Outline for February 22, 2001

1. Greetings and felicitations!
   a. Friday Feb 23 1:10-2:30 (if not in this room, look in 1062 Banier); go to 1101 Hart Hall to view
   b. No class Tuesday (another trip, *sigh* …)
2. Design Principles
3. Example Mechanism: 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*
4. Confidentiality: Bell-LaPadula 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')
5. Integrity Policy: Biba
6. Integrity Policy: Clark-Wilson
   a. Theme: military model does not provide enough controls for commercial fraud, *etc*. because it does not cover the right aspects of integrity
   b. Data items: "Constrained Data Items" (CDI) to which the model applies, "Unconstrained Data Items (UDIs) to which no integrity checks are applied, "Integrity Verification Procedures" (IVP) that verify conformance to the integrity spec when IVP is run, "Transaction Procedures" (TP) takes system from one well-formed state to another
   c. Certification and enforcement rules:
      C1. All IVPs must ensure that all CDIs are in a valid state when the IVP is run
      C2. All TPs must be certified to be valid, and each TP is assocated with a set of CDIs it is authorized to manipulate
      E1. The system must maintain these lists and must ensure only those TPs manipulate those CDIs
      E2: The system must maintain a list of User IDs, TP, and CDIs that that TP can manipulate on behalf of that user, and must ensure only those executions are performed.
      C3. The list of relations in E2 must be certified to meet the separation of duty requirement.
      E3. The sysem must authenticate the identity of each user attempting to execute a TP.
      C4. All TPs must be certified to write to an append-only CDI (the log) all information necessary to resonstruct the operation.
      C5. Any TP taking a UDI as an input must be certified to perform only valid transformations, else no transformations, for any possible value of the UDI. The transformation should take the input from a UDI to a CDI, or the UDI is rejected (typically, for edits as the keyboard is a UDI).

E4. Only the agent permitted to certify entities may change the list of such entities associated with a TP. An agent that can certify an entity may not have any execute rights with respect to that entity.

7. Cryptography
   a. basics (cryptosystems, attacks, codes vs. ciphers, superencryption)
   b. substitution ciphers (Cæsar cipher, Vigenère cipher)
   c. transposition ciphers (rail-fence cipher)
   d. product cipher (DES)
   e. public key crypto (RSA, DH)
   f. cryptographic checksums
   g. key management (Kerberos, PKI)
   h. digital signatures
   i. authentication
   j. Examples: PEM, PGP, IPSec

Saltzer's and Schroeder's Design Principles

Principle of Economy of Mechanism. The protection mechanism should have a simple and small design.

Principle of Fail-safe Defaults. The protection mechanism should deny access by default, and grant access only when explicit permission exists.

Principle of Complete Mediation. The protection mechanism should check every access to every object.

Principle of Open Design. The protection mechanism should not depend on attackers being ignorant of its design to succeed. It may however be based on the attacker's ignorance of specific information such as passwords or cipher keys.

Principle of Separation of Privilege. The protection mechanism should grant access based on more than one piece of information.

Principle of Least Privilege. The protection mechanism should force every process to operate with the minimum privileges needed to perform its task.

Principle of Least Common Mechanism. The protection mechanism should be shared as little as possible among users.

Principle of Psychological Acceptability. The protection mechanism should be easy to use (at least as easy as not using it).