Lecture 23: Lipner’s Model

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Commercial Integrity Constraints

Recall that Steve Lipner (Microsoft) described some integrity concerns you might find in a commercial data processing environment:

- Users will not write their own programs, but use existing production software.
- Programmers develop and test applications on a nonproduction system, possibly using contrived data.
- Moving applications from development to production requires a special process.
- This process must be controlled and audited.
- Managers and auditors must have access to system state and system logs.

Can we use our existing modeling mechanisms to build a secure system that addresses such constraints?

Lipner’s Integrity Matrix Model

Lipner devised his Integrity Matrix Model to handle those concerns via a combination of BLP and Biba Integrity.

There are two confidentiality levels:
- Audit Manager (AM): system audit and management.
- System Low (SL): all other processes.

In addition there are three confidentiality categories:
- Production (SP): production code and data.
- Development (SD): programs under development.
- System Development (SSD): system programs in development.

In addition to the confidentiality constraints, we also impose integrity constraints. There are three integrity classification (highest to lowest):

- System Program (ISP): system software
- Operational (IO): production programs and development software
- System Low (ISL): user level behavior

and two integrity categories:

- Development (ID)
- Production (IP)
**Subject Levels**

Security levels (both confidentiality and integrity) are assigned to subjects based on their roles in the organization and their need to know.

<table>
<thead>
<tr>
<th>User Role</th>
<th>Confidentiality</th>
<th>Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ordinary users</td>
<td>(SL, {SP})</td>
<td>(ISL, {IP})</td>
</tr>
<tr>
<td>Application developers</td>
<td>(SL, {SD})</td>
<td>{ISL, {ID}}</td>
</tr>
<tr>
<td>System programmers</td>
<td>(SL, {SSD})</td>
<td>{ISL, {ID}}</td>
</tr>
<tr>
<td>System managers/auditors</td>
<td>(AM, {SP, SD, SSD})</td>
<td>{ISL, {IP, ID}}</td>
</tr>
<tr>
<td>System controllers</td>
<td>(SL, {SP, SD})</td>
<td>{ISP, {IP, ID}}</td>
</tr>
</tbody>
</table>

Here *downgrade* means the ability to move software (objects) from development to production.

**Object Levels**

Security levels (both confidentiality and integrity) are assigned to objects based on who should access them.

<table>
<thead>
<tr>
<th>Object type</th>
<th>Confidentiality</th>
<th>Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development code/test data</td>
<td>(SL, {SD})</td>
<td>{ISL, {IP}}</td>
</tr>
<tr>
<td>Production code</td>
<td>(SL, {SP})</td>
<td>{ISL, {IP}}</td>
</tr>
<tr>
<td>Production data</td>
<td>(SL, {SP})</td>
<td>{ISL, {IP}}</td>
</tr>
<tr>
<td>Software tools</td>
<td>(SL, {})</td>
<td>{IO, {IP}}</td>
</tr>
<tr>
<td>System programs</td>
<td>(SL, {})</td>
<td>{ISP, {IP, ID}}</td>
</tr>
<tr>
<td>System programs in modification</td>
<td>(SL, {SSD})</td>
<td>{ISL, {ID}}</td>
</tr>
<tr>
<td>System and application logs</td>
<td>(AM, {categories})</td>
<td>{ISL, {}}</td>
</tr>
</tbody>
</table>

**Lipner’s Model**

Some questions:
- Can an ordinary user utilize a system program? Modify it?
- Can a system programmer use production software? Modify it?
- Why is that special downgrade permission required? Could it be done with BLP and Biba alone?

The answers:
- That depends on what “utilize” means. If “utilize” means “read” then he can read, but not modify.
- Neither.
- Moving objects from the development to production world means changing their labels. There’s no obvious way to do that in BLP or Biba.

- Lipner developed a hybrid policy using both BLP and Biba’s Strict Integrity to address commercial integrity concerns.
- Some modifications relating to tranquility were required to allow moving applications from the development to production domains.
- The result is acceptable but not entirely intuitive. Perhaps an entirely new modeling paradigm would be preferable.

**Lessons**

Next lecture: Clark-Wilson Model