

# CSIS 625 Week 13

## Authentication, Application Layer

Copyright 2001, 2002, 2003 – Daniel R. Oelke

For use by students of CSIS 625 for purposes of this class only.

## I. Overview

### A. Presentation Layer continued

1. Authentication

### B. Application Layer

1. Email
  - a. SMTP
  - b. POP3
  - c. IMAP
2. Web browsing – HTTP
3. Telnet
4. FTP

### C. Final Exam review

### D. Questions

## II. Presentation Layer – continued from last week

### A. Authentication

1. Authentication is the process of making sure that someone is who they say they are.
2. It is also the process of making sure that a message has been transported without being modified.
  - a. Much more than error detection
  - b. Mallory might intercept the message, change it and change the CRC
3. One-way hash
  - a. An algorithm that creates a big hashed number and it is very difficult to produce another message with the same number.
  - b. SHA-1(160 bit hash), MD5 (128 bit hash), RIPEMD (128 bit hash)
4. The secure hash can be sent via another transport mechanism that is secure
5. The secure hash could be encrypted with the sender's private key – allowing everyone to decrypt and check the secure hash
  - a. This assumes that the sender keeps their private key from being stolen by someone else.

### B. Authentication & Encryption

1. Authentication often uses many of the same public key encryption algorithms as encryption.
2. Message tampering detection
  - a. Create a secure hash, and then encrypt using the private key.
  - b. Anyone can then decrypt the hash using a public key and compare the result with their own copy of the public key.

## III. Application Protocols

### A. Email

1. Mail is sent/received by a user's email client
  - a. Standards call this the user agent

2. Message flow using pure Internet standards
  - a. The email client uses SMTP to send the message to a local email server
  - b. The local email server looks up a machine that handles email for that domain name
    - (1) Uses DNS – looks for a specific type of record
    - (2) Uses “MX” records
  - c. local email server sends message to destination email server using SMTP
  - d. Recipient's email client uses POP3 or IMAP to retrieve message from their email server
3. Message flow at either end may be different if using proprietary email clients
  - a. Outlook/Exchange
  - b. Lotus Notes
  - c. etc
4. Generally message flow in the middle is using SMTP

## B. SMTP

1. Simple Mail Transport Protocol
2. An ASCII based protocol for delivery of email messages.
3. A push based protocol – client or server pushes email towards its destination
4. The entire header and body of the email message is considered data to SMTP
5. This means it is relatively simple to forge email as coming from someone else.
6. Open Relay – an SMTP server that accepts email not destined for its users.
  - a. Abused by spammers.
  - b. Several real-time blacklists that mail administrators can use to deny all email from these sites
  - c. A problem as this was the default configuration for most SMTP servers until recently.
  - d. SMTP server that is not an open relay accepts email destined for a domain name that it operates, OR from an email client on one of the network addresses that it maintains.
    - (1) Some SMTP servers do not have network addresses that they maintain other than that machine's address
  - e. Only recently have extensions to SMTP allowed for authentication.
7. See handout for example

## C. POP3

1. Post Office Protocol (Version 3)
2. ASCII based protocol
3. Simple protocol
  - a. Has only mailbox per user
  - b. Can only download and/or delete messages
  - c. No uploading of messages
  - d. No separate folders
4. Older than the more powerful IMAP protocol
5. A pull type protocol in that an email client pulls the email messages from the server

## D. IMAP4

1. Internet Mail Access Protocol (version 4)
2. Another ASCII based protocol
3. More complex (and more features) than POP3
  - a. Handles folders and hierarchies of folders for email messages

- b. Allows client to move individual messages to/from the various folders
- c. Can search the messages on the server (saves bandwidth)
- d. Can download just the headers of messages from the server

#### E. Web based mail

- 1. Not a different protocol – just uses web based protocols to access a program on the server that happens to handle email as it's data.
- 2. The web-mail server may use POP3 as a client to get mail from another server
- 3. The web-mail server probably uses SMTP to send outgoing email messages

#### F. HTTP

- 1. HyperText Transfer Protocol
- 2. ASCII based protocol
- 3. Based on a request / response format
- 4. Version 1.0 could only handle a single request per TCP/IP connection
  - a. this leads to dramatic slow downs in performance when many items are needed because of the 3-way handshake time and slow-start part of TCP/IP
- 5. Version 1.1 add the ability to handle multiple requests in a single TCP connection

#### G. Telnet

- 1. Protocol for remote terminal access
- 2. A binary protocol
- 3. Just a few bytes of information are exchanged between the client and the server when a connection is initiated to determine the characteristics of the terminal type.
  - a. Line ending mode (CR, CR/LF, etc)
  - b. local echo
  - c. erase character
  - d. 7-bit or 8-bit
  - e. etc
- 4. Once initial negotiation is done all information is considered text to display on the user's screen.

#### H. FTP

- 1. File Transfer Protocol
- 2. ASCII based protocol
- 3. One socket/connection for control
- 4. Second socket/connection for data transfer
- 5. Control and error messages have a 3 digit number followed by some text.
  - a. The FTP client software interprets and uses the 3 digit code
  - b. The human users reads and interprets the text
  - c. They should have similar meanings.

### IV. Final Exam

A. 2 hours

B. Closed Book

C. Closed notes –

- 1. Except a single sided 3x5inch note card of crib notes will be allowed
- 2. The note card will have to be stapled to your exam.

D. Same format as the mid-term exam.