Lecture 2 Outline

Reading: *text*, §2

1. Access control matrix and entities
   a. Subject, objects (includes subjects)
   b. State is (S, O, A) where A is access control matrix
   c. Rights (represent abstract notions)
2. Instantiating access control matrices
   a. Example 1: UNIX file system
      i. *read*, *write*, *execute* on files
      ii. *read*, *write*, *execute* on directories
   b. Example 2: Boolean expression evaluation
      i. Verbs and rules
      ii. Access Restriction Facility
   c. Example 3: History and limiting rights
3. Primitive operations
   a. **`enter`** r **`into`** $A[s,o]$
   b. **`delete`** r **`from`** $A[s,o]$
   c. **`create subject`** s (note that $\forall x[A[s',x] = A[x,s'] = \varnothing]$)
   d. **`create object`** o (note that $\forall x[A[x,o'] = \varnothing]$)
   e. **`destroy subject`** s
   f. **`destroy object`** o
4. Commands and examples
   a. Regular command: *create•file*
   b. Mono-operational command: *make•owner*
   c. Conditional command: *grant•rights*
   d. Biconditional command: *grant•read•if•r•and•c*
   e. Doing "or" of 2 conditions: *grant•read•if•r•or•c*
   f. General form
5. Miscellaneous points
   a. Copy flag and right
   b. Own as a distinguished right
   c. Principle of attenuation of privilege