

## Outline for May 20, 2003

1. Representation of identity
  - a. X.509 Distinguished Names
2. Access control lists
  - a. What they are
  - b. Abbreviations
  - c. Issues in creation and maintenance
  - d. Revocation
3. Capabilities
  - a. What they are
  - b. Copying and amplifying
  - c. Revocation
  - d. Limits
4. Locks and keys
5. MULTICS ring mechanism
  - a. MULTICS rings: used for both data and procedures; rights are REWA
  - b.  $(b_1, b_2)$  access bracket - can access freely;  $(b_3, b_4)$  call bracket - can call segment through gate; so if  $a$ 's access bracket is  $(32,35)$  and its call bracket is  $(36,39)$ , then assuming permission mode (REWA) allows access, a procedure in:
    - rings 0-31: can access  $a$ , but ring-crossing fault occurs
    - rings 32-35: can access  $a$ , no ring-crossing fault
    - rings 36-39: can access  $a$ , provided a valid gate is used as an entry point
    - rings 40-63: cannot access  $a$
  - c. If the procedure is accessing a data segment  $d$ , no call bracket allowed; given the above, assuming permission mode (REWA) allows access, a procedure in:
    - rings 0-32: can access  $d$
    - rings 33-35: can access  $d$ , but cannot write to it (W or A)
    - rings 36-63: cannot access  $d$
6. Propagated access control lists