Web Security for E-Commerce

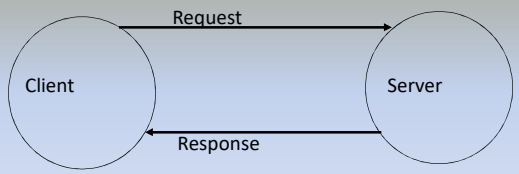
Dr Paras Kothari

Web Concepts for E-Commerce

- Client/Server Applications
- Communication Channels
- TCP/IP

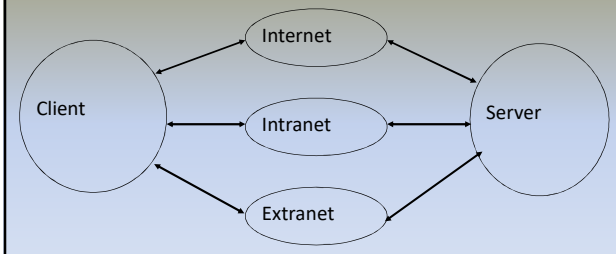
2

Client/Server Applications



3

Communication Channels



4

OSI Model

Application Allows access to network resources

Presentation Translates, encrypts and compresses data

Session Establishes, manages and terminates sessions

Transport Provides end-to-end message delivery & error recovery

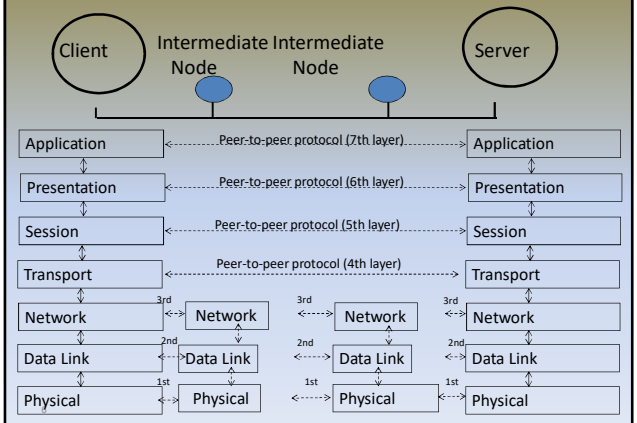
Network Moves packets from source to destination; Provides internetworking

Data Link Organizes bits into frames; Provides node-to-node delivery

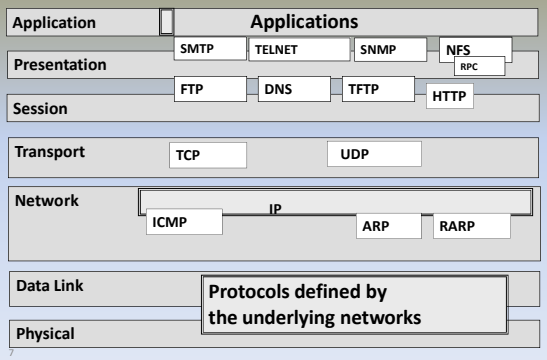
Physical Transmits bits; Provides mechanical and electrical specifications

5

OSI Model cont'd

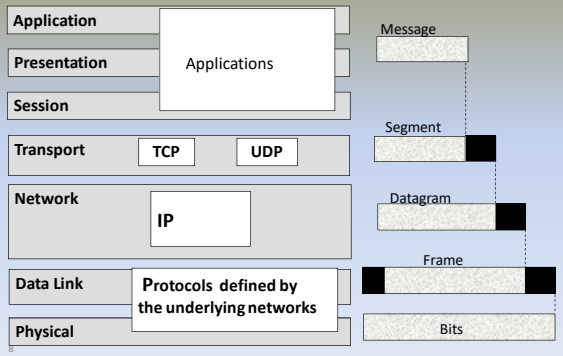


TCP/IP and OSI Model

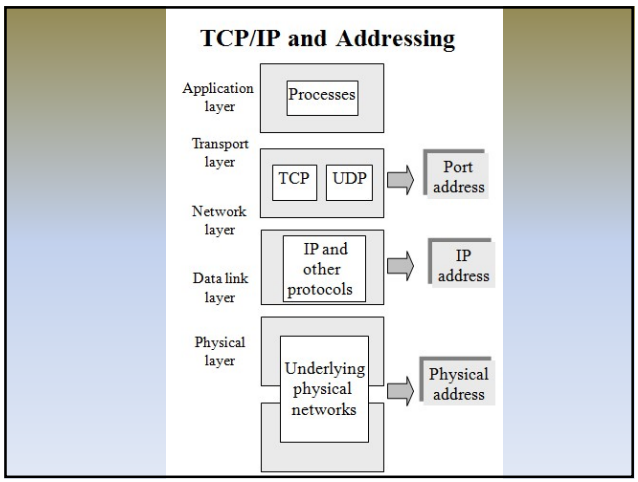


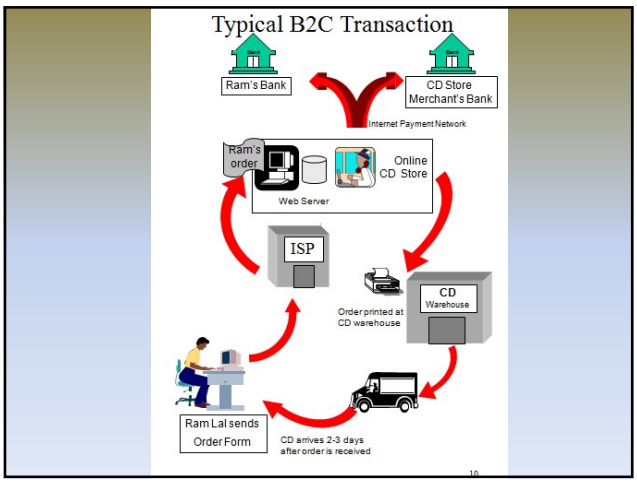
7

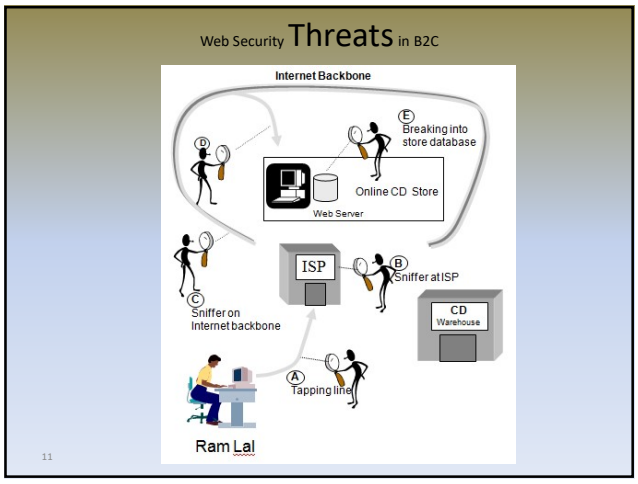
TCP/IP and OSI Model cont'd



8







Security Threats

- Security threats A to D can be handled by providing secure transmission - cryptographic methods
- Threat E and similar types managed by access control methods
- Other types of security threats
  - Illegal access of server computing system (webjacking)
  - Illegal access client computing system
  - Unauthorized use of client information
  - Denial of Service

12

Information Security Threats

- Internet Cryptography Techniques
- Transport Layer Security
- Application Layer Security
- Server Proxies and Firewalls

13

Purpose of Cryptography

- Secure stored information - regardless if access obtained
- Secure transmitted information - regardless if transmission has been monitored

14

Services Provided by Cryptography

- Confidentiality
  - provides privacy for messages and stored data by hiding
- Message Integrity
  - provides assurance to all parties that a message remains unchanged
- Non-repudiation
  - Can prove a document came from X even if X' denies it
- Authentication
  - identifies the origin of a message
  - verifies the identity of person using a computer system

15

Cryptographic Services Allow

- Digital Signatures
  - sign messages to validate source and integrity of the contents
- Digital Envelopes
  - secure delivery of secret keys
- Message Digests
  - short bit string hash of message
- 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

16

Digital Signatures

- Digital Signature
  - 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

17

Digital Envelope

- Public/Private key encryption / decryption useful for internet
- Limitations
  - encryption / decryption slow
  - not reasonable for large documents
- Combine symmetric and asymmetric methods
  - 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

18

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.

19

Digital Certificates (ID)

- Certification Authorities (CA)
  - 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 Case
    - Versign - http://www.versign.com
    - U.S. Post Office - http://www.ups.gov
    - CommerceNet - http//www.commerce.net
  - certificates contain
    - public key
    - e-mail
    - full name
- Digital certificates are secure
  - cannot be forged nor modified

20

Digital Certificates

- 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

21

Secure Channels

- Encrypted Traffic may use
  - Symmetric Key
  - Public/Private Key
- Negotiated Secure Session
  - Secure Socket Layer (SSL)
  - Transport Layer Security (TLS)
  - SSL or TLS provides these services
    - Authenticate users and servers
    - Encryption to hide transmitted data - symmetric or asymmetric
    - Integrity to provide assurance that data has not been altered during transmission
  - SSL or TLS require certificates to be issued by a CA

22

Secure Channels (con't)

- 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

23

Query Session

Confusion comes with lack of understanding … Improve understanding by asking questions