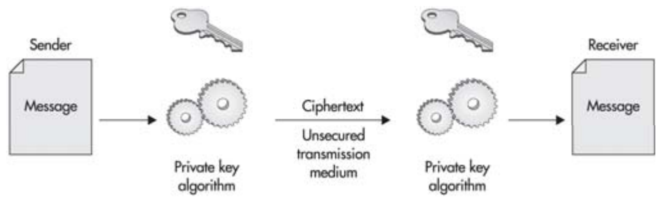
Cryptography

- Cryptography is the science or study of secret writing (cipher texts)
  - Basic idea: convert clear text (also called plain text – the original message) to ciphertext (the encrypted message)
- Three Main Categories
  - Secret Key (Symmetric Encryption)
    - single key is used to encrypt and decrypt information
  - Public/Private Key (Asymmetric Encryption)
    - two keys are used: one for encryption (public key) and one for decryption (private key)
  - One-way Function (Hashing)
    - Information is encrypted to produce a "digest" of the original information that can be used later to prove its authenticity

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
- Other known symmetrical algorithms
  - Triple DES, DESX, GDES, RDES
    - 168 bit key
  - RC2, RC4, RC5
    - variable length up to 2048 bits
  - IDEA - basis of PGP
    - 128 bit key
  - Blowfish
    - variable length up to 448 bits

Symmetric Key Encryption (Secret Key)



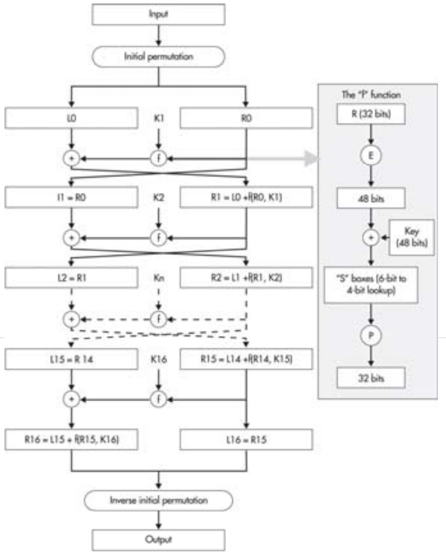
- Also called shared-key encryption
  - Both the sender and receiver use the same digital key to encrypt and decrypt message
- Requires a different set of keys for each transaction
- Strength of encryption technique depends on key length
- Advantages: *fast, ciphertext secure*
- Disadvantages: *must distribute key in advance, key must not be revealed*

Simple Secret-Key Example

- P = “abra” which has the binary representation:
  01100001011000100011100101100001
- Choose a random string of bits as the key
  10011101010010001111010101011100
- Can use a simple XOR of the binary to get C
  11111100001010101000011100111101
- To get P back, use the same algorithm and key

Data Encryption Standard (DES)

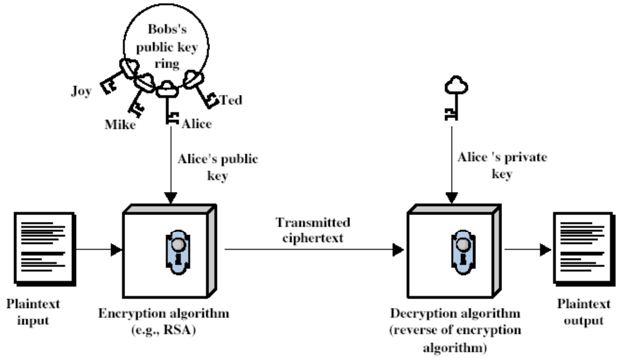
- Developed by IBM in the early 1970s
- Uses a 56-bit key
  - The key uses 7 bits of eight 8-bit bytes (the 8th bit of each byte is used for parity)
- DES is a block cipher that operates on one 64-bit block of plaintext at a time
- There are 16 rounds of encryption in DES, where each round uses a different subkey



Public-Key Encryption (Asymmetric Encryption)

- Probably most significant advance in the 3000 year history of cryptography
- 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 a 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
- Most common algorithm is the RSA algorithm with key lengths from 512 to 1024 bits

Public Key Encryption (Asymmetric Encryption)



- Advantages: *public key widely distributable, does digital signatures*
- Disadvantages: *slow* (RSA is about 1500 times slower than DES), *key distribution*

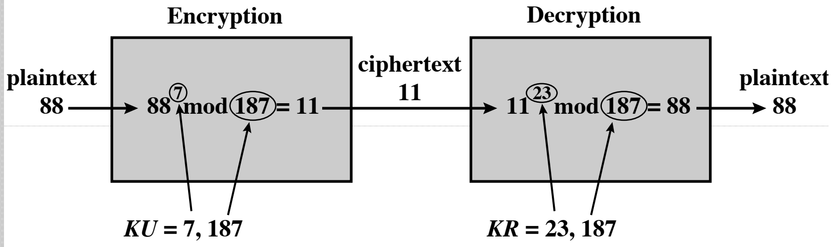
RSA

- by **R**ivest, **S**hamir & **A**dleman of MIT in 1977
- Its security is based on the difficulty of factoring large numbers
- The basic algorithm for confidentiality is very simple:
  - ciphertext = (plaintext)^{e} mod n
  - plaintext = (ciphertext)^{d} mod n
  - private key = {d, n}
  - public key = {e, n}
- The difficulty in calculating d given e and n provides the security

Generating RSA Keys

- To generate an RSA key pair, follow these steps:
  - Choose two prime numbers p and q and keep them secret
  - Calculate $n = p \times q$
  - Calculate $\varphi(n) = (p - 1)(q - 1)$
  - Select e such that e is relatively prime to $\varphi(n)$
    - gcd ($\varphi(n)$,e) = 1; 1< e <$\varphi(n)$
  - Calculate d = e $^{-1}$ mod $\varphi(n)$
  - Public Key KU = {e, n}
  - Private Key KR = {d, n}

Example of RSA Algorithm



One-Way Function

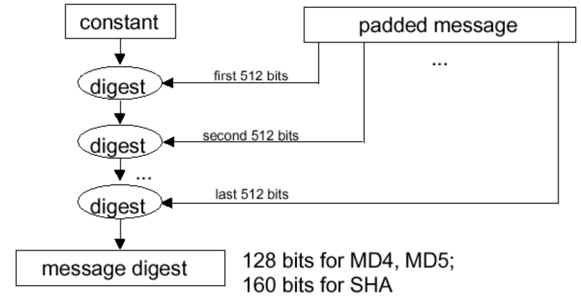
- non-reversible "quick" encryption
- produces a fixed length value called a hash or message digest
- used to authenticate contents of a message
- Common message digest functions
  - MD4 and MD5
    - produces 128 bit hashes
  - SHA
    - produces 160 bit hashes

Structure of MD4, MD5, and SHA

- Pad message to a multiple of 512 bits:

original message	1000 ... 000	64-bit original length

- Compute digest of padded message in 512-bit chunks:



128 bits for MD4, MD5;
160 bits for SHA

Cryptographic Services Allow

- Digital Signatures
  - sign messages to validate source and integrity of the contents
- Message Digests
  - short bit string hash of message
- Digital Envelopes
  - secure delivery of secret keys
- Certificates (Digital IDs)
  - used to authenticate: users, web sites, public keys of public/private pair, and information in general
- Secure Channels
  - encryption can be used to create secure channels over private or public networks

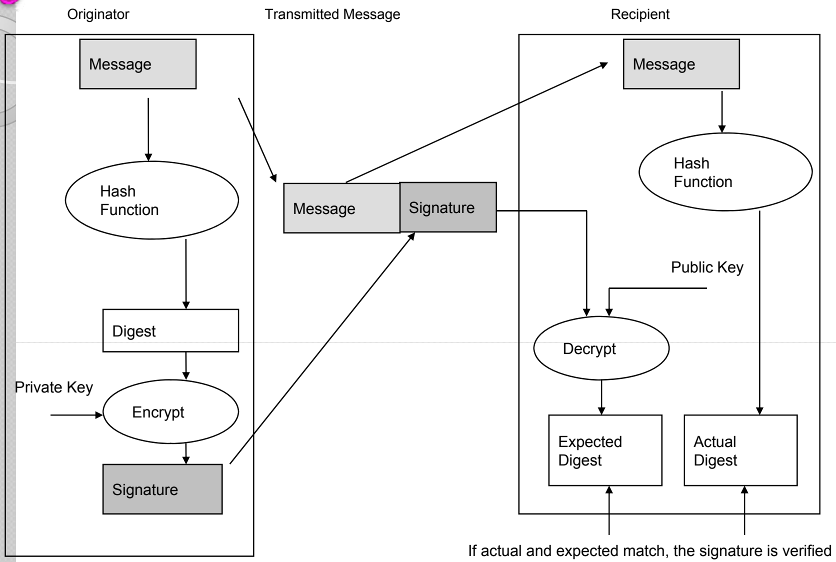
Digital Signatures

- Encrypt sender’s identity string with sender’s private key
- Concatenate the encrypted text and the identity string together
- Encrypt this message with receiver’s public key to create message
- Receiver decrypts the encrypted text with their private key
- the cypher text portion of the message is decrypted with sender’s public key
- The decrypted text can be compared with the normal text to checks its integrity

Message Digests

- How to create and use a message digest
  - sender uses message as input to digest function
  - “sign” (encrypt) output (hash) with sender’s private key
  - send signed hash and original message (in plain text) to receiver
  - receiver decrypts hash with sender’s public key
  - receiver runs plain text message through digest function to obtain a hash
  - if receiver’s decrypted hash and computed hash match then message valid

Message Digests (cont.)

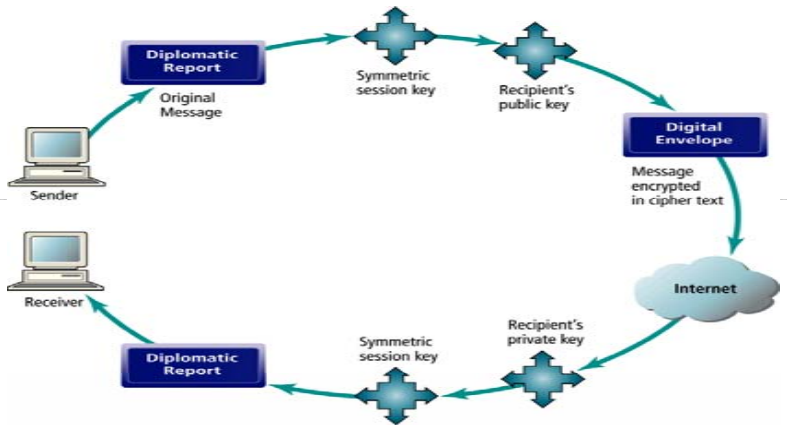


If actual and expected match, the signature is verified

Digital Envelope

- Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time)
- Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key
  - sender creates and uses symmetric (session) key to create cipher text
  - sender uses receiver's public key to encrypt the symmetric key - digital envelope
  - sender transmits both cipher text and digital envelope to receiver

Digital Envelope (cont.)



Understand Key Management

- Key management is one of the most critical aspects of an encryption system
- It includes creating strong keys, distributing them securely, certifying them, protecting while in use, and revoking them when they are compromised or expired
- If keys are transmitted,
  - They must be transported securely to ensure the integrity of the keys
  - They must be checked on arrival to ensure they have not been manipulated (usually done manually or by digital signatures)
- Certificate Authorities (CAs) ensure the integrity of the keys and prevent an attacker from introducing their own keys

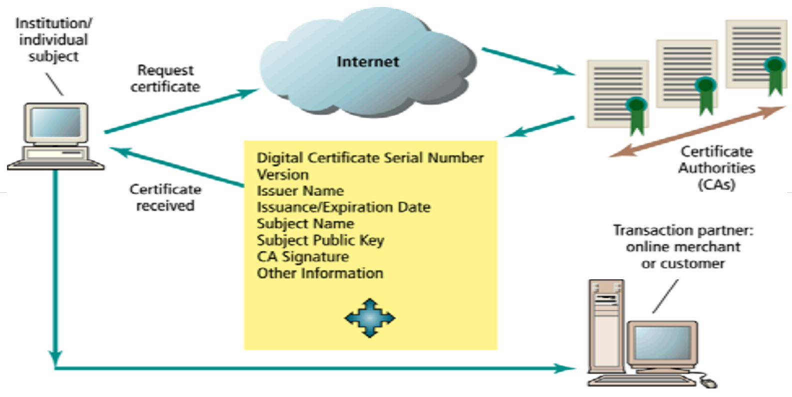
Digital Certificate

- Public keys require integrity protection (provided by certification), but they do not require confidentiality protection. However, all copies of the private key of a public key system must be protected at all times
- Digital document that includes:
  - Name of the holder
  - Public key of the holder
  - Name of trusted third party (certificate authority) that issues certificate
  - Digital certificate serial number
  - Issuance date and Expiration date
  - Digital signature of certificate authority
  - Other identifying information
- Certificate Authorities (CAs)
  - ensure the integrity of the keys and prevent an attacker from introducing their own keys
  - used to distribute the public key of a public/private pair
  - guarantees the validity of the public key
    - does this by verifying the credentials of the entity associated with the public key
  - Some Cases
    - VeriSign - http://www.verisign.com
    - Entrust - http://www.entrust.com
- Public key pairs are generally certified for one or two years
  - Session keys may only exist for a given session and may be deleted after the session

Digital Certificates (cont.)

- Process to create Digital Certificate
  - User generates public/private pair
  - User creates and sends a certificate request his choice of CA contains: identifying information and user's public key
    - Like Server, company, location, state, country and also the documents proving identity
  - CA confirms the accuracy of the information submitted
  - CA creates a certificate containing user's public key and information
  - CA creates message digest from certificate and signs it with CA's private key
  - The signed certificate is sent to the subscriber and also a copy of it may be submitted to the certificate repository, such as a directory service for publication

Digital Certificates (cont.)



Digital Certificates (cont.)

- Using a Digital Certificate
  - before sending a secure message sender request a signed certificate from receiver
  - sender decrypts signed certificate with CA's known public key to obtain message digest of info and public key provided to CA by receiver
  - sender creates a message digest of public key and info provided by the receiver for sender's use
  - sender compare the message digests if they match then receiver is validated

Digital Certificate Verification

- Do I trust the CA? (Is it in my list of trust root certification authorities?)
- Is the certificate genuine?
  - Look up the CA's public key; use it to decrypt the signature
  - Compute the certificate's hash; compare with decrypted sig
- Is the holder genuine? This requires a challenge
- If the holder is genuine, he must know the private key corresponding to the pubic key in the certificate
- Having the certificate is not enough. (They are exchanged over the Internet all the time)
- Send him a nonce (random 128-bit number)

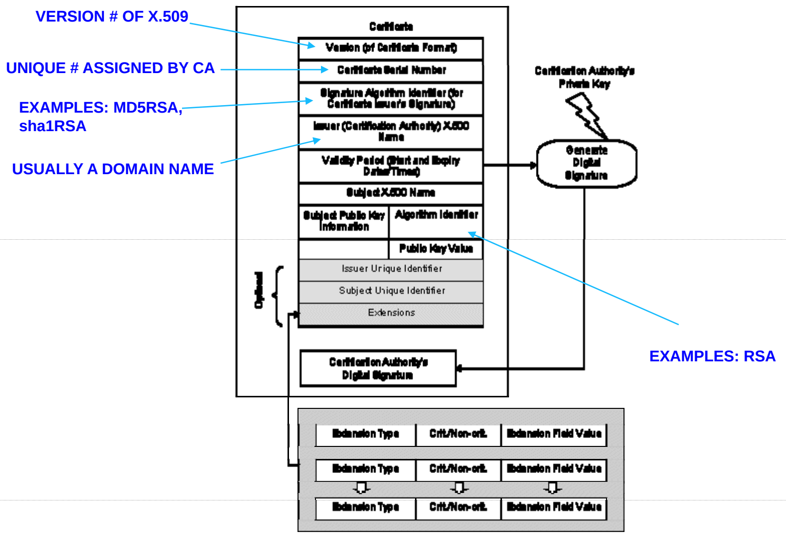
Challenge by Nonce

- If you're really Mr. X, you must know his private key
- So please encrypt this nonce:
  "A87B1003 9F60EA46 71A837BC 1E07B371"
- When the answer comes back, decrypt it using the public key in the certificate
- If the result matches, the remote user knew the correct private key
- Never use the same nonce twice

Types of Digital Certificates

- site certificates
  - used to authenticate web servers
- personal certificates
  - used to authenticate individual users
- software publishers certificates
  - used to authenticate executables
- CA certificates
  - used to authenticate CA's public keys
- All certificates have the common format standard of X.509v3

X.509 Version 3 Digital Certificate


VERSION # OF X.509

UNIQUE # ASSIGNED BY CA

EXAMPLES: MD5RSA, sha1RSA

USUALLY A DOMAIN NAME

EXAMPLES: RSA

Certificate
Version (of Certificate Format)
Certificate Serial Number
Signature Algorithm Identifier (for Certificate Issuer's Signature)
Issuer (Certification Authority) X.500 Name
Validity Period (Start and Expiry Dates/Times)
Subject X.500 Name
Subject Public Key Information
Algorithm Identifier
Public Key Value
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Optional
Certification Authority's Private Key
Generate Digital Signature
Certification Authority's Digital Signature
Extension Type
Crit./Non-crit.
Extension Field Value
Extension Type
Crit./Non-crit.
Extension Field Value
Extension Type
Crit./Non-crit.
Extension Field Value

Public Key Infrastructure (PKI)

- Digital certificates alone are not enough to establish security
  - Need control over certificate issuance and management
- PKI: refers to the CAs and digital certificate procedures that are accepted by all parties
- Functions of a PKI
  - Generate public/private key pairs
  - Identify and authenticate key subscribers
  - Bind public keys to subscriber by digital certificate
  - Issue, maintain, administer, revoke, suspend, reinstate, and renew digital certificates
  - Create and manage a public key repository

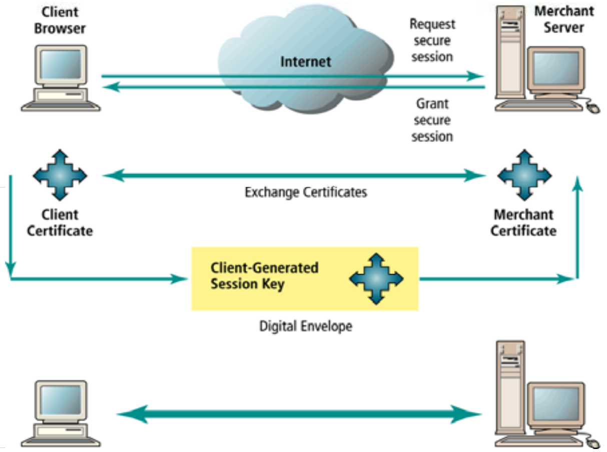
Securing Channels of Communication

- 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)

Internet Tunnels

- Virtual network circuit across the Internet between specified remote sites
  - uses an encrypting router that automatically encrypts all traffic that traverses the links of the virtual circuit
- Tunneling Protocols
  - PPTP by Microsoft - http://www.microsoft.com
  - Layer 2 Forwarding (L2F) by Cisco - http://www.cisco.com
  - L2TP (combines PPTP and L2F) - http://www.ietf.com

Secure Negotiated Sessions Using SSL



Session ID and methods of encryption negotiated.

Certificates exchanged. Identity of both parties established.

Client generates session key, and uses server public key to create digital envelope. Sends to server. Server decrypts using private key.

Encrypted transmission using client-generated session key begins.

Secure Sockets Layer

- SSL History
  - Competitor to S-HTTP
    - S-HTTP an extension of HTTP
  - General purpose encryption system using symmetric encryption
    - S-HTTP only encrypts Web protocols
  - Three versions v1.0, v2.0 and v3.0
    - SSL v3.0 implemented in Netscape 3.0 and Internet Explorer 3.0 and higher
    - SSL v3.0 supports Diffie-Hellman anonymous key exchange and Fortezza smart card

Secure Sockets Layer (cont.)

- SSL Characteristics
  - Operates at the TCP/IP transport layer
  - Encrypts (decrypts) input from application (transport) layer
  - Any program using TCP can be modified to use SSL connections
  - SSL connection uses a dedicated TCP/IP socket (e.g. port 443 for https or port 465 for ssmtp)
  - SSL is flexible in choice of which symmetric encryption, message digest, and authentication algorithms can be used
  - When SSL client makes contact with SSL server they try to pick strongest encryption methods they have in common
  - SSL provides built in data compression
    - compress first then encrypt

Secure Sockets Layer (cont.)

- SSL Characteristics
  - When SSL connection established browser-to-server and server-to-browser communications are encrypted. This includes:
    - URL of requested document
    - Contents of the document
    - Contents of browser forms
    - Cookies sent from browser to server
    - Cookies sent from server to browser
    - Contents of HTTP header
    - But NOT particular browser to particular server
      - socket addresses not encrypted
      - can use proxy server for privacy

Secure Sockets Layer (cont.)

- Establishing an SSL Connection
  - The client (browser) opens a connection to server port
  - Browser sends "client hello" message. Client hello message contains:
    - version of SSL browser uses
    - ciphers and data compression methods it supports
  - The Server responds with a "server hello" message. Server hello message contains
    - session id
    - the chosen versions for ciphers and data compression methods

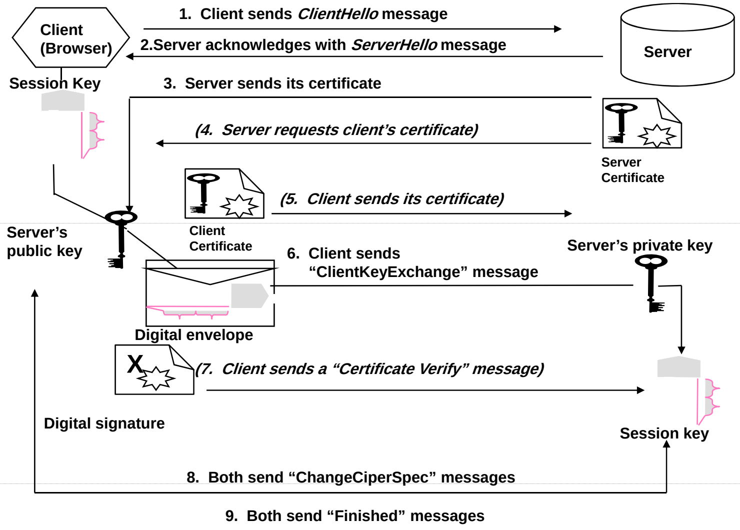
Secure Sockets Layer (cont.)

- Establishing an SSL Connection (con't.)
  - The server sends its certificate
    - used to authenticate server to client
  - Optionally the server may request client's certificate
  - If requested, client will send its certificate of authentication
    - if client has no certificate then connection failure
  - Client sends a "ClientKeyExchange" message
    - symmetric session key chosen
    - digital envelope is created using server's public key and contains the symmetric session key

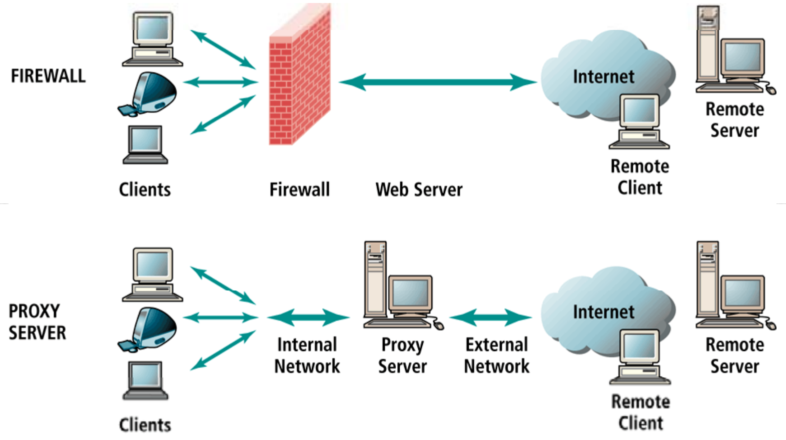
Secure Sockets Layer (cont.)

- Establishing an SSL Connection (con't.)
  - Optionally, if client authentication is used the client will send a certificate verify message
  - Server and client send "ChangeCipherSpec" message indicating they are ready to begin encrypted transmission
  - Client and server send "Finished" messages to each other
    - These are a message digest of their entire conversation up to this point
    - If the digests match then messages were received without interference

SSL Connection Setup


Client (Browser)
Server
1. Client sends *ClientHello* message
2.Server acknowledges with *ServerHello* message
Session Key
3. Server sends its certificate
(4. Server requests client's certificate)
Server Certificate
(5. Client sends its certificate)
Client Certificate
Server's public key
6. Client sends "ClientKeyExchange" message
Server's private key
Digital envelope
X
(7. Client sends a "Certificate Verify" message)
Digital signature
Session key
8. Both send "ChangeCiperSpec" messages
9. Both send "Finished" messages

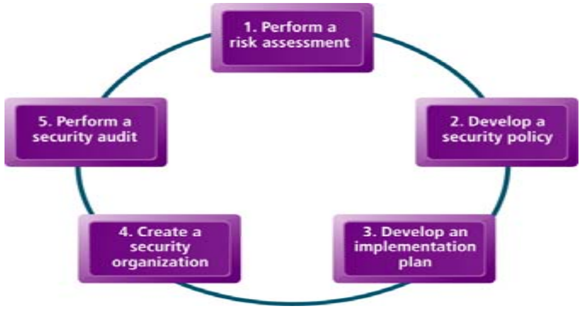
Firewalls and Proxy Servers



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

Developing an E-commerce Security Plan



1. Perform a risk assessment

2. Develop a security policy

3. Develop an implementation plan

4. Create a security organization

5. Perform a security audit

- 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

Q & A

?