ISA 563: Fundamentals of Systems Programming

Secure Socket Programming

April 30, 2012

Communication over Network

- Data communication is not secured by default under TCP IP protocols
- Data can be read and modified by third parties
- Need a mechanism to support data encryption and decryption

Secure Socket Layer

- SSL is a standard for secure communication over the Internet
- Achieves security through integrating data cryptography into the protocol
- Encryption and decryption happen at communication end-points
    - It is (or should be) infeasible to decrypt intercepted data
- SSL can be used with different protocols:
    - HTTP, IMAP, FTP, ...

SSL (cont'd)

- SSL tries to ensure that communication is secure
- Server could be malicious:
  - faking some other server
    - https://www.paypal.com
  - With all letters lower case, the above URL is:
    - https://www.paypai.com
- Client could be malicious:
  - can attack server as usual
- Infrastructure and human factors are important

OpenSSL

- An open source implementation of SSL/TLS protocols
- Also provides:
  - encryption/decryption of files
  - hashing
  - digital certificates
  - digital signatures
  - random number generator
  - command line tools

OpenSSL Client Operations

- Initialize security context
- Open client socket as usual
- Add client socket to SSL connection
- Communicate using SSL
- Close SSL connection
- Clean up

SSL Client Demo

wclient.c