Confidentiality Policies

- Overview
  - What is a confidentiality model
- Bell-LaPadula Model
  - General idea
  - Informal description of rules
  - Formal description of rules
Confidentiality Policy

- Goal: prevent the unauthorized disclosure of information
  - Deals with information flow
  - Integrity incidental
- Multi-level security models are best-known examples
  - Bell-LaPadula Model basis for many, or most, of these
“Governmental” policies

- US Privacy Act
  - Income tax returns are confidential
- Executive privilege
  - People working in the government must limit the distribution of certain docs and info.
Bell-LaPadula Model, Step 1

- Security levels arranged in linear ordering
  - Top Secret: highest
  - Secret
  - Confidential
  - Unclassified: lowest

- Levels consist of security clearance L(s)
  - Objects have security classification L(o)
  - Subjects have security clearance L(s)
### Example

<table>
<thead>
<tr>
<th>security level</th>
<th>subject</th>
<th>object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Secret</td>
<td>Tamara</td>
<td>Personnel Files</td>
</tr>
<tr>
<td>Secret</td>
<td>Samuel</td>
<td>E-Mail Files</td>
</tr>
<tr>
<td>Confidential</td>
<td>Claire</td>
<td>Activity Logs</td>
</tr>
<tr>
<td>Unclassified</td>
<td>Andrew</td>
<td>Telephone Lists</td>
</tr>
</tbody>
</table>

- Tamara can read all files
- Claire cannot read Personnel or E-Mail Files
- Andrew can only read Telephone Lists

*Computer Security: Art and Science*

©2002-2004 Matt Bishop
Reading Information

- Information flows *up*, not *down*
  - “Reads up” disallowed, “reads down” allowed
- Simple Security Condition (Step 1)
  - Subject $s$ can read object $o$ iff, $L(o) \leq L(s)$ and $s$ has permission to read $o$
  - Sometimes called “no reads up” rule
Writing Information

- Information flows up, not down
  - “Writes up” allowed, “writes down” disallowed
- *-Property (Step 1)
  - Subject $s$ can write object $o$ iff $L(s) \leq L(o)$ and $s$ has permission to write $o$
  - Sometimes called “no writes down” rule
- If Tamara copies from the Personnel file to an Activity log, then Claire and Samuel can see the data from the Personnel file.
Basic Security Theorem, Step 1

- If a system is initially in a secure state,
- and every transition of the system satisfies
  - the simple security condition, step 1 (i.e. “no reads up”),
  - and the *-property, step 1 (i.e. “no writes down”),
- then every state of the system is secure
Bell-LaPadula Model, Step 2

- Expand notion of security level to include categories
- Security level is (*clearance, category set*)
- Examples
  - (Top Secret, \{NUC, EUR, ASI\})
  - (Confidential, \{EUR, ASI\})
  - (Secret, \{NUC, ASI\})
Figure 5–2  Lattice generated by the categories NUC, EUR, and US. The lines represent the ordering relation induced by $\subseteq$. 
Levels and Lattices

\[(A, C) \text{ dom } (A', C') \text{ iff } A' \leq A \text{ and } C' \subseteq C\]
  - \(A\) – clearance or classification
  - \(C\) – category (also called compartment)

Examples
  - (Top Secret, \{NUC, ASI\}) \text{ dom } (Secret, \{NUC\})
  - (Secret, \{NUC, EUR\}) \text{ dom } (Confidential, \{NUC, EUR\})
  - (Top Secret, \{NUC\}) \not\text{ dom } (Confidential, \{EUR\})
Reading Information

- Information flows *up*, not *down*
  - “Reads up” disallowed, “reads down” allowed
- Simple Security Condition (Step 2)
  - Subject $s$ can read object $o$ iff $L(s) \text{ dom } L(o)$ and $s$ has permission to read $o$
  - Sometimes called “no reads up” rule
Writing Information

- Information flows up, not down
  - “Writes up” allowed, “writes down” disallowed
- *-Property (Step 2)
  - Subject $s$ can write object $o$ iff $L(o) \subseteq L(s)$ and $s$ has permission to write $o$
  - Sometimes called “no writes down” rule
Basic Security Theorem, Step 2

- If a system is initially in a secure state, and every transition of the system satisfies the simple security condition, step 2, and the *-property, step 2, then every state of the system is secure.
Problem

- Colonel has (Secret, \{NUC, EUR\}) clearance
- Major has (Secret, \{EUR\}) clearance
  - Major can talk to colonel ("write up" or "read down")
  - Colonel cannot talk to major ("read up" or "write down")
- Clearly absurd!
Solution

- Define maximum, current levels for subjects
  - \( \maxlevel(s) \) \( \text{dom} \) \( \curlevel(s) \)

- Example
  - Treat Major as an object (Colonel is writing to him/her)
  - Colonel has \( \maxlevel \) (Secret, \{ NUC, EUR \})
  - Colonel sets \( \curlevel \) to (Secret, \{ EUR \})
  - Now \( L(\text{Major}) \) \( \text{dom} \) \( \curlevel \) (Colonel)
    - Colonel can write to Major without violating “no writes down”