CMPSCI 377 Operating Systems **Fall 2005**

Lecture 22: December 13

Lecturer: Emery Berger *Scribe: Ordonez, Chinnapongse*

Today:

- UNIX Security
- MULTICS Security
- Access Matrices
- Language-Rich Protection
- Security
- Threat Monitoring

22.1 Security

22.1.1 General Information

- Resources are secure if either the cost of attacking the system is greater than the value of protected resources or the time to attack the system is longer than the time during which the resource has value.

22.1.2 Protection Domains

- Access-right: object name, rights-set
- Rights-set: subset of operations that can be performed on the object

22.1.3 UNIX

- Domain implemented as user-id
- Files are an example of an object
- Sometimes the OS does domain switching to execute a task
- Each file associated with a domain bit (setuid bit)
- When the file is executed and setuid = on, user-id is set to owner of file being executed
- when execution completes, the user-id is reset
- ps and lpr are setuid programs

22.1.4 MULTICS

- Has a nested domain structure based in rings
- Let Di and Dj be any two domain rings. If j is less than I Di is contained within Dj
- Lower levels indicate more privileges
- Each process maintains a current ring number

22.1.5 Access Matrices

- Column = access-control list for one object (who can perform what operations)
- Row = capability list (what can be performed on the object)
- Separates design from policy

22.1.6 Dynamic Access Matrices

- Contain operations to add and delete access rights

22.1.7 Implementation of Access Matrices

- Global tables could be used, but they are too big and grouping cannot take place
- Capability lists are lists of objects with their operations
  - object name = capability
  - can check in capability list for access rights

22.1.8 Revocation of Rights

- Access-list scheme: search for right to be revoked and delete it
- This is immediate and can be selective (removes rights for specific users) or partial (removes only certain rights)

22.1.9 Language-Rich Protection

- In Java, code that is not secure will not be run

22.1.10 Security

- Authentication is done using passwords
- Program Threats: 'Malware'
  - Trojan Horse: allows programs written by users to be executed by other users

  - Trap Door: a user identifier that circumvents normal security procedures. This can be included in the compiler-for an example, read 'Reflections on Trusting Trust' by Ken Thompson (http://www.cs.umass.edu/ emery/cmpsci377/papers/thompson.pdf)
  - Worm: standalone program that uses a spawn mechanism
  - Virus: fragment of code embedded in a legitimate program

22.1.11 Threat Monitoring

- Check for suspicious patterns of activity
- Audit Log
- Scan system for holes periodically