Notes for November 30, 2000

1. Greetings and Felicitations!
   a. Discuss project
2. Puzzle of the day
3. Capabilities
   a. Capability-based addressing: show picture of accessing object
   b. Show process limiting access by not inheriting all parent's capabilities
   c. Revocation: use of a global descriptor table
4. 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*
5. Lock and Key
   a. Associate with each object a lock; associate with each process that has access to object a key (it's a cross between ACLs and C-Lists)
   b. Example: use crypto (Gifford). *X* object enciphered with key *K*. Associate an opener *R* with *X*. Then:
      OR-Access: *K* can be recovered with any D_i in a list of *n* deciphering transformations, so
      $R = (E_1(K), E_2(K), ..., E_n(K))$ and any process with access to any of the D_i's can access the file
      AND-Access: need all *n* deciphering functions to get *K*: $R = E_1(E_2(...E_n(K)...))$
6. Mandatory vs. Discretionary;
   a. security levels
   b. categories
7. Bell-LaPadula Model
   a. Simple Security Property: no reads up
   b. Star Property: no writes down
   c. Discretionary Security Property: if mandatory controls say it's okay, check discretionary controls.
   d. Basic Security Theorem: A system is secure if its initial state is secure and no action violates the above rules.
8. Lattice Model
   a. Set of classes *SC* is a partially ordered set under relation ≤ with GLB (⊗), LUB (⊕)
   b. Note: ≤ is reflexive, transitive, antisymmetric
   c. Application to MLS: forms a lattice with elements being the Cartesian product of the linear lattice of levels and the subset lattics of categories
   d. Examples: (A, C) ≤ (A', C') iff A ≤ A' and C ⊆ C';
      (A, C) ⊕ (A', C'') = (max(A, A'), C ∪ C')
      (A, C) ⊗ (A', C') = (min(A, A'), C ∩ C')

Puzzle of the Day

Computer security experts seem to like puns. So if you want to talk as a computer security expert, you must be able to inject bad puns into your conversation. To get you started, here are some puns from what the *Book of Lists 2* calls the world's worst puns. Consider yourselves armed (or forewarned)!

1. The Eskimo stabbed himself with an icicle. He died of cold cuts.
2. In his dessert list, a San Antonio restaurateur suggests, "Remember the alamode!"
3. There was an advice-to-the-lovelorn editor who insisted, "If at first you don't succeed, try a little ardor."
4. The commuter's Volkswagen broke down once too often. So he consigned it to the Old Volks Home.
5. The wise old crow perched himself on a telephone wire. He wanted to make a long-distance caw.
6. A talkative musician couldn't hold a job. Every time he opened his mouth, he put his flute in it.
7. A farmer with relatives in East Germany heard that a food package he had sent had never arrived. Optimistically, he assured them, "Cheer up! The wurst is yet to come."
8. When the promoter of a big flower show was told that a postponement was necessary because the exhibits could not be installed on time, he explained to his backers, "We were simply caught with our plants down."
9. A critic declared that he always praised the first show of a new theatrical season. "Who am I," he asked, "to stone the first cast?"
10. Egotist: a person who's always me-deep in conversation.
11. "It's raining cats and dogs," one man remarked. "I know," said another. "I just stepped into a poodle."
12. An eccentric bachelor passed away and left a nephew nothing but 392 clocks. The nephew is now busy winding up the estate.
13. The baseball pitcher with a sore arm was in the throws of agony.