Authorization is the decisions by which one decides what an entity should be able to do once we authenticated what group they are in. This is done by giving **ACLs**: Access Control Lists.

1 | Principles of Authorization

1.1 | Separate privileges and have users request specific privileges

The more things someone has access to, the more opportunities they/someone have to attack the system. This is, of course a balance: if two privileges are often used together, maybe its appropriate to bundle them.

1.2 | If asking a human to authorize something, make it clear what they are requesting

If users don't understand what you are asking, they may end up just not doing what they want to do, or, worse, they may begin to turn off the security checks entirely.

1.3 | Check authentication and authorization

Its easy to remember to check at a begin of a system, but every time that a privileged action is needed, check both auths again just in case the user swapped/logged out.

1.4 | Be careful about ordering allow and deny detectives

The orderings of authorization directives matter. For instance, we could have permissions for "deny all, allow specific group", which is very different from "allow specific group, deny all".