Outline

- Chapter 18: Protection
- Chapter 19: Security

Protection

- Protect computer resources from being accessed by processes that should not have access
  - Access right: Operations allowed on an object
  - Domain: Set of all access rights
- UNIX: domain is userid, setuid bit in file switches domains
- Multics: rings, tasks can get access based on entry points
- Access Matrix defines protection: rows represent domains & columns represent objects
  - Global table
  - Access list for objects: easier to program
  - Capability list for domains/users:
  - Hybrid: lock-key mechanism
- Revocation of rights:
  - Immediate vs delayed, selective vs general, partial vs total, temporary vs permanent

Revocation

- *Access List* – Delete access rights from access list.
  - Simple
  - Immediate

- *Capability List* – Scheme required to locate capability in the system before capability can be revoked.
  - Reacquisition
  - Back-pointers
  - Indirection
  - Keys

Compiler/language based mechanism

- Compiler based enforcement
  - Specification of protection in a programming language allows the high-level description of policies for the allocation and use of resources

- Java VM
  - Multiple threads within a single JVM have different access rights
- A class is assigned a protection domain when it is loaded by the JVM. The protection domain indicates what operations the class can (and cannot) perform
  - Protection enforced using stack inspection

Security

- Security problem: protection from unauthorized access, malicious modification or destruction
- User authentication:
  - Passwords
    - Encrypted passwords
      - Encrypted form should be secret because attacker can check offline
    - One-time passwords
    - Biometrics
- Threats:
  - Trojan horse
  - Trap door/stack and buffer overflow
  - Worms/viruses
  - Denial of service
  - Intrusion and detection

Risk analysis

- Important to understand threat and perform risk analysis
  - No system is “secure”, systems usually trade security for performance, ease of use etc.
  - If information is worth **x** and it costs **y** to break into system and if (**x** < **y**), then not worth encryption
  - Wasteful to build a system that is more secure than is necessary
    - Ssh in CSE dept – good
  - Palm pilots may not require powerful encryption systems if they are expected to be physically secure

Security classification

- U.S. Department of Defense outlines four divisions of computer security: A, B, C, and D
  - D – Minimal security
  - C – Provides discretionary protection through auditing. Divided into C1 and C2. C1 identifies cooperating users with the same level of protection. C2 allows user-level access control
  - B – All the properties of C, however each object may have unique sensitivity labels. Divided into B1, B2, and B3
  - A – Uses formal design and verification techniques to ensure security
- Windows NT: Configurable security from D to C2
- SuSE Linux Enterprise Server 8 on IBM eServer xSeries - Evaluation Assurance Level 2+ certification (EAL2)
- http://www.radium.ncsc.mil/tpep/epl/historical.html

Security Attacks

- Social engineering attacks
  - Preys on people gullibility (good nature), hardest to defend
    - E.g. I once got an unlisted number from a telephone operator because I sounded desperate (I was, but that was not the point)
    - E.g. Anna kour*va virus, Nigerian email scam, MS update scam
    - E.g. If I walk in with coupla heavy looking boxes into the elevator to go to Fitz 3rd floor (at night) would you let me in? You can get into “secure” companies by looking like you “belong” there
- Denial of service attacks
  - Network flooding, Distributed DOS, holding resources, viruses

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

Intrusion detection

- Detect attempts to intrude into computer systems.
- Detection methods:
  - Auditing and logging
  - Tripwire (UNIX software that checks if certain files and directories have been altered – I.e. password files)
- System call monitoring