

Lecture 15 Outline (May 1, 2015)

Reading: §5–5.2.1,5.3; 6 (omit 6.3)

Assignment: Homework 2, May 1, 2015
Program 3, due May 8, 2015

1. Greetings and felicitations!
2. Full Bell-LaPadula Model
 - a. Add in compartments
 - b. *dom* relation
 - c. BLP as lattice structure
 - d. Simple security property
 - e. *-Property
 - f. Discretionary security property
3. Range of levels
4. Basic Security Theorem
5. Example: Trusted Solaris
6. Tranquility
 - a. Declassification problem
 - b. Strong tranquility
 - c. Weak tranquility
7. Requirements of integrity models
8. Biba Model (strict integrity policy)
9. Clark-Wilson Model
 - a. Theme: military model does not provide enough controls for commercial fraud, etc. because it does not cover the right aspects of integrity
 - b. Components
 - i. Constrained Data Items (CDI) to which the model applies
 - ii. Unconstrained Data Items (UDIs) to which no integrity checks are applied
 - iii. Integrity Verification Procedures (IVP) that verify conformance to the integrity spec when IVP is run
 - iv. Transaction Procedures (TP) takes system from one well-formed state to another
10. Clark-Wilson 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 associated 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 system 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 reconstruct 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.