Notes for November 24, 1999

1. Greetings and Felicitations!
2. Puzzle of the Day
3. 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.
4. ORCON (Originator Controlled; Graubert)
    a. Document/information can be passed on with approval of originator; real world justification is that originator of document trusts recipients not to release documents which they should not.

    b. Untrusted subject *x* marks object *O* ORCON on behalf of organization *X* and indicates it is releasable to subjects acting on behalf of organization *Y.*
    not releasable to subjects acting on behalf of other organizations without *X*’s permission
    any copies made have the same restriction

    c. DAC: can’t do this as the restriction would not copy over (*y* reads *O* into *C*, puts its own ACL on *C*)

    d. MAC: separate category with*O*, *x*, *y*. *y* wants to read *O*, copy to *C*; MAC means *C* has same category as *O*, *x*, *y*, so can’t give *z* access to *C*.
    Say a new organization *w* wants to provide data in *B* to *y* but not to be shared with *x* or *z*. Can’t use *O*’s category. Hence you get explosion of categories.
    Real world parallel: individuals are “briefed” into a category and those represent a formal “need to know” policy that is standard across the entity; ORCON has no central clearinghouse to categorize data; originator makes rules.

    e. Solution?
    owner of object can’t change ACL’s relationship with object (MAC characteristic)
    on copy, ACL is copied as well (MAC characteristic)
    access control restrictions can be tailored on a subject/object basis (DAC characteristic)
5. Malicious logic
    a. Quickly review Trojan horses, viruses, bacteria; include animal and Thompson’s compiler trick

    b. Logic Bombs, Worms (Schoch and Hupp)