Protection and Security

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

• **Topics:**
  - authentication: verifying a claim of cyber-identity
  - certification: verifying a claim of real-world identity
  - authorization: verifying a claim of permission

• **Models:**
  - discretionary vs. nondiscretionary
  - access control vs. flow control

---

**Access Matrix Model**

<table>
<thead>
<tr>
<th>Subjects</th>
<th>( P[s,o] )</th>
<th>Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>( o )</td>
<td></td>
</tr>
</tbody>
</table>

Access Matrix

Grouped by subject

Capability Lists

Access Matrix

Grouped by object

Access Control Lists
Lock and Key Method

subjects possess
a set of keys:

Key
(O, k)

Lock
(k, \{k_1, k_2, \ldots\})

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>☹ 1</td>
<td>☹ 3</td>
<td>☹ 1</td>
</tr>
<tr>
<td>review</td>
<td>☹ 4</td>
<td>☹ 4</td>
<td>☹ 4</td>
</tr>
<tr>
<td>revocation</td>
<td>☹ 3</td>
<td>☹ 3</td>
<td>☹ 3</td>
</tr>
<tr>
<td>reclamation</td>
<td>☹ 2</td>
<td>☹ 2</td>
<td>☹ 2</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
- **monooperational**: 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 monooperational 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**

**Taking a Right**

```
X \( \xrightarrow{t} \) Y \{r\} \{r,w\}
X \( \xrightarrow{t} \) Y \{r\} \{r,w\}
```

```
Take-Grant Model

Granting a Right

\[ X \xrightarrow{\{r,w\}} Z \xrightarrow{g} Y \]

\[ X \xrightarrow{\{r,w\}} Z \xrightarrow{g} \{r\} \]