Chapter 8

8.3 Mandatory Flow Control Models

Sasibala Modala
Department of Computer Science
Georgia State University

28 Oct. 2009
Contents

• Mandatory Flow Control Models
  • Information Flow Control
  • Lattice Model
  • Multilevel Security
    • The Bell-LaPadula Model
    • The Biba Model
  • Comparison Bell - LaPadula and Biba Models.
Contents

• Happenings in the field of Computer Science
  • iList : Intelligent Tutoring System for Computer Science

• Future Endeavors
  • Getting Ready for HTML 5 - 5 New Exciting Features
• How information is propagated from one object to another.
• All the system entities are classified into several Security Classes.
• The security classes of all entities must be specified explicitly and the class of an entity never changes after it has been created.
Lattice Model [1, Randy & Johnson, 1997]

A lattice model of secure information flow is the 7-tuple \( (S, O, SC, F, \oplus, \otimes, \rightarrow) \)

- \( S \) 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.
Lattice Model  [1, Randy & Johnson, 1997]

- Using the previous definitions, a Flow Model is considered secure only if it does not violate the relation \( \rightarrow \).

- Couple of examples are cited in the textbook.

- Example: \( X = \{x,y,z\} \). The least upper bound of security classes \( \{x\} \) and \( \{z\} \) is \( \{x,z\} \). The greatest lower bound of security classes \( \{x,y\} \) and \( \{y,z\} \) is \( \{y\} \).
Lattice Model [1, Randy & Johnson, 1997]

- The relation $\rightarrow$ is reflexive, transitive and antisymmetric for all $A, B, C \in \text{SC}$.
  - Reflexive: $A \rightarrow A$
    - Information flow from an object to another object at the same class does not violate security.
  - Transitive: $A \rightarrow B$ and $B \rightarrow C$ implies $A \rightarrow C$.
    - This indicates that a valid flow does not necessarily occur between two classes adjacent to each other in the partial ordering.
  - Antisymmetric: $A \rightarrow B$ and $B \rightarrow A$ implies $A = B$
    - If information can flow back and forth between two objects, they must have the same classes.
Lattice Model [I, Randy & Johnson, 1997]

- Two other inherent properties are as follows

- Aggregation: $A \rightarrow C$ and $B \rightarrow C$ implies $A \cup B \rightarrow C$
  - If information can flow from both $A$ and $B$ to $C$, the information aggregate of $A$ and $B$ can flow to $C$.

- Separation: $A \cup B \rightarrow C$ implies $A \rightarrow C$ and $B \rightarrow C$
  - If the information aggregate of $A$ and $B$ can flow to $C$, information can flow from either $A$ or $B$ to $C$.
MultiLevel Security [1, Randy & Johnson, 1997]

- Prevent users from obtaining access to information for which they lack authorization.

- Two models are proposed to solve this problem.
  - Bell - LaPadula Model
  - Biba Model.
Bell - LaPadula Model [1, Randy & Johnson, 1997]

- This system mainly concentrates on confidentiality of the system.

- The simple security property:
  
  - SC(s) dominates SC(o): The subject cannot view the information contained in an object unless the security class of Subject is at least as high as the security class of the Object.

- The *- property:
  
  - SC(o) dominates SC(s): This prevents a subject from modifying an Object unless the security class of Object is greater than equal to the class of the Subject.
Bell - LaPadula Model [1, Randy & Johnson, 1997]

Available data flows using an MLS system.

- **File A**: Label: Top Secret, Write only
- **File B**: Label: Secret, Read / Write
- **File C**: Label: Confidential, Read only
- **File D**: Label: Unclassified, Read only

Process
Label: Secret

Processes can read the same or lower security levels but can only write to their own or higher security level.
Biba Model [1, Randy & Johnson, 1997]

- This system mainly concentrates on system integrity.
- Prevent malicious modification of objects.
  - The simple integrity property:
    - $\text{SC}(s)$ dominates $\text{SC}(o)$: The subject cannot modify the information contained in an object unless the integrity class of Subject is at least as high as the security class of the Object.
  - The *- property:
    - $\text{SC}(o)$ dominates $\text{SC}(s)$: This prevents a subject from reading an Object unless the integrity class of Object is greater than equal to the class of the Subject.
Biba Model [I, Randy & Johnson, 1997]
# Comparision

[1, Randy & Johnson, 1997]

<table>
<thead>
<tr>
<th>Bell - LaPadula Model</th>
<th>Biba Model</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How to prevent information leakage</strong></td>
<td><strong>How to protect information corruption.</strong></td>
</tr>
<tr>
<td>Read - SC(s) &gt;= SC(o)</td>
<td>Write - IC(o) &lt;= IC(s)</td>
</tr>
<tr>
<td>Information Flow -</td>
<td>Information Flow -</td>
</tr>
<tr>
<td>E (low &amp; small) → E(high &amp; large)</td>
<td>E (high &amp; large) → E(low &amp; small)</td>
</tr>
<tr>
<td>Any downward flow - violation</td>
<td>Any upward flow - violation.</td>
</tr>
</tbody>
</table>
Most Recent Happenings
An Intelligent Tutoring System for Computer Science

[2,3, Skykes, David Fossati]

- Interactive rich learning environment for students.
- More effective than traditional style of teaching.
Problem
Change the list L so that it represents [2, 3, 1, 8].

Feedback
Welcome to iList - Version 0.60
Starting problem 1.
Warning:
The list L has incorrect values.
You have lost one or more nodes.

Operations
Node *T;
T = new Node;
T->data = 3;
T->link = L->link;
L = T;

Variables
L
T

Heap
1
2
3
4
8

Message
Warning:
The list L has incorrect values.
You have lost one or more nodes.
OK
5 New Exciting Features of HTML 5 - A Bit of History

- Development stopped in 1999 after HTML 4.01.
- Current specifications are inadequate for today’s requirements.
- Address growing demand for more complex web content.
- Thinking began in late 2003.
- W3C expressed interest in the HTML 5 draft developed by WHATWG.
- WHATWG - group from Apple, Mozilla and Opera.
5 New Exciting Features of HTML 5

- New HTML elements that improve our ability to describe content.

\[<p>This text is a paragraph</p>\]
5 New Exciting Features of HTML 5

Describing the structure of a web page in HTML 4

```
<div id="header"> This div element contains branding like the logo
</div>

<div id="nav"> This div element contains the site navigation
</div>

<div id="content"> This div element contains the web page’s main content
</div>

<div id="sidebar"> This div element contains extra information and related content/links
</div>

<div id="footer"> This div element contains copyright information
</div>
```

Describing the structure of a web page in HTML 5

```
<header> This element contains branding like the logo
</header>

<nav> This element contains the site navigation
</nav>

<article> This element contains the web page’s main content
</article>

<aside> This element contains extra information and related content/links
</aside>

<footer> This element contains copyright information
</footer>

Wednesday, October 28, 2009
5 New Exciting Features of HTML 5.

- Improved web forms handling.
5 New Exciting Features of HTML 5.

```html
<form>
  <label>Enter a username *</label>
  <input name="username" type="text" />
  <label>Enter email *</label>
  <input name="email" type="text" />
  <input name="submit" type="submit" value="submit" />
</form>
```

**HTML 4 Representation**

```html
<form>
  <label>Enter a username *</label>
  <input name="username" required type="text" />
  <label>Enter email *</label>
  <input name="email" required email type="text" />
  <input name="submit" type="submit" value="submit" />
</form>
```

**HTML 5 Representation**
5 New Exciting Features of HTML 5.

- APIs for easier web application development.

```html
<video src="myvideo.flv" autoplay="true" controls>
    Fall back text for browsers that don’t support the video element
</video>
```
5 New Exciting Features of HTML 5.

- The canvas element allows image scripting on the fly.

For example, the pie chart gives you a much easier way of understanding the scale of percentages.
• Users can edit and interact with sections of a web page.

• The `contenteditable` attribute (true or false) which allows us to indicate which parts of the web page a user can edit.

• Useful for wiki-style websites, in which content is user-generated.

• Another use of the `contenteditable` attribute would be to create web page templates. You can allow certain regions of a web page to be open to content editing and lock other regions that shouldn't be changed. This gives users of your website who aren't proficient in HTML an opportunity to input content safely without affecting critical areas that should be handled by more knowledgeable users.
5 New Exciting Features of HTML 5 - Summary

- The proposed specifications are expected to reach W3C Candidate Recommendation status in 2012, but that doesn't mean you have to wait that long to start using some of the new things in HTML 5. A lot of modern browsers, for example, have already implemented the `<canvas>` element (including Mozilla Firefox).

- HTML 5 will redefine how web developers mark up content.

- It will provide a better way to describe the content displayed on a web page, enable more complex content types, improve media and web application support, and increase the interoperability of HTML documents.
References


Thank you.