Previous Class

• Concepts
  – Access Control, Subject, Object

• Goals of Access Control
  – Confidentiality, Integrity

• Access Matrix
  – View of Columns: Access Control Lists
  – View of Rows: Capability Lists

• Types of Access Control Policies
  – DAC
  – MAC
  – RBAC
In which scenarios DAC, MAC and RBAC should be used, respectively?

**DAC**: if the information you create really belongs to you and security is not the top priority, DAC is not a bad choice. It is flexible and convenient. E.g., social networks.

**MAC**: if the information you create belongs to your employer and it is highly sensitive, MAC is the choice.

**RBAC**: it can enforce DAC or MAC. When employees change jobs, the admin only needs to grant and revoke roles.
Outline

• Implementation of Policy Models
  – Decoupling Mechanisms and Policies
  – Reference Monitor
• Basics of MAC and Information Flow
• Mandatory Access Control Policy Models
  – Multi-level Security
    • Models for Confidentiality: e.g., Bell-LaPadula Model
    • Models for Integrity: e.g., Biba Model
  – Multi-lateral Security
    • Chinese-wall
Security Mechanism and Policy

- A security policy dictates what is, and what is not, allowed.
- A security mechanism is a method, tool, or procedure for enforcing a security policy.
- Therefore, the same mechanism can be used to enforce multiple different policies.
Decoupling Mechanisms and Policies

• When you implement some techniques or tools as the policy-enforcing mechanism, keep in mind that the policy may change. So the mechanism and policies should not be closely coupled.

• The mechanism should leave room of flexibility of changing policies.

• E.g., even the legislation department changes the traffic rules (policies), the same police (mechanism) can be used.
Security Policy Models

• A Security Policy Model provides a *formal* representation of the access control security policy and its working

• The formalization allows the proof of properties on the security provided by the access control system being designed
Reference Monitor

• When implementing the mechanism, a Reference Monitor that satisfies the following requirements is needed
  – Small enough to be verifiable
  – Non-bypassable
  – Tamper-resistant
MAC

• A *mandatory access control (MAC)* policy is a means of assigning access rights based on regulations by a central authority

• **Goal**: To prevent illegitimate information flow

• **Idea**: Attach a security label to each subject and object; and then perform authorization based on label comparison
Military Security

• Initially (‘70s) most research in information security was applied to the military domain
• Need to protect information that, if known by an enemy, might damage national security
Security Level

• Each subject and each object is assigned a security level
  – E.g., unclassified < confidential < secret < top secret
• A security level
  – for a subject is called a clearance
  – for an object is called a classification
• The clearance assigned to subjects reflects their trustworthiness, and the classification assigned to objects reflects theirs sensitivity
“Need to know” and compartments

• Even one has the “top secret” clearance, it should not mean that she can access everything
• “Need to know”: the access authorization is limited to information needed to perform duties
• How to enforce it?
  – Compartmentalization
  – Fewer people know the object, the less probability the information is leaked
• E.g., Manhattan Project
Security Class and the Ordering

• A security class = \((\text{security\_level}, \text{compartments})\)
• E.g., \((\text{confidential}, \{\text{nuclear, missile}\})\)
  – Security level: confidential
  – Compartments: \{nuclear, missile\}
• Ordering relation: \(\text{SC}_1 = (l_1, c_1), \text{SC}_2 = (l_2, c_2)\)
  – \(\text{SC}_1 \leq \text{SC}_2\) if \(l_1 \leq l_2 \land c_1 \subseteq c_2\)
• Some security classes are incomparable
  – \((\text{top\_secret}, \{\text{aircraft}\})\) and \((\text{securet}, \{\text{shelters}\})\)
Multi-level Security

- When access control is enforced according to the security levels (and compartments) assigned to subject and objects, it is a Multi-level Security (MLS) system.
- A MLS system is typically a Mandatory Access Control system.
Information flow policies

- Defined by Denning (’76)
- Concerned with the flow of information from one security class to another
- Information flow as an ordering relation
- Instead of a list of axioms governing users’ accesses, it simply require that information transfers obey the ordering relation
The BLP model

- A model for Confidentiality (i.e., Secrecy)
- Information cannot flow from a high security class to a low one (or an incomparable one)
  - How to define “high” and “low”?
  - Recall $SC_1 \leq SC_2$ if $l_1 \leq l_2$ && $c_1 \subseteq c_2$ where $SC_1 = (l_1, c_1)$, $SC_2 = (l_2, c_2)$
BLP mandatory access rules

- Object o’s security class: SC(o)
- Subject s’s security class: SC(s)
- **Simple property (or, No Read Up):** subject s can read object o only if SC(s) ≥ SC(o)
- ***-property (or, No Write Down):** subject s can write object o only if SC(s) ≤ SC(o)
  - Trojan horses leaking information are blocked
Figure 13.1 Information Flow Showing the Need for the *-property

CIS 4360 – Secure Computer Systems
BLP information flow
Limitations of the BLP Model

• Sometimes “illegal” information flow is desired
  – E.g., a teacher (high security class) may create a file called “paper”, which should be read by students (low security class)
  – E.g., a teacher may comment on the answers submitted by a student
  – Both are not disallowed in the BLP Model
  – Therefore in practice a declassifying component is needed

• BLP only provides confidentiality
  – In some cases, integrity is the main concern
The Biba Model

- Provides the protection for integrity
  - Information cannot flow from a low security class to a high one
- **Simple property (or, No Read Down):** subject $s$ can read object $o$ only if $SC(s) \leq SC(o)$
- ***-property (or, No Write Up):** subject $s$ can write object $o$ only if $SL(s) \geq SL(o)$
- **Invocation property:** $s_1$ can invoke $s_2$ only if $SL(s_1) \geq SL(s_2)$
- **Example**
  - Security level: soldier < captain < general
  - A captain should not trust an order forged by a soldier
  - An order issued by a general cannot be modified by a caption
Multi-Lateral Security

• Instead of enforcing vertical information flow rules, multi-lateral security prevents information from flowing across departments

• Classic Model: the Chinese Wall Model

• Goal: to prevent conflict of interest
  – E.g., in a financial consultant company, an employee who has read the documents of Bank A (to provide advices) should not access those of Bank B
Multi-Lateral Security

• A Dataset (DS): all objects that belong to the same corporation

• Conflict of Interest (CI) class: All datasets whose corporations are in competition

• A subject S can read on object O only if
  – O is in the same DS as an object accessed by S, or
  – O belongs to a CI from which S has not yet accessed any information
Example: Multi-Lateral Security

Once John has accessed the objects of Bank A, he is not allowed to access those of Bank B, as the two Banks belong to the same CI.
Summary

• Bell-LaPadula (BLP) Secrecy Model
  – No read up
  – No write down

• Biba Integrity Model
  – No read down
  – No write up

• Chinese Wall Model
  – If you have accessed a corporation, you cannot read data from its competitors
Writing Assignments

• Can a user cleared for (S, {dog, cat, pig}) access to documents classified in the following ways under the BLP model?
  – (TS, {dog})
  – (S, {dog})
  – (S, {dog, cow})
  – (S, {monkey})
  – (C, {dog, pig, cat})
  – (C, { })

• Can BLP and Biba be enforced in the same system?