Lecture 24: The Clark-Wilson Model

Lecture 24: 1
The Clark-Wilson Model

Commercial Concerns

Lipner’s Integrity Matrix Model showed that BLP and Biba’s Strict Integrity can be adapted to yield a workable commercial policy. But it’s not necessarily a good fit.

David Clark and David Wilson (1987) argued that commercial security has its own unique concerns and merits a model crafted for that domain.

The overriding concern is consistency among the various components of the system state.

Example: In a bank, the funds at the beginning of the day plus the funds deposited minus the funds withdrawn should equal funds on hand at the end of the day.

Lecture 24: 2
The Clark-Wilson Model

Four Basic Concerns

Clark and Wilson claimed that the following are four fundamental concerns of any reasonable commercial integrity model:

- **Authentication**: identity of all users must be properly authenticated.
- **Audit**: modifications should be logged to record every program executed and by whom, in a way that cannot be subverted.
- **Well-formed transactions**: users manipulate data only in constrained ways. Only legitimate accesses are allowed.
- **Separation of duty**: the system associates with each user a valid set of programs they can run and prevents unauthorized modifications, thus preserving integrity and consistency with the real world.

Lecture 24: 3
The Clark-Wilson Model

Key Concepts

The policy is constructed in terms of the following categories:

- **Constrained Data Items**: CDIs are the objects whose integrity is protected
- **Unconstrained Data Items**: UDIs are objects not covered by the integrity policy
- **Transformation Procedures**: TPs are the only procedures allowed to modify CDIs, or take arbitrary user input and create new CDIs. Designed to take the system from one valid state to another.
- **Integrity Verification Procedures**: IVPs are procedures meant to verify maintenance of integrity of CDIs.
Policy Rules

There are two kinds of rules: Certification and Enforcement.

C1: All IVPs must ensure that CDIs are in a valid state when the IVP is run.
C2: All TPs must be certified as integrity-preserving.
C3: Assignment of TPs to users must satisfy separation of duty.
C4: The operation of TPs must be logged.
C5: TPs executing on UDIs must result in valid CDIs.
E1: Only certified TPs can manipulate CDIs.
E2: Users must only access CDIs by means of TPs for which they are authorized.
E3: The identity of each user attempting to execute a TP must be authenticated.

Clark-Wilson Model

Permissions are encoded as a set of triples of the form:

$\langle \text{user, TP, \{CDI set\}} \rangle$

where $\text{user}$ is authorized to perform a transaction procedure $\text{TP}$, on the given set of constrained data items (CDIs).

Each triple in the policy must comply with all applicable certification and enforcement rules.

Lessons

- Clark and Wilson identified a set of integrity concerns claimed to be of particular relevance within commercial environments: consistency, authentication, audit, etc.
- They proposed a set of mechanisms explicitly designed to address those specific concerns.
- Their policy is quite abstract and must be instantiated with specific data sets (constrained and unconstrained), transformation procedures, verification procedures, etc.

Next lecture: Chinese Wall Policy