1. Goals
   Protection from self
   Protection from others
   Protection of files
   Protection of memory and other resources

Mechanisms and policies
2. Principles of Protection
   Principle of least privilege
3. Domain of Protection
   - Domain Structure
     Static or Dynamic
     Users, processes, procedures can be domains
     Sets of the above
   - Example: Unix
   - Example: MULTICS
4. Access Matrix

<table>
<thead>
<tr>
<th>object domain</th>
<th>$F_1$</th>
<th>$F_2$</th>
<th>$F_3$</th>
<th>printer</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_1$</td>
<td>read</td>
<td></td>
<td>read</td>
<td></td>
</tr>
<tr>
<td>$D_2$</td>
<td></td>
<td></td>
<td></td>
<td>print</td>
</tr>
<tr>
<td>$D_3$</td>
<td></td>
<td>read</td>
<td>exec</td>
<td></td>
</tr>
<tr>
<td>$D_4$</td>
<td></td>
<td>read</td>
<td></td>
<td>read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>write</td>
<td>write</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>object domain</th>
<th>$F_1$</th>
<th>$F_2$</th>
<th>$F_3$</th>
<th>laser printer</th>
<th>$D_1$</th>
<th>$D_2$</th>
<th>$D_3$</th>
<th>$D_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_1$</td>
<td>read</td>
<td></td>
<td>read</td>
<td>switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$D_2$</td>
<td></td>
<td></td>
<td></td>
<td>print</td>
<td></td>
<td></td>
<td>switch</td>
<td>switch</td>
</tr>
<tr>
<td>$D_3$</td>
<td></td>
<td>read</td>
<td>exec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$D_4$</td>
<td>read</td>
<td>write</td>
<td>write</td>
<td>switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Implementation of Access Matrix
   Sparse
   Global Table
   Access lists for Objects
   Capability lists for Domains
6. (Role Based) Access Control
7. Revocation of Access Rights
8. Capability-Based Systems
9. Language-Based Protection
   Java is a good example.
The Security Problem Protection, threat, attack.

Is it like your home?

Breach of confidentiality
Breach of integrity
Breach of availability
Theft of service
Denial of service Some of these happen at simple levels.

Security measures:

Physical
Human
Operating System
Network
Program threats Trojan horse ... consider the use of the “.” character in a search path. The “.” tells the shell to include the current directory in the search. Thus, if a user has “.” in her search path, has set her current directory to a friend’s directory, and enters the name of a normal system command . . .

Trap door emacs
Logic bomb Oregon highways
Stack and buffer overflow
Viruses

System and Network Threats Worms
Port scanning
Denial of service

Cryptography

User Authentication