Security:

goals
- shared use: privacy
- non-interference
- attack: internal, external
- robustness
- confidentiality: data actions
- integrity: data, unauthorized destruction
- availability: denial of service

access controls:
- privilege escalation: setuid

```
root
+----+----+
<table>
<thead>
<tr>
<th>getty</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
</tr>
</tbody>
</table>
| reads user password
| checks sets ID -> user |
```

```
Blockboard:

```
/inst/bin/hwsubsystem
setuid HWS
```
**Capabilities:**

**Unix:**
- root with all capabilities
- root with dropped capabilities

**Authentication:**

- No authentication
  - hard-wired terminal, etc.

**something you know:** password
- have token
  - do biometrics

```plaintext
<table>
<thead>
<tr>
<th>passwd</th>
</tr>
</thead>
<tbody>
<tr>
<td>plain text</td>
</tr>
<tr>
<td>hashed</td>
</tr>
<tr>
<td>hash + nonce (&quot;salt&quot;)</td>
</tr>
<tr>
<td>challenge + auth. (CHAP)</td>
</tr>
</tbody>
</table>
```

```plaintext
passwd + x ↦ f x
```

```plaintext
CHAP
```

```plaintext
SYS
```

```plaintext
X ↦ f x
```

```plaintext
hash(x + passwd)
```

```plaintext
hash(passwd + x)
```

```plaintext
user
```

```plaintext
secure
```

```plaintext
insecure
```

```plaintext
sys
```

```plaintext
secure
```

```plaintext
insecure
```