CS 556 – Computer Security
Fall 2012

Dr. Indrajit Ray
Email: indrajit@cs.colostate.edu

Department of Computer Science
Colorado State University
Fort Collins, CO 80523, USA
CLARK-WILSON MODEL

MODEL OVERVIEW

Model Discussion
Integrity in Clark-Wilson Model

- Data integrity
  - Quality
  - Correctness
  - Authenticity
  - Accuracy
- System integrity
  - Successful and correct operation of system
Integrity in Clark-Wilson Model

- Integrity defined by a set of constraints
- Data is in a consistent state when it satisfies these constraints
  - For some data integrity may not matter
- If all relevant data is in consistent state, system integrity is satisfied
Separation of Duty

- No single person or entity should perform a task from beginning to end but the task should be divided among two or more people or entities.
Well-formed Transactions

- User should not be able to manipulate data arbitrarily but only in constrained, well-defined ways that preserve the integrity of the data.
**Principle of Least Privilege**

- An entity should be able to access only such information or resources that are necessary to its legitimate purpose
MODEL OVERVIEW
CW Model Components

- **CDI**: Constrained Data Items
  - Data that is subject to integrity controls

- **UDI**: Unconstrained Data Items
  - These data items are not subject to integrity controls
**Model Discussion**

- **IVP**: Integrity Verification Procedures
  - These procedures test if the CDIs conform to the integrity constraints

- **TP**: Transaction Procedures
  - These procedures are used to change the CDIs
  - They take the system from one valid state to another
Certification Rules and Enforcement Rules

- Ensure integrity is achieved and is preserved
  - **Certification Rules** – Integrity monitoring rules enforced by the administrator
  - **Enforcement Rules** – Integrity preserving rules guaranteed by the system
Certification Rules

- **C1 - IVP Certification** – The system will have an IVP for validating the integrity of any CDI
- **C2 - Validity** – The application of a TP to any CDI must maintain the integrity of that CDI. CDIs must be certified to ensure that they result in a valid CDI
Certification Rules (cont’d)

- **C3 - Modification** – A CDI can only be changed by a TP. TPs must be certified to ensure they implement the principles of separation of duties & least privilege.
- **C4 - Journal Certification** – TPs must be certified to ensure that their actions are logged.
- **C5** – TPs which act on UDIs must be certified to ensure that they result in a valid CDI.
Enforcement Rules

- **E1 - Enforcement of Validity** – Only certified TPs can operate on CDIs
- **E2 - Enforcement of Separation of Duty** – Users must only access CDIs through TPs for which they are authorized
- **E3 - User Identity** – The system must authenticate the identity of each user attempting to execute a TP
- **E4 - Initiation** – Only administrator can specify TP authorizations
Model Discussion
Handling Untrusted Inputs

- Any TP that takes as input a UDI may perform only valid transformations, or no transformations, for all possible values of the UDI. The transformation either rejects the UDI or transforms it into a CDI.
  - For example, in a bank ATM, numbers entered at the keyboard are UDIs so cannot be input to TPs as such. TPs must validate numbers (to make them a CDI) before using them; if validation fails, TP rejects UDI.
Separation of Duty

- Only the certifier of a TP may change the list of entities associated with that TP. No certifier of a TP, or of an entity associated with that TP, may ever have execute permission with respect to that entity.
  - Enforces separation of duty with respect to certified and allowed relations.
Ensuring Integrity

- Provides an assurance that CDIs can be modified only in constrained ways.
  - Ensured by rules C1, C2, C5, and E1 and E4
- Provides an ability to control access to resources
  - Ensured by rules C3 and E2 and E3.
Ensuring Integrity (cont’d)

- Provides an ability to ascertain after the fact that changes to CDIs are valid and the system is in a valid state
  - Provided by rules C1 and C4
- Provides an ability to uniquely associate an user to her/his action
  - Enforced by rule E3
Summary

- Model of integrity suitable for many commercial scenarios
- Problem with difficulty to implement well-formed transactions