February 2, 2023 Outline

Reading: *text*, §6.4, 7

Assignments: Homework #2, due February 7
Project Progress Report, due February 14

Note: There will be no class on February 9, 2023 (that's next Thursday)

1. Countermeasures
   (a) Manipulate opening of connection
   (b) Control which packets get through, or the rate at which they get through
2. Amplification attacks
3. Brewer-Nash (Chinese Wall) Policy
   (a) 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)
   (b) Intuitive goal: keep one subject from reading different CDs in the same COI, or reading one CD and writing to another in same COI
   (c) Simple Security Property: Read access granted if the object:
      i. is in the same CD as an object already accessed by the subject; or
      ii. is in a CD in an entirely different COI.œ
   (d) Theorems:
      i. Once a subject has accessed an object, only other objects in that CD are available within that COI;
      ii. Subject has access to at most 1 dataset in each COI class
   (e) Exceptions: sanitized information
   (f) *-Property: Write access is permitted only if:
      i. Read access is permitted by the simple security property; and
      ii. No object in a different CD in that COI can be read, unless it contains sanitized information
   (g) Key result: information can only flow within a CD or from sanitized information
   (h) Aggressive Chinese Wall model
   (i) Comparison to BLP
   (j) Comparison to Clark-Wilson
4. Clinical Information System Security model
   (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
5. Role-based Access Control (RBAC)
   (a) Definition of role
   (b) Partitioning as job function
   (c) Axioms
   (d) Containment and other uses
   (e) $RBAC_0$, $RBAC_1$, $RBAC_2$, $RBAC_3$