

Outline for May 12, 2005

1. 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. Key result: information can only flow within a CD or from sanitized information
 - i. 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.
 - j. Comparison to Clark-Wilson: specialization of Clark-Wilson
2. CISS
 - a. Intended for medical records; goals are confidentiality, authentication of annotators and integrity
 - b. Patients, personal health information, clinician
 - c. Assumptions and origin of principles
 - d. Access principles
 - e. Creation principle
 - f. Deletion principle
 - g. Confinement principle
 - h. Aggregation principle
 - i. Enforcement principle
 - j. Comparison to Bell-LaPadula: lattice structure but different focus
 - k. Comparison to Clark-Wilson: specialization
3. ORCON
 - a. Originator controls distribution