Message Digest

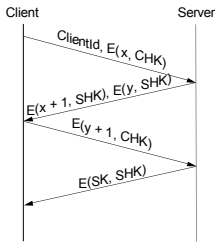
- Cryptographic checksum
  - just as a regular checksum protects the receiver from accidental changes to the message, a cryptographic checksum protects the receiver from malicious changes to the message.
- One-way function
  - given a cryptographic checksum for a message, it is virtually impossible to 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.

Authentication

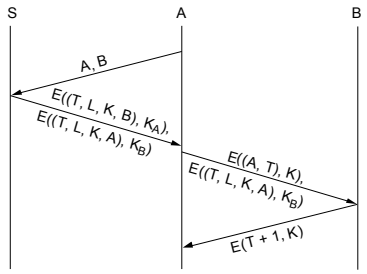
- Identification verification process
  - E.g. kerberos certificates, digital certificates, smart cards
- Used to grant resources to authorized users

Authentication Protocols

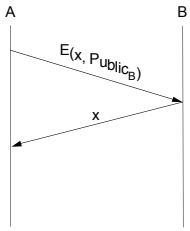
- Three-way handshake



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

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)

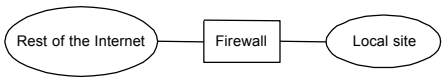
- Chain of Trust
  - if *X* certifies that a certain public key belongs to *Y*, and *Y* certifies that another public key belongs to *Z*, then there exists a chain of certificates from *X* to *Z*
  - someone that wants to verify *Z*'s public key has to know *X*'s public key and follow the chain
- Certificate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

Common technology - firewalls

- Firewalls are used to restrict the kinds of network traffic in/out of companies
  - Application level proxies
  - Packet level firewalls
- Does not prevent end-to-end security violations
  - People sometimes email list of internal computer users outside firewall to scrupulous "researchers"
  - Emails viruses exploit certain vulnerabilities in VBS to get around firewalls

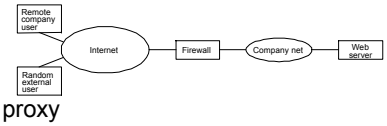
Firewalls

- 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?

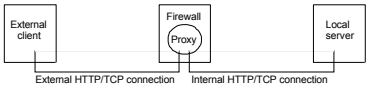


Proxy-Based Firewalls

- Problem: complex policy
- Example: web server



- Solution: proxy



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