CSC 402 – Internet Technology

Recap

- E-mail
- SMTP
- SMTP vs. HTTP
- MIME

Mail Access Protocol

- A typical user reads mail with a user agent that executes on his local machine.
- By executing the user agent on a local PC, users enjoy a rich set of features, including the ability to view multimedia messages and attachments.
- There are currently two popular mail access protocols.
    - POP3 (Post Office Protocol - Version 3).
    - IMAP (Internet Mail Access Protocol).

POP3

- Defined in RFC 1939
    - A very simple mail access protocol.
    - Rather limited functionality.
- POP3 operation begins when the user agent (the client) opens a TCP connection to the mail server (the server) on port 110.
- With the TCP connection established, POP3 progresses through three phases:
    - Authorization.
    - Transaction.
        - User agent retrieves messages, user agent can also mark messages for deletion, remove deletion marks, and obtain mail statistics.
    - Update
        - Occurs after the client has issued the quit command, ending the POP3 session.
        - Mail server deletes the messages marked for deletion.
- In a POP3 transaction, the user agent issues commands, and the server responds to each command with a reply.
- There are two possible responses:
    - +OK (sometimes followed by server-to-client data), server confirms that the previous command was fine.
    - -ERR, server states that something was wrong with the previous command.

POP3 Drawbacks

- After a user has downloaded his messages to the local machine using POP3 possible actions include:
- Creating mail folders and move the downloaded messages into the folders.
- Deleting messages, moving them across folders, searching for messages (by sender name or subject).
- Problematic for a nomadic user
  - Folders and messages located in the local machine.
  - What if the user wants to maintain a folder hierarchy on a remote server that can be accessed from any computer?
    - Impossible with POP3.

IMAP

- To solve this and other problems, the Internet Mail Access Protocol (IMAP), defined in RFC 2060, was proposed.
  - Like POP3, IMAP is a mail access protocol.
- Many more features than POP3.
  - Allows users to manipulate remote mailboxes as if they were local
  - Provides commands that allow user to search remote folders for messages matching specific criteria.
- IMAP implementation is much more complicated than a POP3
  - IMAP server must maintain a folder hierarchy for each user.
  - This state information persists across a particular user's successive accesses to the IMAP server.
- Recall that a POP3 server does not maintain any information about a particular user once the user quits his POP3 session.

Telnet

- Remote terminal protocols that runs in application layer TELetype NETwork – application-layer protocol used for setting up a terminal session with a remote host in client-server manner.
  - Also referred to as remote session protocol.
  - Dates back to 1969.
    - First RFC was issued in 1971 (RFC137).
    - Predates currently used protocol stack model.
- Current version follows the RFC854 from 1983.
  - Running on top of TCP using port 23.

Telnet

- Telnet protocol defines an interactive, text based communication session between a client and a host.
  - Simple and straight-forward.
  - Sessions are not encrypted – messages are send in plain text.
- Telnet is also the name of the application providing the client side of the Telnet protocol.
- Due to its vulnerability, on most machines TELNET was substituted by the SSH protocol.

SSH

- SSH (Secure SHell) – has the same functionality as Telnet, but comes with public-key cryptography for authenticating users and encrypting the exchanged data.
  - The first version, SSH-1 was proposed in 1995 by Tatu Ylönen, a researcher at Helsinki University of Technology.
  - ‘Made in Finland’.
  - In 1996 a revised version called SSH-2 was designed.
    - It became an official Internet standard in 2006 (RFC4251).
- SSH protocol consists of three major components
  - The Transport Layer Protocol.
    - Provides server authentication, confidentiality, and integrity with perfect forward secrecy.
  - The User Authentication Protocol.
    - Authenticates the client to the server.
  - The Connection Protocol.
    - Multiplexes the encrypted tunnel into several logical channels.

PGP

- Sending an email between two distant sites means that the email has to transit dozens of machines on the way.
  - Those machines may read and record the message.
  - Privacy is thus non-existent by default.
- There are systems for secure e-mails.
  - PGP (Pretty Good Protocol) being one of them. It is a protocol for signing and encrypting email.
- Essentially the product of one single person – Phil Zimmermann released on 1991.
  - RFC 1991 (now obsolete), 2440, 4880, and 5581.
  - Complete email security package providing privacy, authentication, digital signatures, and compression in an easy-to-use form
  - Complete package, including source code distributed freely on Internet: e.g., www.pgpi.org
  - Available on Unix, Linux, Windows, Mac OS
  - Based on IDEA for encryption (128-bit key), RSA for key management, MD5 for data integrity

PGP

- Controversy surrounding PGP
  - No license was required for its non-commercial use. There was not even a nominal charge and the complete source code was included with all copies.
  - Zimmermann did nothing to stop people from posting PGP on websites – US government claimed that he violated US laws (they compared it with export of arms and ammunition) and investigated the case for 5 years before dropping it.
  - He, himself, never posted PGP on a website.
  - Patent infringement: RSA Security Inc claimed that PGP's use of RSA infringed on its patent (eventually settled); same problems with using IDEA
  - Many version of PGP exist – users can download and modify the code. Discuss here original PGP. Other versions: Open PGP, GNU Privacy Guard, etc.

PGP

- Many version of PGP exist – users can download and modify the code. Other versions: Open PGP, GNU Privacy Guard, etc.
- Sending a message:
  - Alice first hashes her message with MD5 and then encrypts the hash with her private RSA (RSA algorithm; Rivest-Shamir-Adleman algorithm) key.
    - RSA key is a private key based on RSA algorithm. Private Key is used for authentication and a symmetric key exchange during establishment of an SSL/TLS (Transport Layer Security, Secure Sockets Layer (SSL)) session.
  - Encrypted hash and message are concatenated and encrypted with ZIP (based on Lempel-Ziv algorithm)
  - PGP asks the user for a random input from the keyboard
    - Based on the input and on the typing speed, PGP generates a 128-bit message key.
    - Key KM is then encrypted with Bob's public key.
  - The two components are concatenated and converted to base64.
    - Some email software only allows sending ASCII text.
    - Converting to base64 will give the symbols.
- Receiving a message
  - Bob reverses the base64 encoding and decrypts the IDEA key with his own private key.
  - Using this key he decrypts the message to get P1.Z and decompresses it.
  - Separate the plaintext from the encrypted hash and decrypt the hash with Alice's public key.
  - Compute the hash of the message and check the match with the received hash.

PGP

- PGP supports 4 RSA key lengths and it is up to the user to select the appropriate one according to his needs.
    - Casual (384 bits) – easily broken today
    - Commercial (1024 bits) – breakable by “three-letter” organizations
    - Military (2048 bits) – not breakable by anyone on Earth
    - Alien (4096 bits) – not breakable by anyone on other planets, either?!
    - Since RSA is only used on 256 bits, everyone should use alien keys
- Key management: Private and Public Key

PGP

- Private key
  - Each user maintains two data structures locally: a private key ring and a public key ring
  - Private key ring contains one or more personal private-public key pairs
    - One may have more than one pair
    - Each pair has an identifier – the low-order 64 bits of the public key.
      - Users are responsible to create public keys with different identifiers.
    - The private keys on disk are kept encrypted using a special (arbitrarily long) password.
  - The public key can be uploaded on dedicated servers: e.g. keyserver.pgp.com.
- Public key
  - Public key ring contains public keys of the user's correspondents and their IDs, plus an indication of how strongly the user trusts the key.
  - When the user inserts a new public key, PGP is asserting the trust the user has in that key: key legitimacy field (computed by PGP)
  - To revoke a public key, the user should issue a key revocation certificate, signed by the owner – this is just like a normal signature certificate; the user should send this revocation certificate to everybody he knows as quickly as possible