Security and Protection

Prof. James L. Frankel
Harvard University

Version of 7:33 PM 20-Nov-2018

Security and Protection

- Confidentiality/Privacy
  - Keep secret data secret
- Integrity
  - Data can be modified only with permission
- Availability (Denial of Service attacks)
  - Systems must remain accessible and usable
- Authenticity
  - There should be evidence that the system and data are real
- Accountability
  - It should be possible to determine what was done to data or a system
- Non-repudiability
  - Proof of authenticity & integrity with high confidence
- Etc.

Intruders

- Casual prying by non-techies
- Snooping by insiders
- Determined attacks to make money
- Commercial & military espionage

Accidental Data Loss

- Acts of God
- HW & SW errors
- Human errors

Authentication (1 of 2)

- How break-ins occur?
- Don't indicate if the login name is incorrect
  - Can happen with an early error response (no such user)
  - Can happen with a message after login name and password
  - Can happen with a request to unlock an account with lost password
- Weak passwords by users
- Unreadable password file with clear text passwords in the password file
- Encrypted passwords
  - Always encrypt and store and compare the encrypted forms
- Use a “Salt” with each password
  - Salt is stored with the password in the file
  - Salt is concatenated with the password and then encrypted
  - Must be done with each possible password for each account
  - Each password is encrypted with different random data

Authentication (2 of 2)

- One time passwords
  - List of passwords
  - One-way Hash Chain (Leslie Lamport, 1981)
    - Function: y = f(x); Given x, easy to determine y, but not vice versa
    - Secret password: s; Number of passwords: n
    - If n = 4: $Password_1 = f(f(f(f(s))))$; $Password_2 = f(f(f(s)))$; $Password_3 = f(f(s))$; $Password_4 = f(s)$
- Challenge/response
- Physical object
  - SecurID
  - Chip in card (smart card)
- Biometrics
  - Fingerprints
  - Iris recognition
  - Face recognition
  - Signature analysis
  - Voice biometrics

Insiders

- Logic bombs
- Back doors
- Login spoofing
- Rootkits

Attacks

- Trojan Horses
  - Pretends to be useful software, but has a malicious purpose as well
- Viruses
  - Spread through distribution of a file
- Worms
  - Spread by themselves
- Spyware
  - Gathers information without a user’s permission or knowledge

Exploiting Code Bugs

- Buffer overflow
  - Stack canaries
- Format string
- Dangling pointers (using memory after freeing it)
- Integer overflow
- Command injection
- Time-of-check to time-of-use attack (TOCTTOU)
  - Something changes between the time that a precondition is checked and the time at which an attack is made
  - That time difference allows the attack action to take place even though it should not be allowed

Gaining Privileged Access

- Gaining privileged access through the OS kernel
  - HW: CPU, memory pages, disk drives, printers
  - SW: processes, files, databases, semaphores
- Gaining privileged access through setuid root/setgid programs

Principle of Least Authority (POLA)

- Need to Know

ACLs – Access Control Lists

- **Principals** have access to **Objects**
- Specific **rights** are granted
- Some ACLs can also deny certain rights in addition to granting them

- NTFS in Windows implements ACLs for file access
  - It has both granted and denied ACL rights

Capabilities

- A list of **objects** and **rights** are associated with **each process**

Cryptography

- Secret-key (or symmetric-key) cryptography (examples are AES, RC4)
  - Usually it is fairly easy to determine the decryption key given the encryption key
    - Sometimes they are even the same
  - The shared keys for both encryption and decryption make this technique less desirable
- Public-key cryptography (Diffie-Hellman)
  - Different keys for encryption and decryption
  - Given one, it is virtually impossible to discover the other
  - Encryption key can be made public

Crypto Examples

- Q1: multiply $\pi \times \pi$
- Q2: determine the square root of π^2

- RSA uses multiplying and factoring hundreds of digits with modulo math

- One-way functions
- Crypto hashes
  - MD5 16 byte
  - SHA-1 20 byte
  - SHA-256 32 byte
  - SHA-512 64 byte

Bell-LaPadula Model – Enforces Secrecy

- Documents (objects) have a security level
- People (processes) also have a security level

- Process at security level *k* can read objects at its level or lower
- Process at security level *k* can write objects at it level or higher

- This guarantees that a process cannot leak data to lower levels
- This guarantees that a process cannot access data at higher levels

Biba Model – Enforces Integrity (just the opposite)

- Process at security level *k* can write objects at its level or lower
- Process at security level *k* can read objects at its level or higher

- This guarantees that a process cannot write data that would destroy the integrity of higher level documents
- This guarantees that a process will read data (*i.e.,* be directed) by higher levels

Dilemma Between Maintaining Secrecy & Integrity

- Difficult to maintain both secrecy and integrity

Covert Channels

- Steganography
  - Embed information in public, non-encrypted data
  - For example, embed a message in a large image file (JPEG, MPEG, GIF, etc.)