Outline for October 2, 2014

Reading: *text*, §1, 2

1. Basic components
   a. Confidentiality
   b. Integrity
   c. Availability
2. Threats
   a. Snooping
   b. Modification
   c. Masquerading; contrast with delegation
   d. Repudiation of origin
   e. Denial of receipt
   f. Delay
   g. Denial of service
3. Role of policy
   a. Example of student copying files from another
   b. Emphasize: policy defines security
   c. Distinguish between policy and mechanism
4. Goals of security
   a. Prevention
   b. Detection
   c. Recovery
5. Trust
   a. First problem: security mechanisms correctly implement security policy
   b. Second problem: policy does what you want; define secure, precise
6. Operational issues; change over time
   a. Cost-benefit analysis
   b. Risk analysis (comes into play in cost-benefit too)
   c. Laws and customs
7. Human Factors
   a. Organizational problems
   b. People problems (include social engineering)
8. Access control matrix and entities
   a. State is (S, O, A) where S subjects, O objects, A access control matrix
   b. Entries are rights (represent abstract notions)
9. 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
10. 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: $grant \cdot read \cdot if \cdot r \cdot or \cdot c$
11. Miscellaneous points
    a. Copy flag and right
    b. Own as a distinguished right
    c. Principle of attenuation of privilege