Computer Security
CS 426
Lecture 25

Integrity Protection: Biba, Clark Wilson, and Chinese Wall

Plan for this lecture

- Biba
- Clark-Wilson
- Chinese Wall

What is integrity?

- Attempt 1: Critical data do not change.
- Attempt 2: Critical data changed only in “correct ways”
  - E.g., in DB, integrity constraints are used for consistency
- Attempt 3: Critical data changed only through certain “trusted programs”
- Attempt 4: Critical data changed only as intended by authorized users.

The Biba Model

- Kenneth J. Biba: "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, April 1977.

- Motivated by the fact that BLP does not deal with integrity

Biba: Integrity Levels

- Each subject (program) has an integrity level
- Each object has an integrity level
- Integrity levels are totally ordered

- Integrity levels different from security levels in confidentiality protection
  - a highly sensitive data may have low integrity
  - What is an example of a piece of data that needs high integrity, but no confidentiality?

Five Mandatory Policies in Biba

- Strict integrity policy
- Subject low-water mark policy
- Object low-water mark policy
- Low-water mark Integrity audit policy
- Ring policy

Strict Integrity Policy (BLP reversed)

- Rules:
  - s can read o iff $i(s) \leq i(o)$
    - no read down
    - stops indirect sabotage by contaminated data
  - s can write to o iff $i(s) \geq i(o)$
    - no write up
    - stops directly malicious modification

- Fixed integrity levels
- No information path from low object/subject to high object/subject

Subject Low-Water Policy

- Rules
  - s can always read o; after reading $i(s) \leftarrow \min[i(s), i(o)]$
  - s can write to o iff $i(s) \geq i(o)$
- Subject's integrity level decreases as reading lower integrity data
- No information path from low-object to high-object

Object Low-Water Mark Policy

- Rules
  - s can read o; iff $i(s) \le i(o)$
  - s can always write to o; after writing
    $i(o) \leftarrow \min[i(s), i(o)]$

- Object's integrity level decreases as it is contaminated by subjects

- Objects with high labels are not contaminated

Low-Water Mark Integrity Audit Policy

- Rules
  - s can always read o; after reading $i(s) \leftarrow \min[i(s), i(o)]$
  - s can always write to o; after writing $i(o) \leftarrow \min[i(s), i(o)]$
- Tracing, but not preventing contamination
- Similar to the notion of tainting

The Ring Policy

- Rules
  - Any subject can read any object
  - s can write to o iff $i(s) \geq i(o)$

- Integrity levels of subjects and objects are fixed.

- Intuitions:
  - subjects are trusted to process low-level inputs correctly

Object Integrity Levels

- The integrity level of an object may be based on
  - Quality of information (levels may change)
    - Degree of trustworthiness
    - Contamination level:
  - Importance of the object (levels do not change)
    - degree of being trusted
    - Protection level: writing to the objects should be protected
- What should the relation between the two meanings, which one should be higher?

Integrity vs. Confidentiality

Confidentiality	Integrity
Control reading • preserved if confidential info is not read	Control writing • preserved if important obj is not changed
For subjects who need to read, control writing after reading is sufficient, no need to trust them	For subjects who need to write, has to trust them, control reading before writing is not sufficient

Integrity requires trust in subjects!

Key Difference between Confidentiality and Integrity

- For confidentiality, controlling reading & writing is sufficient
  - theoretically, no subject needs to be trusted for confidentiality; however, one does need trusted subjects in BLP to make system realistic
- For integrity, controlling reading and writing is insufficient
  - one has to trust all subjects who can write to critical data

Impacts of The Need to Trust Subjects

- A small security kernel is no longer possible
- No need to worry about covert channels for integrity protection
- How to establish trust in subjects becomes a challenge.

The Clark-Wilson Model

- David D. Clark and David R. Wilson. “A Comparison of Commercial and Military Computer Security Policies.” In IEEE SSP 1987.
- Military policies focus on preventing disclosure
- In commercial environment, integrity is 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

Two 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
    - e.g., double-entry bookkeeping
    - e.g., passwd

Can manipulate data only through trusted code!

Two High-level Mechanisms for Enforcing Data Integrity

- Separation of duty
  - 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
  - e.g., the two-man rule

Implementing the Two High-level Mechanisms

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

The Clarke-Wilson Model for Integrity

- Unconstrained Data Items (UDIs)
  - data with low integrity
- 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

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 to data items, but rather permissions to execute certain programs

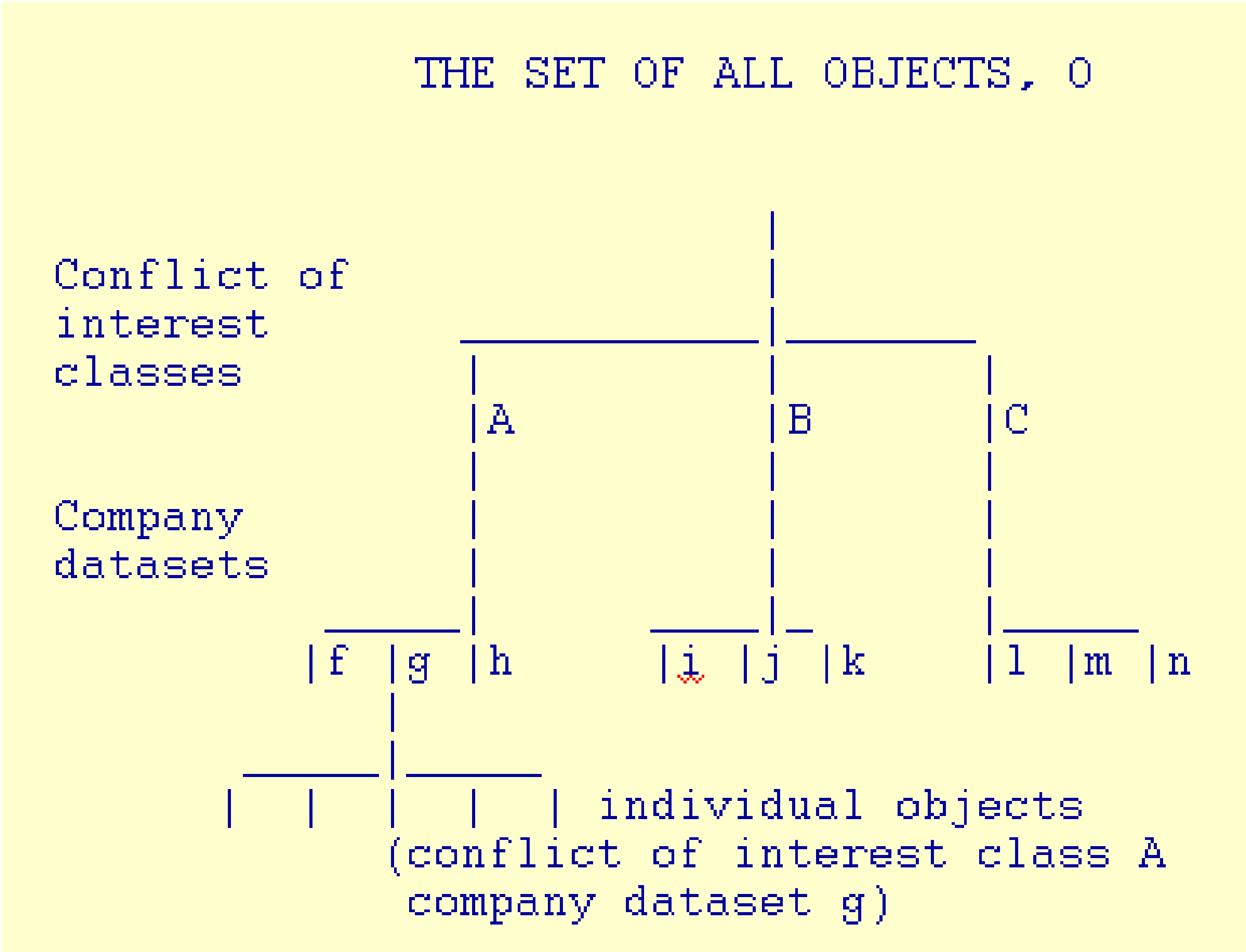
Comparison with Biba

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

- Clark-Wilson focuses on how to ensure that programs can be trusted

The Chinese Wall Security Policy

- Goal: Avoid Conflict of Interest
- 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



From http://www.gammassl.co.uk/topics/chinesewall.html

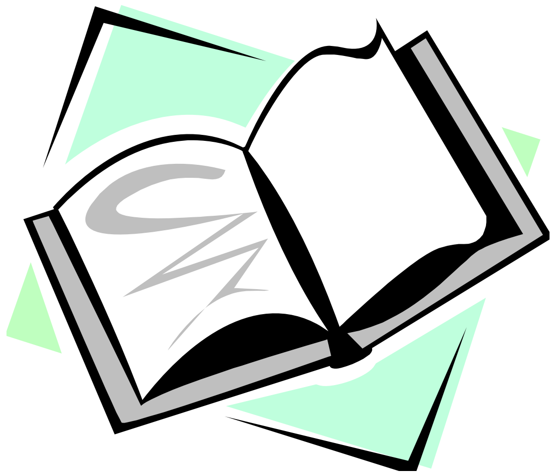
Simple Security Rule in Chinese Wall Policy

- 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.

Readings for This Lecture

- Required Readings:
  - David D. Clark and David R. Wilson. “A Comparison of Commercial and Military Computer Security Policies.” In IEEE SSP 1987.
- Optional Readings:
  - David FC. Brewer and Michael J. Nash. “The Chinese Wall Security Policy.” in IEEE SSP 1989.



Coming Attractions …

- Integrity protection in operating systems