

CIS 375: Layers 6 and 7

Module 8: Spring 2008

Business

- Midterm is next week. Midterm is in Rm 216.
- Take the Sample Quiz ASAP.
- 30 MC questions from the slides/wiki materials.

The Presentation Layer

- (Layer 6)
- This layer contains mechanisms which convert or transform data for transmission or after reception.

Encryption

- SSL Encryption resides on Layer 6
- SSL encryption is based on OpenSSL encryption algorithms.
- The most common use of this protocol
 - HTTPS Port 443
 - Port 80 http connects are the redirected to 443 where keys are exchanged etc.
 - The public key encryption system exchanges private keys.

HTTPS

- Requires the admin to create a public key certificate which is used for exchange of information.

Private key encryption

- Substitution Ciphers (Caesars, et. al.)
- Private key encryption is usually the fastest key approach but has security risks since the keys must be exchanged out of band.
- Likewise, managing many many keys is difficult.

Public Key Encryption

- Using known keys a one way algorithm is used so that what goes in one end is processed against the key and only the other key holder can decipher the result.
 - Plain Text >> Public Key Encipherment >> Public Key >> Ciphertext >> Private Key >> Private key decipherment >> Plain Text – transfer an encrypted document.
 - Plain Text >> Private Key >> Private Key Encipherment >> ciphertext >> public key >> public key decipherment >> signed document.

The Hybrid Approach

- HTTPS uses public key encryption to exchange private session keys (generated each round).
- Private key encryption is then used from that point forward in the session.

Other encryption approaches

- VPN – Virtual Private Networks
 - Uses some encryption scheme to encapsulate packets in an encrypted wrapper. This creates a kind of “tunnel” across the network/internet network which is a private pipeline.
 - This may be used for intranets via the internet as well.

Other Encryption Approaches

- SSH – Uses OpenSSL
- Port 22 daemon
- Also supports SFTP over the same channel
- SSH uses encrypted wrappers viz. VPN.

Yours

- You can use the libs from openssl for creating your own encrypted wrappers programs. Thus you could write a daemon which encrypts and decrypts using the public key or private key approaches in openssl.

Layer 7

- Application Layer – where socket based apps are developed.
 - Application starts and ends the network exchange process.
 - Is really part of the layer 5-7 group of theoretical layers.

Thus...

- If SSH exists on layer 7, it uses layer 6 to encrypt/decrypt, layer 5 to manage the tcp session, layer 4 to create the packets and sequence numbers.
- Other applications on the system may use these protocols to transmit data
 - E.g. Halo 99: Return to Intertrode uses ssh to communicate to the server (even though the user doesn't see it).

Common layer 7 protocols

- FTP 20/21
- SSH 22
- Telnet 23
- SMTP 25
- HTTP 80
- POP 110
- IMAP ??
- S/POP
- S/IMAP
- HTTPS
- DNS
- DHCP

UDP Redux

- Remember UDP is NOT connection based.
- UDP sends a datagram blind and just hopes it arrives.
- No real error checking on this protocol.
- Typically used for things with small data loads that become evident when not complete
 - DNS
 - DHCP