CH14 – Protection / Security
Basics

• Potential Violations – Unauthorized release, modification, DoS
• External vs Internal Security
• Policy vs Mechanism
  – Security vs Protection
• Protection domain (of a subject) – resources it can access, permissible operations.
• Design Principles – economy, complete mediation, open design, separation of privileges, least priviledge, least common mechanisms, acceptable, failsafe
Access Matrix

• Objects – entities to which access needs to be controlled (columns)
• Subjects – entities which access the objects (rows)
• Generic rights subjects have on objects
• Protection State is a triplet (S,O, Protection Matrix)
• Implementation Issues – sparsity of matrix
Access Control Lists

- Columnwise enumeration of (subject, rights)
- Requires search for subject, thus slowing access
  - Use of “shadow” registers
- Revocation is easy, as is review of access
- Storage can be further reduced by considering protection groups
- Modifying the ACL – self vs hierarchical
Capabilities

- Row-wise enumeration of (object, rights)
- Object can be specified as an address, with addressing via a table
  - Relocatability, sharing across programs
- Prevent the subject from tampering
  - Tagged, partitioned, encrypted
- Efficient, simple, flexible
- Problems – propagation control, review, revocation, garbage collection
Hybrid methods

• Lock and Key approach
  – Every subject has capability list indicating object and a “key”
  – Every object has ACL containing access modes and the lock guarding them
  – Rights guarded by a lock are granted to a subject whose key “opens” the lock
  – Revocation is easy – delete lock
Safety in Access Matrix

- Protection state can be changed via well understood finite set of commands e.g. create/delete subject/object, add right, delete right etc.

- These commands are *guarded*

- These operations themselves are “rights” to be protected
Safety notions

• A “safe” systems does not permit subject to get rights on object without consent of owner – impossible?
• Weaker condition – can an action lead to leakage of access rights (even this is undecidable)
• A commands leaks a right if it can enter the right into a cell which did not contain it
“Advanced” Protection Models

• Take Grant model – describes protection state as graph.
  – S, O are nodes, edge label x denotes rights.
  – Special rights take and grant
  – Protection problem is still to see if graph can be taken to state where an edge with a desired label is added – undecidable in general, linear for particular restrictions
Bell LaPadua model

• Deals with information flow
  – S, O and security levels, each S has clearance, each O has classification. Each S also has “current clearance”
  – Access rights are RO, RW, Append, Execute. Owner has “control attribute” which allows it to pass above 4 rights (but not the CA).
  – Simple Security: S cannot read O whose classification is higher than S’s clearance
Bell Lapadua model

The Star Property

– S has Append access only to those O whose classification is higher or equal to its clearance
– S has R access only to those O whose classification is lower or equal to its clearance
– S has RW access only to those O whose classification is equal to its clearance
Bell Lapadula – State Transitions

- Stae of the protection system can be changed by well defined operations
  - get access, release access, give access, rescind access, create object, delete object, change security level
- Changes are protected by rules/conditions
- Can be restrictive, static
Lattice Model

• Consists of subjects, objects and security classes
• The relation → defines permissible information flow amongst classes
  – information can flow between objects if it is permissible amongst the classes they belong too.
  – The relation is reflexive (flow can happen amongst objects in the same class), antisymmetric (if c1 → c2, then c2 \(\not\rightarrow\) c1), transitive (c1 → c2 and c2 → c3 \(\Rightarrow\) c1 → c3)
More lattice model

• An information flow policy (SC, \(\rightarrow\)) forms a lattice if it is partially ordered and least upper bound and greatest lower bound exist on set of security classes
  – Bell Lapadula can be thought of as a linear lattice
  – Example of Dennig’s nonlinear Lattice with 3 properties
Military Model

• Four categories – unclassified, confidential, secret, top secret. These are rank ordered.
• Many “compartments”
• Class or clearance is the tuple (rank, compartment)
• A subject dominates an object if its rank is GEQ and it has permissions on all compartments of the object.
• Example with 2 ranks and compartments