# Access Control

## Table of contents



## 1 Access Control

Access control refers to the methods and policies used to restrict and manage who can view or use resources. Its about ensuring that only authorized individuals can access certain data, systems, or functions and preventing unauthorized access.

The key concepts of access control are identification, authentication, authorization, and accountability.

- Identification is the ability to attest to one's identity.
- Authentication is the confirmation of one's identity.
- Authorization is the specifying of access rights for resources.
- Accountability is the acknowledgement and assumption of responsibility for actions.

Access control needs to be enforced at various levels for different systems.

### 1.1 Access Control Models

There are four major access control models:

1. Discretionary Access Control (DAC) - In this model, every object in a system has an owner who can grant access to users as they see fit.
2. Mandatory Access Control (MAC) - With mandatory access control, access is granted as clearance. If a user is granted a certain level of clearance, then they have access to all objects available at that level of clearance. This is common in governmental contexts.
3. Role-Based Access Control (RBAC) - Role based access control involes granting access to resources based on the defined functions of the role that someone plays. For example, the instructors at a university have a different role than the students and can access information concerning individual students in ways that students cannot.
4. Attribute-Based Access Control (ABAC) - This model is dependent on attributes such as the time of day or the location of the users or resources. This model give the most control over who gets access to what.

## 2 Port Knocking

In networking, a port is a virtual endpoint that allows access to the machine. Each port is like a "channel" where a specific type of traffic is allowed. To access a port, you typically include the ip address and follow it with a colon, then the port. For example: `138.47.123.123:8000` would access port 8000. Ports are numbered from 0 to 65535.

Some ports are reserved for certain usage, for example if you're using your computer to host a website, you will use port 443 to deliver content over HTTPS and port 80 to deliver unsecured HTTP content.

Here is a list of some of the reserved ports and their usages:

- 20 - FTP (File Transfer)
- 21 - FTP (Control commands for file transfer)
- 22 - SSH (Secure Shell access)
- 25 - SMTP (Email)
- 143 - IMAP (Email)
- 80 - HTTP (Regular web traffic, not secure)
- 443 - HTTPS (Web traffic, secure)

"Knocking" on a port is the idea of briefly visiting a port to see if it is open, in the same way one might visit a door and knock on it to see if anyone is home. If a port is closed, then no one can get into the computer. Security wise, it is be great to keep all of the ports closed, however, if we want to remotely access a computer, this is simply not possible.

One way around this is through port knocking. Port knocking allows us to keep a port closed until a combination of other ports are visited. That is, trying to access certain ports in a certain order will result in the desired port becoming open for a brief amount of time. Note that this is basically security through obscurity, which should not be the security we count on.

More secure ways for keeping the machine safe would be through a symmetric key for a single port or through single packet authorization (SPA).

## 3 Single Packet Authorization

Single packet authorization (SPA) is a network security technique used to control access to available services. SPA works through the following simple process:

1. The client sends an SPA packet to the server.
2. The server checks the validity of the SPA packet. This can include checking an encryption key, the source ip address, a timestamp, and more.
3. If the SPA packet contains valid information, then the server grants access to the appropriate ports (for example, SSH) for the client's IP.
4. If invalid the server silently drops the packet and no feedback is given.

SPA is significantly more secure than Port Knocking since it is difficult to detect and involves an actual encryption key.