Outline for April 20, 2000

1. Greetings and felicitations!
   a. Office hours this week after today: W4-5, Th2-3

2. Chinese Wall Policy
   a. Arises as legal defense to insider trading on London stock exchange
   b. Low-level entities are objects; all objects concerning the same corporation form a CD (company dataset);
      CDs whose corporations are in competition are grouped into COIs (Conflict of Interest classes)
   c. Intuitive goal: keep one subject from reading different CDs in the same COI, or reading one CD and writing
to another in same COI
   d. Simple Security Property: Read access granted if the object (a) is in the same CD as an object already
      accessed by the subject, or (b) is in a CD in an entirely different COI. Assumes correct initialization
   e. Theorems: (1) Once a subject has accessed an object, only other objects in that CD are available within that
      COI; (2) subject has access to at most 1 dataset in each COI class
   f. Exceptions: sanitized information
   g. * Property: Write access is permitted only if (a) read access is permitted by the simple security property;
      and (b) no object in a different CD in that COI can be read, unless it contains sanitized information
   h. Comparison to BLP: (1) ability to track history; (2) in CW, subjects choose which objects they can access
      but not in BLP; (3) CW requires both mandatory and discretionary parts, BLP is mandatory only.

3. ORCON
   a. Originator controls distribution
   b. DAC, MAC inadequate
   c. Solution is combination

4. Role-based Access Control (RBAC)
   a. Definition of role
   b. Partitioning as job function
   c. Discuss Data General model

5. Secure vs. Precise
   a. Confidentiality only
   b. Assume: output of a function encodes all available information about inputs (such as resource usage, etc.)
   c. Protection mechanism: given function $p$, it’s a function $m$ such that either $m = p$ for a given set of inputs, or
      $m$ produces an error message
   d. Confidentiality policy: function which checks that the particular inputs are in the authorized set of inputs
   e. Security: $m$ is secure iff there is an $m'$ such that, for all inputs, $m = m'(c(...)$, i.e., $m$'s values consistent with
      stated confidentiality policy
   f. Precision: $m_1$, $m_2$ distinct protection mechanisms. $m_1$ as precise as $m_2$ if, for all inputs, $m_1 = p$ implies $m_2 = p$.
      $m_1$ is more precise if there is an input such that $m_1 = p$ and $m_2 \neq p$ on that input.
   g. Union: $m_1 \cup m_2 = m_3$, where $m_3 = p$ iff $m_1 = p$ and $m_2 = p$; otherwise, $m_3 = m_1$.
   h. ICBS: Let $m_1$, $m_2$ be secure protection mechanisms for a program $p$ and policy $c$. Then $m_1 \cup m_2$ is also a
      secure protection mechanism for $p$ and $c$. Further, $m_1 \cup m_2$ is more precise than either $m_1$ or $m_2$.
   i. Generalizing: for any program $p$ and security policy $c$, there exists a precise, secure mechanism $m^*$ such
      that, for all secure mechanisms $m$ associated with $p$ and $c$, $m^*$ is more precise than $m$.
   j. BUT: there is no effective procedure that determines a maximally precise, secure mechanism for a policy
      and program.