

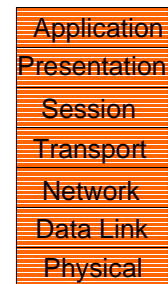
CSE/EE 461 – Lecture 23-supp

Network Security

David Wetherall
djw@cs.washington.edu

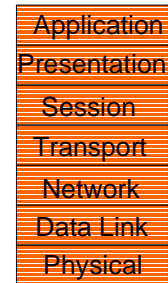
Last Time

- Network security
- Focus
 - How do we secure distributed systems?
- Topics
 - Privacy, integrity, authenticity
 - Cryptography



This Time

- Network security
- Focus
 - How do we secure distributed systems?
- Topics
 - Example protocols
 - Firewalls
 - Read Peterson 8.3, 8.4



Key Distribution

- Public key systems depend on the distribution of keys!
 - Public Key Infrastructures (PKIs), e.g., Verisign
 - An Achilles heel?
- Certificates (X.509)
 - Distribute keys by trusted certification authority (CA)
 - “I swear X’s public key is Y”, signed by CA
 - Still requires bootstrapping ...
 - Also allows us to can build chains of trust
 - e.g., public keys for a domain name so that “.edu” (root) certifies “washington.edu”’s key, they certify “cs...”’s key ...
 - Certificate Revocation Lists needed to “undo” associations!

Example Systems

- Pretty Good Privacy (PGP)
 - For authentic and confidential email
- Secure Sockets (SSL) and Secure HTTP (HTTPS)
 - For secure Web transactions
- IP Security (IPSEC)
 - Framework for encrypting/authenticating IP packets

PGP

- Application level system
- Based on public keys and a “grass roots” Web of trust
- Sign messages for integrity/authenticity
 - Encrypt with private key of sender
- Encrypt messages for privacy
 - Could just use public key of receiver ...
 - But encrypt message with secret key, and secret key with public key of receiver to boost performance

SSL/TLS and HTTPS

- Secure transport layers targeted at Web transactions
 - SSL/TLS inserted between TCP and HTTP to make secure HTTP
- Extra handshake phase to authenticate and exchange shared session parameters
 - Such as secret keys used for encryption
 - Client might authenticate Web server but not vice-versa
 - Certificate Authority embedded in Web browser
- Performance optimization
 - Refer to shared state with session id
 - Can use same parameters across connections
 - Client sends session id, allowing server to skip handshake

djw // CSE/EE 461, Winter 2001

L23-sup.7

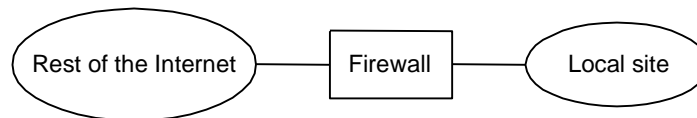
IPSEC

- Framework for encrypted and authenticated IP packets
 - Choice of algorithms not specified
- Uses new protocol headers inside IPv4 packets
 - Authentication header
 - For message integrity and origin authenticity
 - Optionally “anti-replay” protection (via sequence number)
 - Encapsulating Security Payload
 - Adds encryption for privacy
- Depends on key distribution (ISAKAMP)
 - Sets up security associations
- Example use: secure tunnels between corporate offices

djw // CSE/EE 461, Winter 2001

L23-sup.8

Filter-based Firewalls

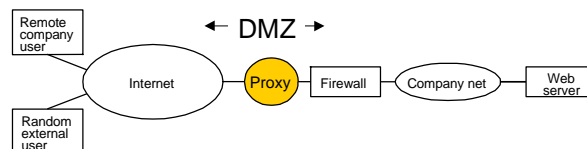


- Sit between site and rest of Internet, filter packets
 - Enforce site policy in a manageable way
 - e.g. pass (*,*, 128.7.6.5, 80), then drop (*, *, *, 80)
 - Rules may be added dynamically to pass new connections
- Sometimes called a “level 4” switch
 - Acts like a router (accepts and forwards packets)
 - But looks at information up to TCP port numbers (layer 4)

djw // CSE/EE 461, Winter 2001

L23-suppl.9

Proxy-Based Firewalls



- Problem: Filter ruleset can be complex/insufficient
 - Adequate filtering may require application knowledge
- Run proxies for Web, mail, etc. just outside firewall
 - In the “de-militarized zone” DMZ
 - External requests go to proxies, only proxies connect inside
 - External user may or may not know this is happening
 - Proxies filter based on application semantics

djw // CSE/EE 461, Winter 2001

L23-suppl.10