



Security

March 9, 2001



Security

What is security?

- Techniques that control access to use a shared resource
 - Uses of shared resource must be authorized
- Authorized - who, what when, why
 - IRS agent authorized to access a tax evader's files, but what about agent's neighbor's files?
- Controlling access is a negative goal
 - Hard to prove that no unauthorized access occurred

2



Security, cont.

Examples of Security Techniques

- Tickets
- Access Control Lists
- Encryption (e.g., PGP)
- EM shielding
- Pad Locks
- Independent certifications
- Obscurity

3



Security, cont.

Security Is Very Difficult

- Suppose every email message out of your computer is intercepted and read by a human
- Can you nevertheless send out the contents of a 1 Gig file undetected, using email?
 - Yes, lots of ways
- Use metadata to hide 1 Gig file
 - Much slower, but effective

➡ Time value of data varies

4



Design Principles

- KISS - Keep It Small and Simple
- Fail-safe defaults (e.g., permission, not exclusion)
- Complete, systematic, and holistic approach
- Open design
- Explicit assumptions
- Least authority
- Human acceptability
- Immediate feedback

5



Example: Virtual Memory

- Distinct pages for data
 - Virtual page number must be in page map
- Distinct memory spaces for processes
 - Hardware - page map address register points to a process's page map
- Kernel/User bit
 - Authorizes access to page map address register
 - Can be set only to Kernel by user program and vice versa

6



Protecting Information - No Guarantees

- Not practical to try to fully protect some information
 - e.g., Medical records from doctors, IRS data from IRS agents
- To better protect, use authentication and log who did what, when, and why
- Allow interested parties to audit the log

7



Protecting Information - Cryptography

- Idea - Reversibly transform plaintext into seemingly random ciphertext
 - Plaintext - the original text
 - Ciphertext - the encrypted text
- 6 main categories of attack:
 - Ciphertext-only, known plaintext, chosen plaintext, adaptive chosen plaintext, chosen ciphertext, adaptive ciphertext

8



Protecting Information - Public/Private Keys

- An entity has a private (secret) key K_s , and a public key K_p
- K_s and K_p are computed in private by an entity
 - No need to share K_s !
- $\{\{\text{message}\}K_s\}K_p = \{\{\text{message}\}K_p\}K_s = \text{message}$

➔ Can be used for securing communication channels as well as for authentication

9



Server-Mediated Authentication

- Two users want to communicate
- Use a trusted server to connect them
- Server can use public key encryption
 - No need to store user's private keys
- Server responds to host1 comm. request with $\{\{\text{session-key}, K_{\text{host1}}\}K_{\text{host2}}, \text{session-key}\}K_{\text{host1}}$
- Host 2 can now authenticate Host 1, and communicate on an encrypted channel

10



X.509 Certificates

- Used by SSL
- Issued by well-known certificate authorities (e.g., Verisign)
- Contain the issuer's name + signature, issuee's name + issuee's public key, valid dates, admin info
- To verify, need to securely obtain certificate authority's public key
 - e.g., send $\{\text{signature}, \text{nonce}, K_{\text{client}}\}K_{\text{cert}}$, receive $\{\text{issuee name}, \text{public key}, \text{valid dates}, \text{nonce}\}K_{\text{client}}$

11



SSL

- Step 1 - Exchange certificates
 - Certificate authenticates a user
 - Certificate-issuing service must be recognized by both parties
- Step 2 - Establish cipher
 - Flexibility - can use different ciphers
 - Use a pre-master key to generate session keys

12