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**

- **Access Matrix**

<table>
<thead>
<tr>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>s_1</td>
<td>s_2</td>
<td>s_3</td>
</tr>
</tbody>
</table>

  - Grouped by subject

  **Capability Lists**

<table>
<thead>
<tr>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>s_1</td>
</tr>
<tr>
<td>s_2</td>
</tr>
<tr>
<td>s_3</td>
</tr>
</tbody>
</table>

**Lock and Key Method**

- Subjects possess a set of keys:

```
Key (O, k)
```

- Objects are associated with a set of locks:

```
Lock (k, (r_1, r_2, ...))
```

---

**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>★</td>
</tr>
<tr>
<td>review</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>revocation</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>reclamation</td>
<td>★</td>
<td>★</td>
<td>★</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

**Taking a Right**

\[
\begin{align*}
X & \rightarrow Y \\
Y & \rightarrow Z
\end{align*}
\]

\[\{r,w\}\]

**Granting a Right**

\[
\begin{align*}
X & \rightarrow Y \\
Y & \rightarrow Z
\end{align*}
\]

\[\{r\}\]

\[\{r,w\}\]