Access Control Mechanisms

Abbreviations of Access Control Lists

- What systems do this?

Abbreviations of Access Control Lists

- What systems do this?
  - Unix
  - What do they look like?

Abbreviations of Access Control Lists

- What systems do this?
  - Unix
  - Owner, Group, Other

Abbreviations of Access Control Lists

- What systems do this?
  - Unix
  - Owner, Group, Other
  - Possible problems?

Abbreviations of Access Control Lists

- What systems do this?
  - Unix
  - Owner, Group, Other
  - Possible problems?
    - What if I wanted to exclude someone? How would I do this?

Abbreviations of Access Control Lists

- What systems do this?
  - Unix
  - Owner, Group, Other
  - Possible problems?
    - What if I wanted to exclude someone? How would I do this?
    - Make a group that includes everyone but that person and give the group access to the file

Full ACL's

- Base permissions
  - owner ---
  - group ---
  - other ---
- Extended permission enabled
  - specify --- u:tony
  - permit --- g=sys
  - deny --- u:jed, g=faculty

Full ACL's

- Problems?
  - Conflicts, who wins?
    - Most restrictive, least restrictive, first entry?
  - What about root/admin
    - In Solaris, root/admin ignore abbreviated, however full ACL even applies to root

ACL

- Where is the ACL stored?
  - With the file?
  - With the user?

Capabilities

- Store the rules with the user
  - Is this good or bad?
  - Why, (not)?
  - How would you circumvent this?

Capabilities VS ACL

- What does your favorite OS do?
  - Mac?
  - Linux?
  - Windows?

Vulnerability Analysis

- What is penetration testing?
  - What are the different types?
  - How are they useful?
  - What do they tell us and not tell us?

Vulnerability Analysis

- What is penetration testing?
  - What are the different types?
    - External attacker with no knowledge of the system
    - External Attacker with access to the system
    - Internal attacker with access to the system
  - How are they useful?
  - What do they tell us and not tell us?

Vulnerability Analysis

- What is penetration testing?
  - What are the different types?
    - External attacker with no knowledge of the system
    - External Attacker with access to the system
    - Internal attacker with access to the system
  - How are they useful?
  - What do they tell us and not tell us?
    - If penetration testing shows no flaws what are the implications?
    - Where does good design come in?

Flaw Hypothesis Methodology

- Information gathering
- Flaw hypothesis
- Flaw testing
- Flat generalization
- Flaw elimination

7 Flaw classes (from RISOS)

- Incomplete parameter validation
- Inconsistent parameter validation
- Implicit sharing of privileged/confidential data
- Asynchronous validation/inadequate serialization
- Inadequate identification/authentication/authorization
- Violable prohibition/limit
- Exploitable logic error

7 Flaw classes (from RISOS)

- Parameter is not checked before use
- Improper format from one function to another
- OS fails to isolate processes and the users properly
- Time-of-check to time of use
- System allows user to be erroneously ID, one user can assume anther's privilege
- System designers fail to handle bounds conditions properly
- All other problems