Computer and Network Security

R. E. Newman

Computer & Information Sciences & Engineering
University Of Florida
Gainesville, Florida 32611-6120
nemo@cise.ufl.edu

General Purpose Operating System Security (Pfleeger 4/e Ch. 4; 2/e Ch. 6)

Hardware Engineering!

More Software Engineering!

1 Protection Services for Operating Systems

1.1 Goals

1. Inescapable mediation - check every access
2. Least privilege - need-to-know
3. Verify acceptable usage - sematantics

1.2 What is to be protected/shared?

1.2.1 CPU

1.2.2 Memory

1.2.3 Serially sharable devices

1. printer
2. tape

1.2.4 (pseudo-) Concurrently sharable resources

1. disk

1.2.5 Code

1. programs
2. subroutines
3. libraries

1.2.6 Data

1.2.7 System information

1. user names
2. file names
3. services, etc.

1.3 Methods of separation

1.3.1 Physical

1.3.2 Temporal

1.3.3 Logical

1.3.4 Cryptographic

1.4 Protection/sharing types

1.4.1 None

1.4.2 Isolation (VM)

1.4.3 All-or-nothing (coarse)

1.4.4 Access limitation (RM)

1.4.5 Capabilities

1.4.6 Limit use of object (fine grained)

1.5 Granularity

1.5.1 Coarse - all or nothing

1.5.2 By size of element (bit/byte/word/block)

1.5.3 By logical structure of element (object, sub-object)

1.5.4 By access type

1. create
2. read
3. write
4. execute
5. append
6. copy
7. print
8. rename
9. delete

2 Mechanisms

2.1 H/W

2.1.1 Protection/mode bits & protected instructions

1. set mode
2. I/O
3. set clock
4. etc.

2.2 Memory Protection

2.2.1 Fence

2.2.2 Base/bounds

1. absolute
2. relocatable

2.2.3 VM

1. Paging
2. Segmentation
3. Hybrids

2.2.4 Tagged memory

1. instructions vs. data
2. read-only vs. read-write
3. ownership
4. control data vs. ordinary data

2.3 Devices/files

2.3.1 Locks

2.4 Object-based protection

2.4.1 Goals

1. Inescapable mediation - check every access
2. Least privilege - need-to-know
3. Verify acceptable usage - sematantics

2.5 Access Control Matrix (ACM)

2.5.1 General

1. domains/objects - bindings
2. extensibility - domains as objects
3. limitations - copy-right, restricted copy-right, etc.

2.5.2 Theory

1. HRU result - undecidability
2. TAM

2.5.3 Implementations

1. ACL
   directory structures
2. Capability List
   SFT

2.6 Procedure-oriented Access

- trusted procedures only have access (Gates)

2.7 File Protection

2.7.1 Basic forms

1. All-or-none
2. Group
3. Single protections
   (a) Password
   (b) Encryption
4. Temporary (setuid)
5. Per-object/per-user - ACLs

2.8 User Authentication (I&A)

2.8.1 Loose-lipped systems

2.8.2 Types

1. What you are
2. What you have
3. What you know

2.8.3 Passwords

1. Storage
   (a) protected memory
   (b) encrypted
   (c) hashed
2. Attacks
   (a) page fault example
   (b) finger attack
   (c) probable passwords - joe accounts
   (d) brute force
   (e) hash chains
   (f) rainbow tables

3. Good passwords
   (a) user-generated
   (b) system-generated
   (c) change management
   (d) one-time passwords
   (e) challenge-response systems
   (f) COPS

4. Issues

   (a) Interception

   (b) Strong vs. weak authentication

   (c) Change

   (d) Recall

2.8.4 Biometrics - what you are

1. Fingerprint
2. Retinal scan
3. Iris scan
4. Voice identification
5. Hand dimensions
6. Facial features
7. Signature pressure patterns
8. I/O device usage patterns (keystrokes, mouse)

9. Issues

   (a) user acceptance
   (b) reliability/robustness
   (c) discrimination
   (d) costs
   (e) limitations - roaming users

2.8.5 Artifact-oriented - what you have

1. Examples
   (a) ATM card
   (b) Key
   (c) ID card
   (d) SecureID, etc. PRNG one-time PINs synchronization

2. Issues -

(a)

(b) loss/destruction

(c) interception

(d) misalignment/loss of synch

(e) cost