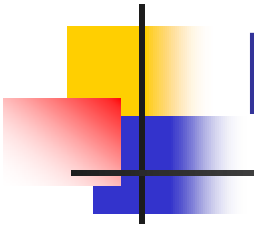
CS590U

Access Control: Theory and Practice

Lecture 10 (February 10)

Integrity: Biba and Clark-Wilson



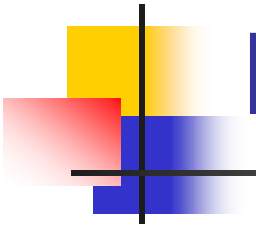
Motivation

- Bell-LaPadula and other information-flow based security definitions address confidentiality, what about integrity
- What does integrity mean?
  - data not changed in “incorrect” ways
- Difference between confidentiality & integrity
  - a subject cannot leak a piece of confidential information without reading it, but can introduce low-integrity information without reading any
  - some trust has to be placed on subjects for integrity

Biba's Integrity Models

- Based on Bishop's book & Amoroso's book
- Four models
  - Mandatory integrity model
  - Subject low-water mark model
  - Object low-water mark model
  - Ring model

Biba's Mandatory Integrity Model

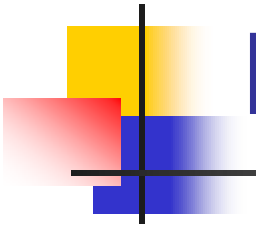


- Each subject(program) has an integrity level
  - reflects confidence on the program executing correctly (what does `correctly' mean?)
- Each object has an integrity level
  - reflects degree of confidence in the data
- Integrity levels are totally ordered
- Integrity levels different from security levels
  - a highly sensitive data may have low integrity (e.g., information collected by spy)

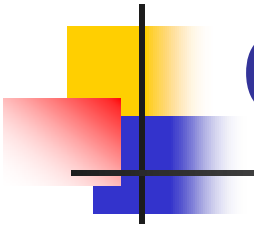
Biba's Strict Integrity Policy

- Three rules:
  1. s and read o iff i(s) = i(o)
  2. s can write to o iff i(o) = i(s)
  3. s_1 can execute s_2 iff $i(s_2) = i(s_1)$
- Questions:
  - What does it mean that a subject is trusted to execute correctly at integrity level i1?
    - generate information at level i1 from any data
    - generate information at level i1 when reading any data above i1
    - generate information at the same level as input

Subject Low-Water Mark Model



- The reading rule is relaxed; rules 2 & 3 still apply
- Rule 1 is changed: when s reads o, the integrity level of s is set to min[i(s), i(o)].
  - if the integrity levels are not totally ordered, then glb[i(s), i(o)]
- Guess: initially a subject's integrity level is set to highest
  - all subjects are trusted, a subject can introduce wrong data without reading wrong data.
- Ensures that there is no information path from low integrity data to high integrity data

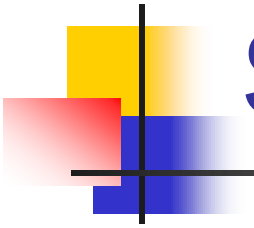


Object Low-Water Mark

- The writing rule is relaxed: when s writes o, the integrity level of o is set to min[i(s),i(o)].
- Also ensures that there is no information path from a low integrity object to a high integrity object
- Subject & object low-water mark may be combined

Biba's Ring Policy

- Rules
  - Any subject can read any object
  - s can write to o iff $i(o) = i(s)$
  - s_1 can execute s_2 iff $i(s_2) = i(s_1)$
- Intuitions:
  - subjects are trusted to process inputs correctly, and to generate outputs of a certain integrity level



Summary of Biba's Models

- Different models assume different kinds of trust in subjects
  - the ring model assumes subjects can correctly process inputs and generate data of a certain integrity level
  - the low-water mark models assume subjects do not introduce low integrity information themselves, but may be contaminated by the source
  - the strict MAC model assumes subjects may be contaminated by the source and can only generate data of a certain integrity level

Key Difference between Confidentiality and Integrity

- For confidentiality, no trust needs to be placed on subjects
  - one does need trusted subjects to make system realistic, but they are not needed for confidentiality
- For integrity, one has to trust subjects
  - therefore; one has to justify such trust

Lipner's Five Requirements for Integrity

1. Users will not write their own programs, but will use existing production programs and databases
2. Programmers will develop and test programs in a nonproduction system. If they need to acces production programs or databases, they may be provided with copies of the information they need through a special process
3. "Promotion" of programs from development to production status is a controlled event

Lipner's Five Requirements for Integrity

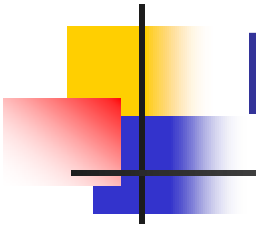
4. The installation system programmers' actions shall be controlled and audited
5. Management and audit function shall have access to the system state and an audit trail of selected activities (both system actions and user interactions with the applications)

A Comparison of Commercial and Military Computer Security Policies

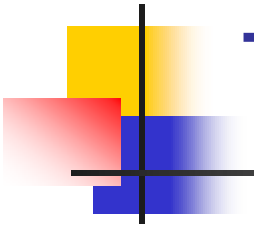
David D. Clark and David R. Wilson.

In Oakland'1987.

Impact of the Clark-Wilson Paper

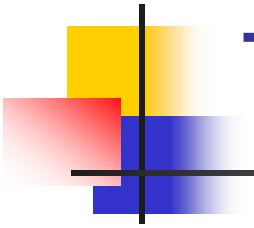


- Shift the focus of the field from military MAC policies to other requirements of access control
- 290 citations on Google Scholar
  - after Sandhu et al.'s RBAC paper, Bell & LaPadula's 1976 paper among all access control papers



The Focus is on Integrity

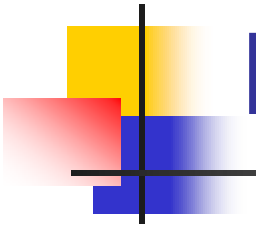
- Military policies focus on preventing disclosure
- In commercial environment, preventing unauthorized data modification is usually paramount
  - no user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted



The Goal of the Paper

- Defend the following two conclusions
  - there is a distinct set of security policies, related to integrity rather than disclosure, which are often of highest priority in the commercial data processing environment
  - Some separate mechanisms are required for enforcement of these policies, disjoint from those in the Orange Book

High-level Mechanisms for Enforcing Data Integrity



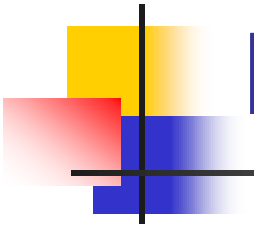
- Well-formed transaction
  - a user should not manipulate data arbitrarily, but only in constrained ways that preserve or ensure data integrity
    - e.g., use a write-only log to record all transactions
    - double-entry bookkeeping

High-level Mechanisms for Enforcing Data Integrity

- Separation of duty among the employees
  - ensure external consistency: data objects correspond to the real world objects
  - separating all operations into several subparts and requiring that each subpart be executed by a different person

Implementing the Two High-level Mechanisms

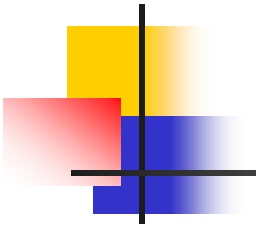
- Mechanisms are needed to ensure
  - a data item can be manipulated only by a specific set of programs
  - programs must be inspected for proper construction, controls must be provided on the ability to install and modify these programs
  - each user must be permitted to use only certain sets of programs
  - assignment of people to programs must be controlled and inspected



Differences from MAC

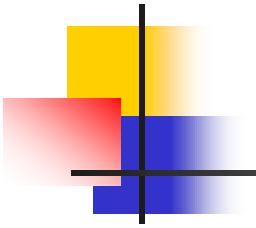
- A data item is not associated with a particular security level, but rather with a set of TPs
- A user is not given read/write access o data items, but rather permissions to execute certain programs

The Clarke-Wilson Model for Integrity (1)



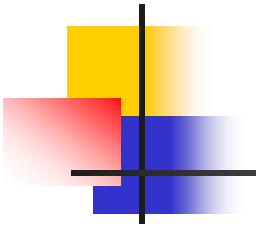
- Unconstrained Data Items (UDIs)
- Constrained Data Items (CDIs)
  - data items within the system to which the integrity model must apply
- Integrity Verification Procedures (IVPs)
  - confirm that all of the CDIs in the system conform to the integrity specification
- Transformation Procedures (TPs)
  - well-formed transactions

The Clarke-Wilson Model for Integrity (2)



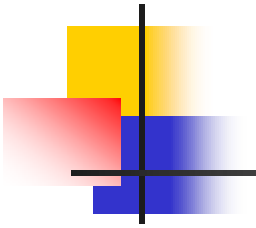
- C1: (Certification) All IVPs must properly ensure that all CDIs are in a valid state at the time the IVP is run
- C2: All TPs must be certified to be valid. That is, they must take a CDI to a valid final state, given that it is in a valid final state to begin with. For each TP, the security officer must specify the set of CDIs that the TP has been certified.

The Clarke-Wilson Model for Integrity (3)



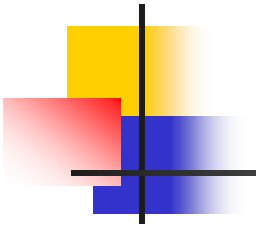
- E1: (Enforcement) The system must ensure that only TPs can access CDIs and any TP can only access the CDIs it is certified for.
- E2: The system must maintain a relation of the form, (UserI, TPi, (CDIa, CDIa, CDIc,...). A user can only execute TPs that it is allowed to access.

The Clarke-Wilson Model for Integrity (4)



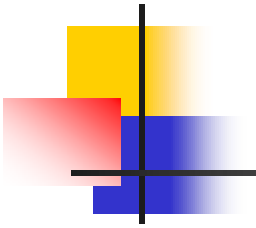
- C3: The relation in E2 must be certified to meet the separation of duty requirement.
- E3: The system must authenticate the identity of each user attempting to execute a TP

The Clarke-Wilson Model for Integrity (5)



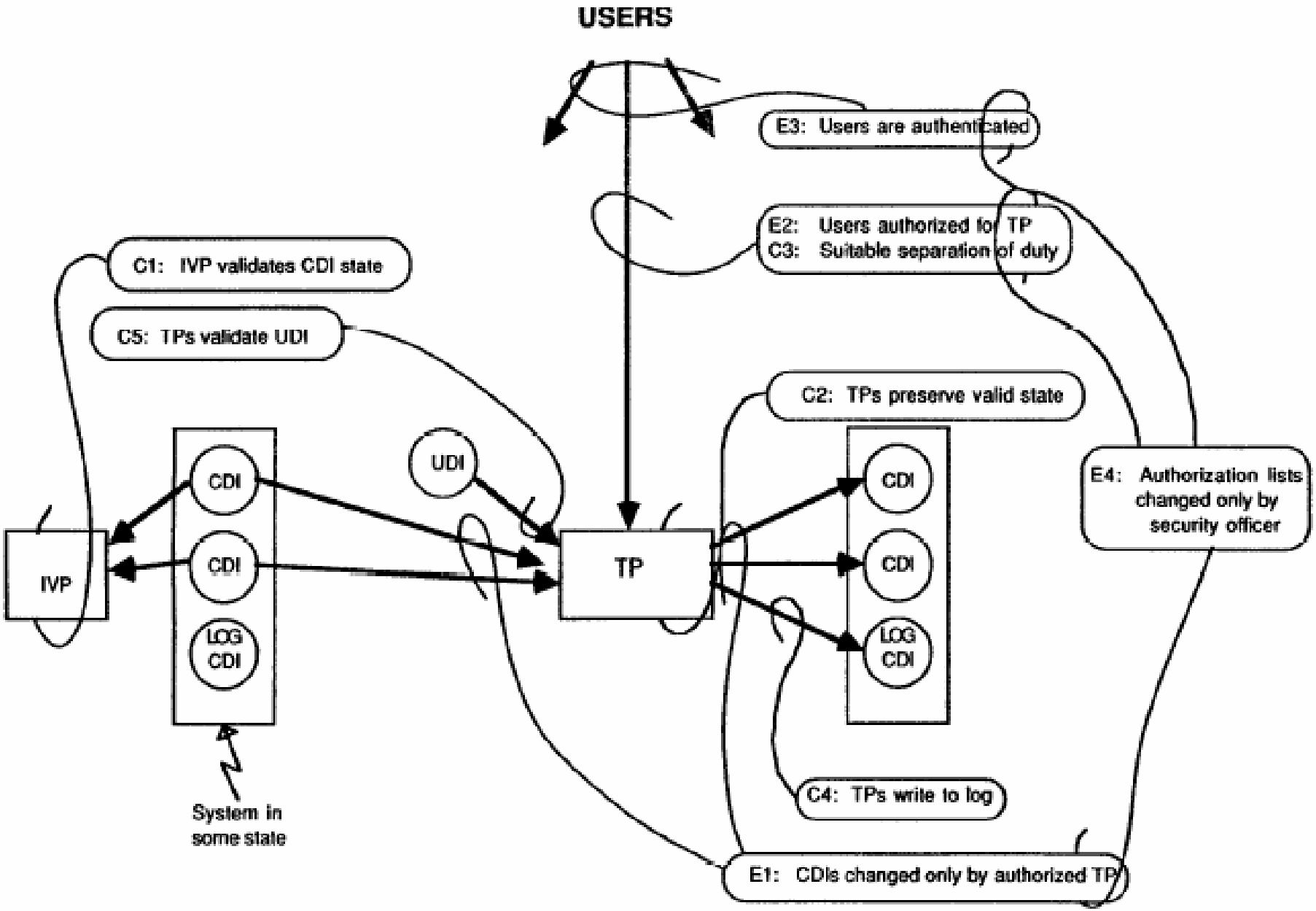
- C4: All TPs must be certified to write to an append-only CDI (the log) all information necessary to permit the nature of the operation to be reconstructed.
- C5: Any TP that takes a UDI as input must be certified to perform only valid transformations, or no transformations, for all possible values of the UDI. The transformation either rejects the UDI or transforms it into a CDI.

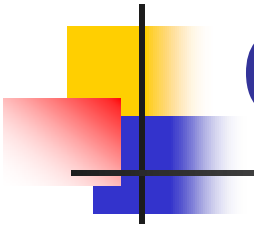
The Clarke-Wilson Model for Integrity (6)



- E4: Only the agent permitted to certify entities may do so. An agent that can certify entity (TP or CDI) may not have any execute rights with respect to that entity.

Figure 1: Summary of System Integrity Rules





Comparison with Biba

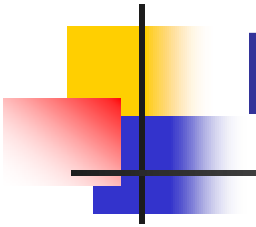
- Biba lacks the procedures and requirements on identifying subjects as trusted

The Chinese Wall Security Policy

David FC. Brewer and Michael J. Nash.

in Oakland'1989.

The Chinese Wall Security Policy

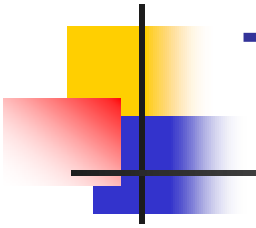


- Data are stored in a hierarchical arranged system
  - the lowest level consists of individual data items
  - the intermediate level group data items into company data sets
  - the highest level group company datasets whose corporation are in competition

Simple Security Rule in Chinese Wall Policy

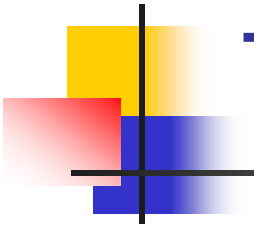
- Access is only granted if the object requested:
  - is in the same company dataset as an object already accessed by that subject, i.e., within the Wall,

    or
  - belongs to an entirely different conflict of interest class.



Theorems:

- T1: Once a subject has accessed an object the only other objects accessible by the same subject lie within the same company dataset or within a different conflict of interest class
- T2: A subject can at most have access to one company dataset in each conflict of interest class

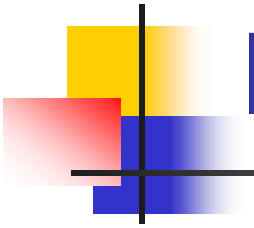


Theorems:

- T3: If for some conflict of interest class X there are X_y company datasets then the minimum number of subjects which will allow every object to be accessed by at least one subject is X_y.

Sanitized Information

- Motivation: enable comparison of information of multiple companies in a conflict of interest set
- Sanitization disguise a corporation's information, in particular to prevent the discovery of that corporation's identity

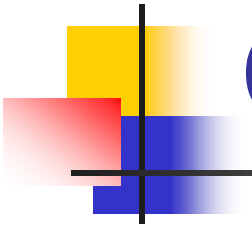


*-Property in Chinese Wall Policy

- Write access is only permitted if
  - access is permitted by the simple security rule, and
  - no object can be read which is in a different company dataset to the one for which write access is requested and contains unsanitized information

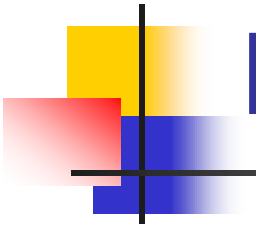
Theorem

- T4: The flow of unsanitized information is confined to its own company dataset; sanitized information may however flow freely throughout the system



Comparison with Bell-LaPadula

- Point in the paper: use compartment for company data-set does not work because
  - no access history is maintained in BLP
  - subject labels cannot change dynamically
- Point countered by Ravi Sandhu
  - Chinese Wall Policy can be implemented



End of Lecture 10

- Next lecture
  - Role-Based Access Control