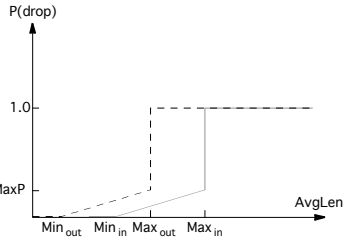
Differentiated Services

- Problem with IntServ: scalability
- Idea: segregate packets into a small number of classes
  - e.g., premium vs best-effort
- Packets marked according to class at edge of network
- Core routers implement some per-hop-behavior (PHB)
- Example: Expedited Forwarding (EF)
  - rate-limit EF packets at the edges
  - PHB implemented with class-based priority queues or Weighted Fair Queue (WFQ)

DiffServ (cont)

- Assured Forwarding (AF)
  - customers sign service agreements with ISPs
  - edge routers mark packets as being “in” or “out” of profile
  - core routers run RIO: RED with in/out



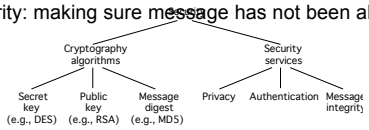
- http://www.debone.com/videoLinks.html
- http://www.earthcam.com/usa/newyork/timessquare/livestream.html

Chapter 8: Security

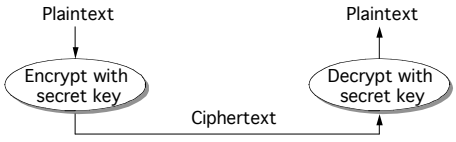
- Outline
  - Encryption Algorithms
  - Authentication Protocols
  - Message Integrity Protocols
  - Key Distribution
  - Firewalls

Overview

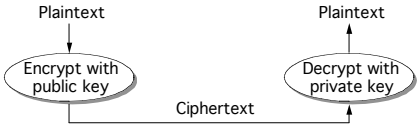
- Cryptography functions
  - Secret key (e.g., DES)
  - Public key (e.g., RSA)
  - Message digest (e.g., MD5)
- Security services
  - Privacy: preventing unauthorized release of information
  - Authentication: verifying identity of the remote participant
  - Integrity: making sure message has not been altered



Secret Key (DES)



Public Key (RSA)



- Encryption & Decryption

$c = m^e \bmod n$

$m = c^d \bmod n$

Message Digest

- Cryptographic checksum
  - just as a regular checksum protects the receiver from accidental changes to the message, a cryptographic checksum protects the receiver from malicious changes to the message.
- One-way function
  - given a cryptographic checksum for a message, it is virtually impossible to figure out what message produced that checksum; it is not computationally feasible to find two messages that hash to the same cryptographic checksum.
- Relevance
  - if you are given a checksum for a message and you are able to compute exactly the same checksum for that message, then it is highly likely this message produced the checksum you were given.

IP Security

- Payload is in the clear text - anyone in the middle can see it
- No way of knowing who the sender is - just trust the header
- No way of knowing if the data was modified - checks protect against network errors, not malicious attacks
- Solution: Virtual Private Network (VPN)
  - Make node appear in the same network as say a company, while actually outside the network
  - IPSEC is a secure VPN technology

IPSEC

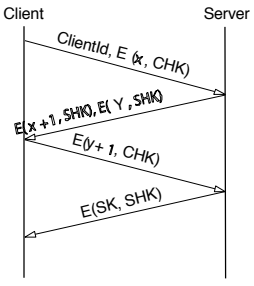
- Authentication - Know the sender
- Encryption - Cannot eves drop
- Operates in host-to-host or host-to-network or network-to-network modes
- With Two Major modes
  - Tunnel
  - Transport
    - AH (Authentication Header)
    - ESP (Encapsulating Security Protocol)
    - AH + ESP

Exchanging Keys

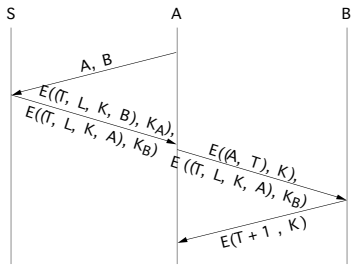
- Exchange keys between client and server
  - Manual Keying
  - Internet Security Association and Key Management Protocol (ISAKMP)
  - Certificates
- IPSEC:
  - Works for all IP datagrams (UDP, TCP, RTSP, etc.)
  - Complicated to setup and not interoperable (yet)
- Application level:
  - SSL, SSH tunnels

Authentication Protocols

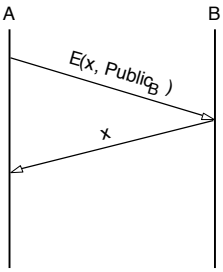
- Three-way handshake



- Trusted third party (Kerberos)



- Public key authentication



Message Integrity Protocols

- Digital signature using RSA
  - special case of a message integrity where the code can only have been generated by one participant
  - compute signature with private key and verify with public key
- Keyed MD5
  - sender: m + MD5(m + k) + E(k, private)
  - receiver
    - recovers random key using the sender's public key
    - applies MD5 to the concatenation of this random key message
- MD5 with RSA signature
  - sender: m + E(MD5(m), private)
  - receiver
    - decrypts signature with sender's public key
    - compares result with MD5 checksum sent with message

Message Integrity Protocols

- Digital signature using RSA
  - special case of a message integrity where the code can only have been generated by one participant
  - compute signature with private key and verify with public key
- Keyed MD5
  - sender: m + MD5(m + k) + E(E(k, rcv-pub), private)
  - receiver
    - recovers random key using the sender's public key
    - applies MD5 to the concatenation of this random key message
- MD5 with RSA signature
  - sender: m + E(MD5(m), private)
  - receiver
    - decrypts signature with sender's public key
    - compares result with MD5 checksum sent with message

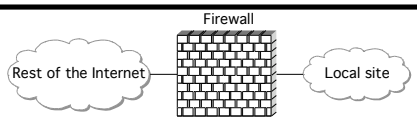
Key Distribution

- Certificate
  - special type of digitally signed document:
    - "I certify that the public key in this document belongs to the entity named in this document, signed X."
  - the name of the entity being certified
  - the public key of the entity
  - the name of the certified authority
  - a digital signature
- Certified Authority (CA)
  - administrative entity that issues certificates
  - useful only to someone that already holds the CA's public key.

Key Distribution (cont)

- Chain of Trust
  - if X certifies that a certain public key belongs to Y, and Y certifies that another public key belongs to Z, then there exists a chain of certificates from X to Z
  - someone that wants to verify Z's public key has to know X's public key and follow the chain
- Certificate Revocation List

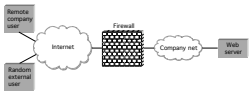
Firewalls



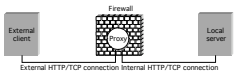
- Filter-Based Solution
  - example
    (192.12.13.14, 1234, 128.7.6.5, 80)
    (*,*, 128.7.6.5, 80)
  - default: forward or not forward?
  - how dynamic?
  - stateful

Proxy-Based Firewalls

- Problem: complex policy
- Example: web server



- Solution: proxy



- Design: transparent vs. classical
- Limitations: attacks from within

Denial of Service

- Attacks on end hosts
  - SYN attack
- Attacks on routers
  - Christmas tree packets
  - pollute route cache
- Authentication attacks
- Distributed DoS attacks