Application Security

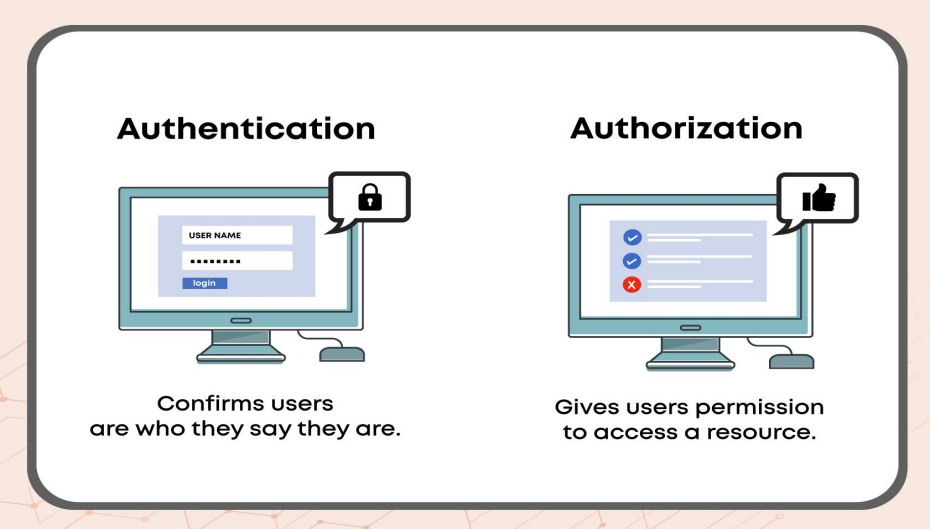
What is Application Security?

Application security is an application-level security measure that prevents the theft or hacking of application code and data. Application security can include hardware, software, and processes that identify or mitigate security vulnerabilities.

The main aspects of Application Security:

1. Authentication: Security Authentication is the process of confirming the user's credentials and identity. Operating systems typically identify/authenticate users using three methods: password, physical identification, and biometrics.
   Example: When we go to the airport, you are supposed to show some identity proof like an Adhar Card or Passport to enter inside the airport. This is an example of authentication.

2. Authorization: System security authentication is the process of giving a user access to a particular resource or feature. Authorization also signifies the system access control and user privileges in a secure environment, authorization should always follow certification.
   Example: Suppose you have written an essay in a google doc. You are the owner of the google doc but can grant access for editing, viewing or commenting as required. Simply, you can authorize other people to access the google doc. This is an authorisation.



Basic Authentication:

Basic authentication works by asking website visitors to enter their username and password. This method is widely used because it is supported by most browsers and web servers.

The advantages of basic authentication are:

1. Works through a proxy server.
2. Compatible with most internet browsers.
3. Allows users to access resources that are not on the IIS server.

Challenges of basic authentication are:

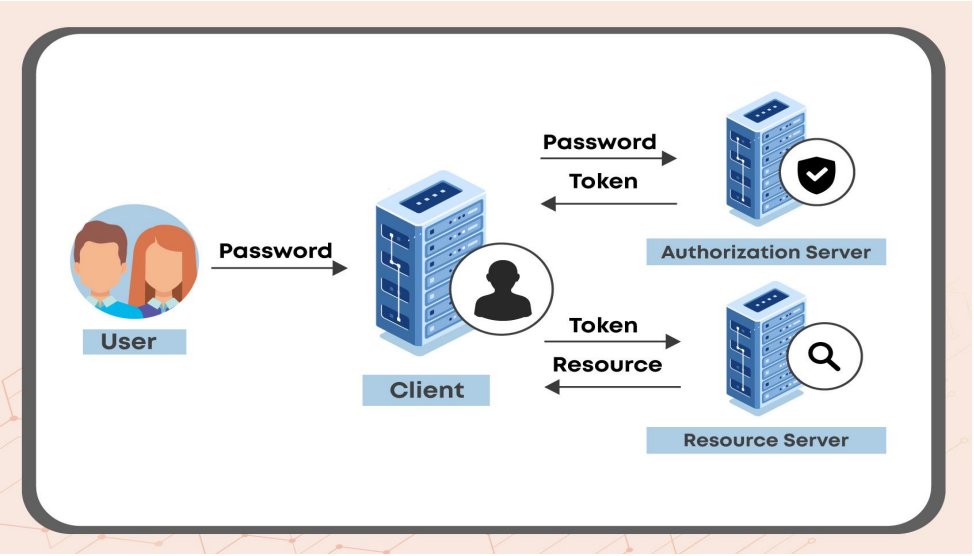
1. Information is sent over the network in cleartext. The information is encoded in base64 encoding but is sent in an unencoded format. Passwords sent with Basic authentication can be cracked easily.
2. By default, users must be able to log on locally to use Basic authentication.
3. Basic authentication is vulnerable to replay attacks.

Basic authentication does not encrypt user credentials, so traffic must always be sent over an encrypted SSL session. Users who authenticate with Basic Authentication must provide a valid username and password.

Token-Based Authentication/Access Token Based Authentication

Token-Based Authentication also known as Access token authentication is the process of validation and identity verification of the user. Other web authentication methods include biometrics and password authentication. Each authentication method is unique, but all methods fall into one of three categories: knowledge (what you know), inheritance (what you have), and possession (what you have).

Example: Bank Websites like ICICI Bank. Application expires if left idle for more time.



Password authentication falls under the category of Knowledge because users use previously created words and phrases to verify their identity. Biometrics is an example of "what you are" because it uses biological characteristics such as fingerprints. Finally, token-based authentication belongs in the owner category.

OAuth Authentication:

OAuth is an authentication protocol that allows the user to trust the application and interact with another without revealing the user's password. OAuth is an open standard authorization framework or protocol that provides "specified and secure access" functionality to your application.

For example, you can tell Facebook that ESPN.com can connect to your profile or post updates to your Timeline without having to specify your Facebook password on ESPN. This greatly reduces the risk. Your Facebook password will remain secure even if ESPN is compromised.