

# Computer Security

## CS 426

### Lecture 15



## Integrity Protection: Biba, Clark-Wilson, and Chinese Wall

# Announcements

- Mid-term exam on October 18
  - cover all materials up to this lecture, except for the lecture on Crypto by Prof. Nita-Rotaru
- Lecture on Tuesday October 16 will review homework 2 and cover new materials
- Future quizzes will be announced at least one day before the class
- TA's office hour
  - Wednesday and Friday 2:30pm to 3:30pm
  - LWSN 2161

# Review

- Terminologies: Trusted, Trustworthy, TCB, Trusted Path, Trusted Computing
- Eight design principles due to Saltzer & Schroeder
- Security features for “trusted OS”
- Reference monitor in “trusted OS”
  - three features
- Orange Book (TCSEC): 7 levels
- Common Criteria: Protection Profiles, EAL 1-7

# Plan for this lecture

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

# What is integrity?

- Integrity: Critical data not changed in “incorrect” ways
- Confidentiality vs. Integrity

Confidentiality	Integrity
Control reading	Control writing
For subjects who need to read, control they writing is sufficient	For subjects who need to write, control what they read is <b>not</b> sufficient

Integrity requires trust in subjects!

# 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

# 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
- No low-to-high information path

# 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 low-to-high information path

# Object Low-Water Mark Policy

- Rules
  - s can read o; iff  $i(s) \leq i(o)$
  - 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

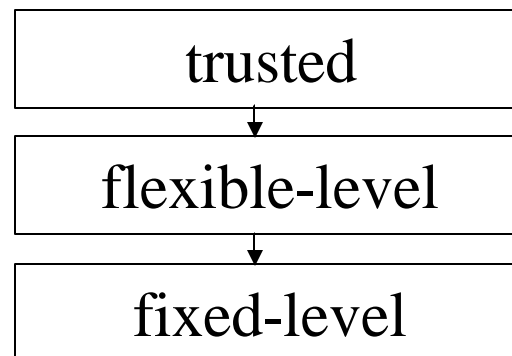
- Rules
  - s can always read o; after reading
$$i(s) \leftarrow \min[i(s), i(o)]$$
  - s can always write to o; after writing
$$i(o) \leftarrow \min[i(s), i(o)]$$
- Tracing, but not preventing contamination

# 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

# Meanings of Subject Integrity Levels

- When a subject has integrity level  $x$ ,
- three possibilities:
  1. **trusted**: generate information at level  $x$  from any data
  2. **flexible-level**: for any level  $y = x$ , can generate information at  $y$  when reading data at  $y$  or higher
  3. **fixed-level**: generate information at level  $x$  when reading data of integrity level  $x$  or higher



# Object Integrity Levels

- An object integrity level may be based on
  - **Quality** of information (levels may change)
    - degree of trustworthiness
  - **Importance** of the object (levels do not change)
    - degree of being trusted
- What should the relation between the two meanings, which one should be higher?

# Level Meanings for Biba Policies

	Subject integrity meaning	Object integrity meaning
Strict	Fixed-level	Importance + Quality
Subject Low-Water Mark	Flexible-level	Importance + Quality
Object Low-Water Mark	Fixed-level	Quality
Low-Water Mark Integrity Audit	Flexible-level	Quality
Ring	Trusted to handle low input	Importance

# 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 subjects

# 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

# 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.

# Coming Attractions ...

- October 16:
  - Role Based Access Control

