


PURDUE UNIVERSITY

Computer Security CS 426 Lecture 16

Integrity Protection: Biba, Clark-Wilson
Chinese Wall



Elisa Bertino
Purdue University
IN, USA
bertino@cs.purdue.edu

Center for Education and Research
in Information Assurance and Security

1

PURDUE UNIVERSITY

Goal of Biba Model

- Integrity policy: “formal access constraints which is effectively enforced, protect data from improper modification”
 - *Integrity Considerations for Secure Computer Systems, MTR-3153, Biba, K. J. 1975*
- Prevent data modification by unauthorized parties
- Prevent unauthorized data modification by authorized parties

2

PURDUE UNIVERSITY

Modes of Access

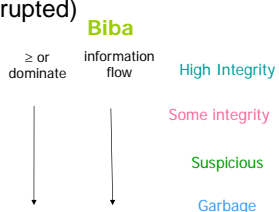
- Observation
- Modification
- Execution

3

PURDUE UNIVERSITY

The Biba Model *strict integrity policy*

- BLP prevents information from flowing down (thus being disclosed)
- *Biba* prevents information from flowing up (thus getting corrupted)



The diagram shows two vertical arrows pointing downwards. The left arrow is labeled "≥ or dominate" and the right arrow is labeled "information flow". To the right of the arrows, four levels of integrity are listed from top to bottom: "High Integrity" (blue), "Some integrity" (red), "Suspicious" (green), and "Garbage" (yellow).

4

Notation

S=Subjects, O=objects, IL= integrity levels

$il_1 \geq il_2$ says that i_1 dominates i_2

$\min(il_1, il_2)$ is the lesser between il_1 and il_2

$il(s)$, $il(o)$ = integrity level of $s \in S$ and $o \in O$.

$\langle s, r, o \rangle$ says that s can read o

$\langle s, w, o \rangle$ says that s can write o

$\langle s, x, s' \rangle$ says that s can execute s'

5

Five Mandatory Policies in Biba

- Strict integrity policy
 - Constraints read, write, and execute operations
- Low-water mark policy
 - It relaxes the strict integrity policy
 - Two types:
 - Subject low-water mark policy
 - Object low-water mark policy
- Low-water mark integrity audit policy
 - It does not control read or write; it simply traces “contamination”
- Ring policy
 - It trusts that subjects handle the data correctly even if data is of low quality

6

Biba Strict Integrity Policy

For any $s \in S$ and $o \in O$

1. $\langle s, r, o \rangle$ iff $il(o) \geq il(s)$ (read-up)
2. $\langle s, w, o \rangle$ iff $il(s) \geq il(o)$ (write-down)
3. $\langle s_1, x, s_2 \rangle$ iff $il(s_1) \geq il(s_2)$ (execute-down)

- Can add compartments to get full dual of BLP
- The execute rule prevent a ‘dirty’ subject s_1 from touch a ‘clean’ object indirectly by invoking s_2 .

7

Subject Low-Water Mark Policy

- **s can always read o;**
 - after reading $il(s) \leftarrow \min[il(s), il(o)]$
- $\langle s, w, o \rangle$ iff $il(s) \geq il(o)$
- $\langle s_1, x, s_2 \rangle$ iff $il(s_1) \geq il(s_2)$
- **!!!The Low-Water Mark Policy model is dynamic !!!:**
Subject’s integrity level decreases as reading lower integrity data
 s can read down, but once it does, its integrity level drops (so it cannot corrupt other objects)

Example: After a machine reads emails infected with worm, the machine is no longer trusted and isolated

No low-to-high information path

8

Object Low-Water Mark Policy

- $\langle s, r, o \rangle$ iff $il(o) \geq il(s)$
- **s can always write to o;**
after writing $il(o) \leftarrow \min[il(s), il(o)]$
- **!!!Also dynamic !!!** Object's integrity level decreases as it is contaminated by subjects
- **Example:** After a virus is detected, whatever files were written by the virus are no longer trusted and therefore are deleted
- Objects with high integrity labels are not contaminated

9

Low-Water Mark Integrity Audit Policy

- Each object and subject gets a corruption integrity level CL
- **S can always read O**
– after reading $CL(s) \leftarrow \min[CL(s), CL(o)]$
- **S can always write to O**
– after writing $CL(o) \leftarrow \min[CL(s), CL(o)]$
- *Tracing, but not preventing contamination*

10

The Ring Policy

- Any subject can read any object
- $\langle s, w, o \rangle$ can write to o iff $il(s) \geq IL(o)$
- $\langle s_1, x, s_2 \rangle$ iff $il(s_1) \geq il(s_2)$
- Integrity levels of subjects and objects are fixed.
- Subjects are trusted to process low-level inputs correctly

11

Confidentiality vs. Integrity

- For confidentiality, controlling reading and 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 subjects

12

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

13

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!

14

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

15

Implementation

- 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

16

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

17

Differences from MAC

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

18

Comparison with Biba

- Biba lacks the procedures and requirements for identifying subjects as trusted
- Clark-Wilson focuses on how to ensure that programs can be trusted

19

Conflict of Interest

- It is a well known concept
- An example in the financial world is that of a market analyst working for a financial institution providing corporate business services
- Such analyst must uphold the confidentiality of information provided to him by his firm's client; this means he/she cannot advise corporations where he/she has *insider knowledge* of the plans, status and standing of a competitor
- However the analyst is free to advice corporations which are not in competition with each other, and also to draw on general market information

20

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

21

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.

22

Chinese Wall Policy

Introduced by Brewer and Nash in 1989

The motivation for this work was to avoid that sensitive information concerning a company be disclosed to competitor companies through the work of financial consultants

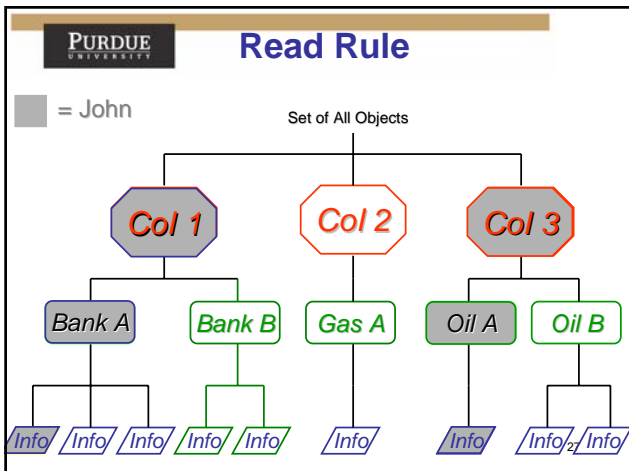
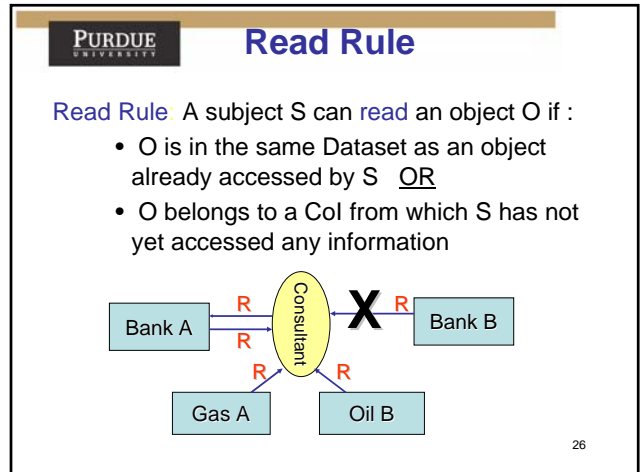
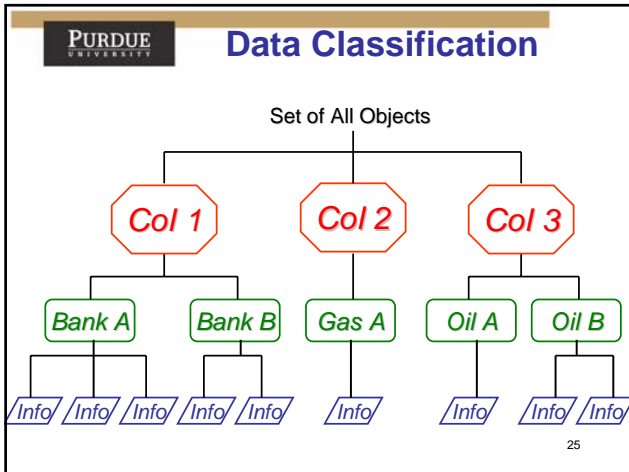
- It dynamically establishes the access rights of a user based on what the user has already accessed

23

Chinese Wall Policy

- *Subjects*: Active entities accessing protected objects
- *Objects*: Data organized according to 3 levels
 - » Information
 - » DataSet
 - » Conflict-of-Interest (Col) classes
- *Access Rules*
 - » Read rule
 - » Write rule

24

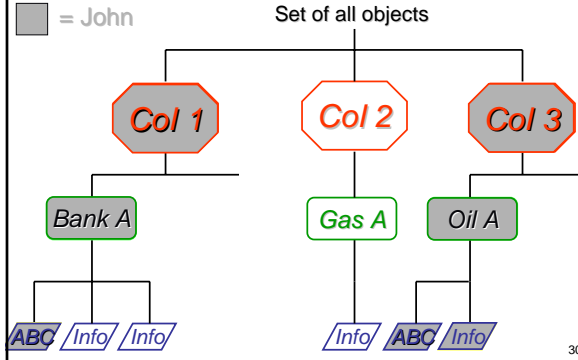


- PURDUE UNIVERSITY** **Comparison with BLP**
- The Chinese Wall Policy is a combination of free choice and mandatory control
 - Initially a subject is free to access any object it wishes
 - Once the initial choice is made, a *Chinese Wall* is created for that user around the dataset to which the object belongs
 - Note also that a Chinese Wall can be combined with DAC policies
- 28

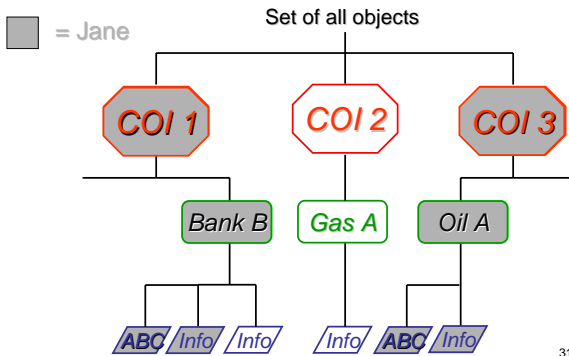
Write Rule

- The Read Rule does not prevent indirect flow of information
- Consider the following case:
 - John has access to
 - Oil A and Bank A
 - Jane has access to
 - Oil B and Bank A
 - If John is allowed to read Oil A and write into Bank A, it may transfer information about Oil A that can then be read by Jane

Write Rule



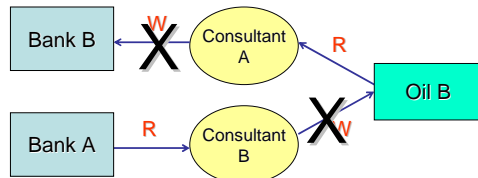
Write Rule



Write Rule

Write Rule: A subject S can write an object O if:

- S can read O according to the Read Rule AND
- No object has been read by S which is in a different company dataset to the one on which write is performed



Write Rule

Thus, according to the write rule:

The flow of information is confined to its own company dataset

33

Sanitized Information

- Brewer and Nash recognize the need for analysts to be able to compare information they have with that relating to other corporations
- Thus they recognize that access restriction can be lifted for **sanitized information**
- Sanitization takes the form of disguising a corporation's information, so to prevent the discovery of that corporation identity

34

Criticisms to the Model (R. Sandhu)

The Write Rule of BN is very restrictive:

- A user that has read objects from more than one dataset is not able to write any object
- The user can only read and write objects from a single dataset

35