

Principles of Information Security CS 5323 Lecture Ten

Prof. William Winsborough
October 2, 2007

Business

- Recall: we will have an exam covering material we (read and) discussed in class October 11
 - This one will be worth about 20% of the final grade
- Read chapter 6 of Gollmann for Wed. October 4

2 October 2007

Winsborough CS 5323 Lecture 10

2

Low-level Security Features

- Low-level features may
 - (Pro) Be easier to analyze, yielding higher assurance
 - (Pro) Reduce performance overheads
 - (Con) Not match the level at which some security policy needs to be stated
- Usable security needs to be based on a layered approach

2 October 2007

Winsborough CS 5323 Lecture 10

3

80x86 Policy Based on Rings

- Policy: "Procedures can only access objects in their own ring or in outer rings. Procedures can invoke subroutines only within their own ring."
- Gates are system objects that allow execute-only access to a procedure in an inner ring
- Confused Deputy Problem
 - Outer-ring procedure invokes an inner-ring procedure to copy inner-ring data to the outer ring
 - Doesn't violate the above policy
 - Still, it's a problem and the 80x86 provides mechanisms that can be used to prevent this attack

2 October 2007

Winsborough CS 5323 Lecture 10

4

Protecting Memory

- Basic points
 - Segmentation divides memory into logical units (user code and data, system code and data)
 - Paging divides memory into chunks of uniform size for efficient memory management
 - Segments are defined by base and bound (fence)
 - Addresses contain segment ID and offset
 - User code can only read and modify user data

2 October 2007

Winsborough CS 5323 Lecture 10

5

OS Security is Multifaceted

- Identification and authentication
 - Privileges of user are associated with any subjects (processes) they initiate
- Access control
 - Prevention of unauthorized actions
- Audit log of security related events
 - Detection of security breach
- Installation and configuration

2 October 2007

Winsborough CS 5323 Lecture 10

6

Unix: Principals

- User identities (UIDs)
 - Superuser (root) UID is always 0
- Info about Principals
 - User accounts
 - /etc/passwd
username:password:UID:GID:ld string:home directory:login shell
 - Home directories
 - .profile
- Superuser
 - Basically, no security checks are performed for superuser actions
- Groups
 - /etc/group
group name:group password:GID:list of users

2 October 2007

Winsborough CS 5323 Lecture 10

7

Unix: Subjects

- Processes
 - Initiated by *exec* or *fork* system calls
 - Process ID (PID)
 - Real UID/GID
 - Inherited from parent process
 - Effective UID/GID
 - Inherited from parent process or from file being executed

2 October 2007

Winsborough CS 5323 Lecture 10

8

Unix: Objects

- Objects (resources) include files, directories, memory devices, and I/O devices
- An inode represents a file or a directory
 - Directory entries point to inodes
 - inodes contain type of file, access rights, owner uid, owner group gid, access time, modification time, inode alteration time, size of file, physical location
 - It does not include the name

2 October 2007

Winsborough CS 5323 Lecture 10

9