CS590U
Access Control: Theory and Practice

Lecture 7 (January 31)

Integrity: Biba

Integrity Considerations for Secure Computer Systems

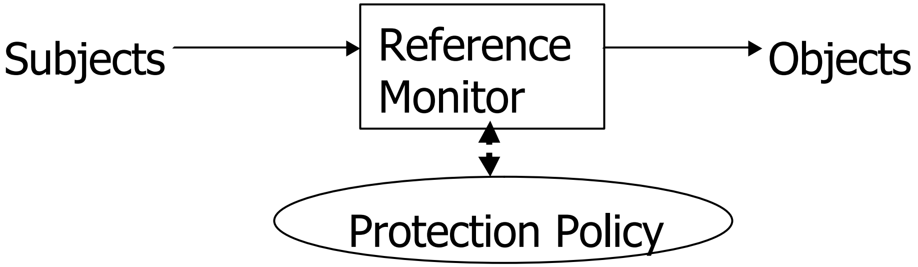
MITRE Report

Biba

Motivation

- Bell-LaPadula and other information-flow based security definitions address confidentiality, what about integrity
- What does integrity mean?
  - system integrity: system behave as expected
  - data integrity: data not changed in “incorrect” ways
- One 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

The Reference Monitor Concept



- A reference monitor must satisfy three properties
  - complete: all accesses are monitored and enforced
  - protected: its function may not be maliciously or accidentally modified by unauthorized forces
  - provably proper behavior: it must faithfully enforce the specified protection policy

Access Modes

- Observation: viewing of information
  - testing of information that results in a choice of distinct states of the observing subject
- Modification:
- Invocation: a service request from one subject to another
  - the subject being requested is modified.

Integrity Defined

- A subsystem possesses the property of integrity if it can be trusted to adhere to a well-defined code of behavior.
- How to guarantee integrity?
  - the subsystem needs to be initially determined (by some external agency) to perform properly.
    - e.g., using program verification technique
  - ensure that subsystem cannot be corrupted to perform in a manner contrary to the original determination.

The Integrity Problem

- The formulation of access control policies and mechanisms that provide a subsystem with the isolation necessary for protection from subversion
  - protection from intentionally malicious attack: unprivileged, intentionally malicious modification

Integrity Threats

- Two dimensions
  - subsystem external vs. subsystem internal
  - direct vs. indirect
- Four combinations:
  - external direct
  - external indirect
  - internal direct
  - internal indirect

Biba’s Integrity Policies

- Mandatory integrity policy
  - a protection policy, once defined for an object, is unchangeable and must be satisfied for all states of the system (as long as the object exists)
- Discretionary integrity policy
  - a protection policy may be dynamically defined by the user

Integrity Levels

- 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
    - quality of info in an object vs. importance of an object
- 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)

Five Mandatory Policies

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

Strict Integrity Policy

- Three rules:
  1. s can read o iff i(s) = i(o)
     - stops indirect sabotage by contaminated data
  2. s can write to o iff i(o) = i(s)
     - stops directly malicious modification
  3. s_1 can execute s_2 iff $i(s_2) = i(s_1)$
     - stops improper activation of more privileged subjects to cause damage to “higher” integrity level objects
- Ensures no information path from low-integrity object to high-integrity object
  - why is this desirable?

Subject Integrity Levels

- What does it mean that a subject is trusted to execute correctly at integrity level i1?
- Three possibilities:

1. generate information at level i1 from any data
2. generate information at level i1 when reading data of integrity level i1 or higher
3. generate information at any level i = i1 when reading data of integrity level i or higher

Object Integrity Levels

- An object integrity level may be based on
  - Quality of information (levels may change)
  - Importance of the object (levels do not change)
- Intuitively, quality integrity level should be at least as high as importance integrity level
- Quality integrity level may be higher than importance integrity level

Subject Low-Water Policy

- Subject’s integrity level decreases as reading lower integrity data
- 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)]
- Ensures that there is no information path from low integrity data to high integrity data

Object Low-Water Mark Policy

- The writing rule is relaxed: when s writes o, the integrity level of o is set to min[i(s),i(o)].
  - implies that object integrity level represents quality rather than importance
- Also ensures that there is no information path from a low integrity object to a high integrity object

Low-Water Mark Integrity Audit Policy

- The integrity levels of subjects and objects both change to reflect the contamination
  - After s observes o, the integrity level of s is lowered to min(i(s), i(o))
  - After s modifies o, the integrity level of o is lowered to min(i(s), i(o))

The Ring Policy

- Integrity levels of subjects and objects are fixed.
- 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 integrity 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

End of Lecture 7

- Next lecture
  - The Clark-Wilson Model and the Chinese Wall Model