Mandatory Flow Control Models

Kelly Westbrooks
Department of Computer Science
Georgia State University

April 5, 2007
Mandatory Flow Control Models

Information Flow Control

Lattice Model

Multilevel Models
  - The Bell-LaPadula Model
  - The Biba Model
Mandatory Flow Control Models

**Definition**

The **Mandatory Flow Control Models** are the subset of computer security models that require access control of all subjects and objects under its control on a *systemwide basis*.

Only *trusted* objects are allowed to violate access control rules in a mandatory flow control model.
The major problem with the Access Control Matrix Model

- The *Confinement Problem*: How to determine whether there is any mechanism by which a subject authorized to access an object may leak information contained in that object to some other subjects not authorized to access that object.

- The confinement problem is *undecidable* due to the characteristic of discretionary transfer of access rights between subjects in the access control matrix model.

- Security control should be applied to the information in addition to the subject holding the information.
Information Flow Control is concerned with how information is disseminated or propagated from one object to another.

- System entities are partitioned into *security classes*
- Every channel through which information can flow between security classes has regulation applied to it.
Introduced by Dr. Dorothy Denning of Georgetown University.

The best known information flow control model.

Based upon the concept of a lattice from mathematics.

The security of a system based upon the lattice model is easily proven mathematically.
The Lattice Model (continued)

**Definition**

A relation between set $A$ and set $B$ is a subset of $A \times B$.

**Definition**

A partial order $\leq$ is a relation between $A$ and $A$ with the following properties:

- **reflexive** $\forall a \in A, \ a \leq a$
- **antisymmetry** $\forall a, b \in A, \ a \leq b \text{ and } b \leq a \Rightarrow a = b$
- **transitivity** $\forall a, b, c \in A, \ a \leq b \text{ and } b \leq c \Rightarrow a \leq c$

A total order is a partial order such that $\forall a, b \in A, \ a \leq b \text{ or } b \leq a$.
The Lattice Model (continued)

**Definition**

A **poset**, or *partially ordered set* is a set $P$ equipped with a partial order $\leq$. A **linearly ordered** set is a set equipped with a total order.

**Definition**

Given a poset $P$ and a subset $S \subseteq P$, the **supremum** of $S$ is the element $s \in P$ such that $\forall x \in \{y \in P \mid \forall z \in S, z \leq y\}$, $s \leq x$. The **infimum** of $S$ is the element $i \in P$ such that $\forall x \in \{y \in P \mid \forall z \in S, y \leq z\}$, $x \leq i$.

**Definition**

A **lattice** is a poset $P$ such that $\forall S \subseteq P$, $|S| = 2$, $S$ has both a supremum and an infimum.
<table>
<thead>
<tr>
<th>The Lattice Model (continued)</th>
</tr>
</thead>
</table>

- All subjects and objects are partitioned into security classes.
- Security classes form a poset.
- Information flow only occurs in the direction of the partial ordering; information can only flow from a lower class to a higher class.
A lattice model of secure information flow is the 7-tuple $\langle S, O, SC, F, \oplus, \otimes, \rightarrow \rangle$:

- $S$ set of subjects
- $O$ set of objects
- $SC$ poset of security classes
- $F$ the binding function $F : S \cup O \rightarrow SC$
- $\oplus$ The infimum operator on $SC$
- $\otimes$ The supremum operator on $SC$
- $\rightarrow$ The flow relation on pairs of security classes.
In addition to reflexitivity, antisymmetry, and transitivity, there are two other mathematical properties of a lattice that are useful for secure information flow control models:

**aggregation** \( A \rightarrow C \) and \( B \rightarrow C \) \( \Rightarrow \) \( A \cup B \rightarrow C \)

**separation** \( A \cup B \rightarrow C \) \( \Rightarrow \) \( A \rightarrow C \) \textit{and} \( B \rightarrow C \)
Multilevel Security is a special case of the lattice-based information flow model. There are two well-known multilevel security models:

**The Bell-LaPadula Model**  Focuses on confidentiality of information

**The Biba Model**  Focuses on system integrity
The Bell-LaPadula Model

- $L$ is a linearly ordered set of *security levels*
- $C$ is a lattice of *security categories*
- The security level is called the *clearance* if applied to subjects, and *classification* if applied to objects.
- Each security category is a set of *compartments* that represent natural or artificial characteristics of subjects and objects and is used to enforce the *need-to-know* principle.
- The lattice of security classes is $L \times C$. If $A, B \in SC$, $A$ *dominates* $B$ if $A$'s level is higher than $B$'s level and $B$'s category is a subset of $A$'s category.
Security with respect to confidentiality in the Bell-LaPadula model is described by the following two axioms:

**Simple security property** reading information from an object \( o \) by a subject \( s \) requires that \( F(s) \) dominates \( F(o) \)

***-property** Writing information to an object \( o \) by a subject \( s \) requires that \( F(o) \) dominates \( F(s) \)
The Biba Model

- $L$ is a linearly ordered set of *integrity levels*
- $C$ is a lattice of *integrity categories*
- Integrity categories are used to enforce the *need-to-have* principle.
- The lattice of security classes is $L \times C$. 
Security with respect to integrity in the Biba model is described by the following two axioms:

**Simple security property** Writing information to an object $o$ by a subject $s$ requires that $F(s)$ dominates $F(o)$

***-property** Reading information from an object $o$ by a subject $s$ requires that $F(o)$ dominates $F(s)$
The Bell-LaPadula Model is concerned with information confidentiality
- subjects reading from an object must have higher a security class than the object.
- objects being written to by a subject must have higher security class than the subject.

The Biba model emphasizes information integrity
- subjects writing information to an object must have higher a security class than the object.
- objects being read from by a subject must have higher security class than the subject.