Protection and Security

- **Areas of Concern:**
  privacy: legal, social
  security: external vs. internal
  protection: mechanisms

- **Topics:**
  authentication: verifying a claim of identity
  authorization: verifying a claim of permission

- **Models:**
  discretionary vs. non-discretionary
  access control vs. flow control

Access Matrix Model

Access Matrix

- **Objects:**
  $O_1, O_2, O_3$

- **Subjects:**
  $s_1, s_2, s_3$

  grouped by subject

  $s_1$

  $s_2$

  $s_3$

  **Capability Lists**

Lock and Key Method

- **Subjects** possess a set of keys:

  Key $(O, k)$

  Lock $(k, [r_1, r_2, ...])$

  objects are associated with a set of locks:

Comparison of methods

<table>
<thead>
<tr>
<th></th>
<th>Capability list</th>
<th>Access Control links</th>
<th>Locks &amp; Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>propagation</td>
<td></td>
<td></td>
<td>🐄 1 🐄 3 🐄 1</td>
</tr>
<tr>
<td>review</td>
<td>🐄</td>
<td>🐄</td>
<td>🐄 4</td>
</tr>
<tr>
<td>revocation</td>
<td>🐄</td>
<td>🐄</td>
<td>🐄 4</td>
</tr>
<tr>
<td>reclamation</td>
<td>🐄</td>
<td>🐄</td>
<td>🐄 4</td>
</tr>
</tbody>
</table>

1. need copy bit/count for control
2. need reference count
3. need user/hierarchical control
4. need to know subject-key mapping
Safety

- **primitive operation**: the atomic actions of the protection model
- **commands**: useful, commonly used collections of primitive operations
- **mono-operational**: all commands are primitive operations
- **“leaks”**: a command leaks a given right if its execution can cause the right to be propagated to a subject not previously possessing that right
- **safety**: an initial state/configuration is safe for a given right if there does not exist a reachable state within which a command leaks that right
- **decidability**: safety is decidable for a mono-operational system. Safety is not decidable for an arbitrary configuration of an arbitrary protection system however, safety may be decidable for specific protection systems

Take-Grant Model

**Granting a Right**

- $g$ from $X$ to $Y$
- $g$ from $X$ to $Z$
- $t$ from $Y$ to $Z$

**Taking a Right**

- $g$ from $X$ to $Y$
- $g$ from $X$ to $Z$
- $t$ from $Y$ to $Z$