Network II
CS 184
IP and TCP Protocol Security

Department of Computer Science
George Washington University

Relevant Reading

- Relevant reading:
  - Security Problems in the TCP/IP Protocol Suite by Steve Bellovin. Computer Communications Review, Vol 19, No. 2, pp 22-48, April 1989.
  - Sequence Integrity using Hash Chains by Matt Barrie. http://www.ee.usyd.edu.au/~mattb/2001/lectures/attacks.pdf
  - Bugtraq Mailing list http://online.securityfocus.com/popups/forums/bugtraq/faq.shtml
  - Vulnerability Database http://online.securityfocus.com/bid
  - Crypto-Gram Newsletter http://www.counterpane.com/crypto-gram.html
  - CERT Statistics http://www.cert.org/stats/cert_stats.html

What are Network Security Risks?

- Information disclosure:
  - IP addresses and DNS names of machines, active ports, network topology.
- Connection Capture (Man-in-the-middle)
  - TCP connection capture.
  - Modified DNS replies.
- DOS
  - Network traffic DOS
    - Ping, SYN-flood, …