A Framework of Web Security

- Web System is composed of:
  - The Client
  - Client’s Operating System
  - Client’s Local Area Network
  - The Internet
  - The Server’s LAN
  - The Server’s Host Operating System
  - The Web Server Program

- The security of Web System can be compromised by holes in any of these components.

Firewalls & The Web

- A Firewall is a security mechanism which protects the computer and data on a private local area network from the uncontrolled activities of untrusted users and software on another network.

- Security Enhancement Devices:
  - Packet Filters
  - Circuit Gateway
  - Application Proxy
Security over Public Network

Tools
- Cryptography
  - Private Key
  - Private/Public Key
- Message Digest
- Digital Certificates
- Certificates
Secure HTTP

Developed by CommerceNet, Palo Alto, CA. NCSA Mosaic Supports it.

Secure Socket Layer (SSL)

Netscape uses SSL 2.0 and Microsoft® has a copy PCT (Private Communications Technology).

Security Toll Booth

- How do clients know that a server’s public key is valid? What keeps an imposter server from sending its public key instead?
  - The answer is “trusted” certificate authority that signs the public key.
  - Netscape Commerce Server requires a digital certificate. A browser will only authenticate a server which has a key signed by Netscape® (not available to public), or VeriSign® (an RSA spinoff company).
  - It costs $295 for first server, and $75 additional servers for first year. $75 thereafter each year to get a certificate.
  - Soon USPS will compete with VeriSign®.

SSL or S-HTTP?

- Neither is complete, and both are still under development.
- S-HTTP provides ultimate control to user.
  - Each document can have separate certificate and authentication.
  - Difficult to manage.
- SSL easy to manage and transparent.
  - But the security stops at the SSL layer.
  - Can be used for FTP, Telnet.
Battle Continues..

- Leading encryption company RSA which has billed itself the most trusted name in e-security has had its web site successfully compromised twice recently, and seems to have changed web server platforms on each occasion.

- On Thursday 10th February www.rsa.com was running Solaris and Netscape-Enterprise. By Sunday 13th it had switched to Linux and Apache/2.0, while today (Monday 14th February) it is running NT4 and Microsoft-IIS/4.0. It would be interesting to know the reasons for these changes; sometimes companies change platforms as a knee jerk reaction to a security or reliability problem, but going through the three most common platforms in four days seems exceptional. Presumably at least one of the attacks was a subversion of the DNS entry for www.rsa.com (checklist email from netcraft).

Interested in Learning More?

- We will learn more on Internet Security on the advanced IAD class:

  - Topics to cover:
    - Public Key cryptography
    - X.509 digital certificates.
    - Virus spreading models.
    - Virus detection & removal techniques.
    - Distributed denial of service
    - Intrusion detection