Protocol Downgrade Attack
Sometimes an attacker can use protocol downgrade while a user tries to access a server, and become the middleman. A simple example would be a person sitting in a cafe trying to access his/her bank’s site.

Here if the user tries to access the bank’s site with HTTP or forgets to mention HTTPS and browser by default uses HTTP, then an attacker can become the middleman. All the queries and results will go through him. He will convert the HTTPS results by bank to HTTP and send to the user.

Note: To avoid this kind of problem make sure to use HTTPS wherever possible and try to use ”SSL Everywhere” plugin in firefox.

Access Control
- Service provider receives request from clients.
- Need to specify which client can perform which actions.
- Need to implement decisions.

1. Access Control Matrix {RBAC(Role Based Access Control)}
2. Access control lists
3. Bell-Lapadula

1. Access Control Matrix:
   ACM is basically a matrix that describes who can do what to what.
   There are three entities in ACM.
   - Subject: users (unix, windows) or applications (android)
   - Objects: In case of file systems, objects are files and directories.
   - Operations: For files (read and write) and Directories (create, delete, lookup and list)

Commands: What certain commands do...

\[
\text{\texttt{chmod} (executor, object, user, permission)}
\]
\[
\text{if}(A[\text{executor}][\text{object}] \ni \text{"owner")}
\]
\[
\text{then } A[\text{user}][\text{object}] \leftarrow \text{permission}
\]
chown: Here condition will be checked
(executor == root)

<table>
<thead>
<tr>
<th>Subject</th>
<th>/etc/passwd</th>
<th>abc</th>
<th>xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rob</td>
<td>Read, write</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gaurav</td>
<td>Read, write, owner</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: Access Control Matrix

Harrison Ruzzo Ullman Model (HRU Model): It determines whether ACM can evolve to bad state is undecidable.

2. Access Control Lists (ACL)
Most systems store ACLs. This is basically just a column of the Access Control Matrix.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>faculty</td>
<td>r</td>
</tr>
<tr>
<td>rob</td>
<td>rw</td>
</tr>
</tbody>
</table>

Figure 3: Access Control List

Major Issue: ACL’s monotonocity (i.e. Order Dependence)
Suppose a user is mentioned in an ACL and also a group is mentioned with the same user. Now if the permission given to that user and its group are different then, how to proceed. There are few strategies that can be used:
- First Match
- Last Match
- Most Restrictive
- Most Permissive
- More Specific

Negative Values in ACL: An ACL can be either "normal" or "negative". Normal rights grant the specified access permissions, while negative rights allow one to cancel specific permissions for a user or group on an ACL.
3. Bell-Lapadula
This model focuses on data confidentiality and controlled access to classified information. The entities in an information system are divided into subjects and objects. The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system satisfies the security objectives of the model.

There are two types of tags:
- Access Level (like Top Secret, Secret, FOUO For Official Use Only, Public)
- Compartments (Area like JFK, Stony Brook, Area51)

Object \((L, CS)\) \{Level \(L\) and Compartment \(CS\)\}
Subject \((L', CS')\)
In this scenario the access is allowed only if \(L' \gg L\) and \(CS' \supseteq CS\)

Mandatory Access Control System vs Discretionary Access Control System
In the most common implementations of Discretionary Access Control, users "own" their directories and the files and programs they contain. They can grant and deny access and execution privileges for these to other users. Users can also be parts of groups. They may be able grant or restrict access to all members of a group. In Mandatory Access Control the operating system controls the ability of a subject or initiator to access or generally perform some sort of operation on an object or target. The object or target can be something like a process, a file, a directory, a program, or a memory segment. Subjects and objects each have a set of security attributes. Whenever a subject attempts to access an object, an authorization rule enforced by the operating system kernel compares these security attributes to the policy and decides whether the access or operation will be allowed. With mandatory access control, this security policy is centrally controlled by a security policy administrator; users do not have the ability to override the policy and, for example, grant access to files that would otherwise be restricted.

**No Write Down Policy** (In Mandatory Access Control System)
Suppose two files are edited as follows:
1. File1(Secret, Area51)
2. File2(Top Secret, JFK)
If these files are edited then output file be tagged as EditedFile(Top Secret, Area51 and JFK)
For access level, most restrictive level will be used and for compartments, all the compartments will be used. This is called "No Write Down Policy".