1. Security: The security is combination of authentication and authorization.

2. Authentication: It is checking identity of user.

3. Authorization: It is verifying the access permission on resources of a users.

Example Banking App:

================

* To get into Bank app app, the user must be authenticated.
* Based on role/desg of logged-in user the access permissions on the resources will be given or will be denied.

Ex: Customer role users can operate deposit,withdraw transactions.

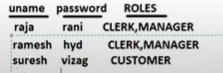
Clerk role users can operate deposit,withdraw, Loan transactions.

Manager role users can do all operations.

4. Important Components in Security Implementation:

=====================================

1. Security Realm /Authentication information Provider.
2. Authentication Manager.
   1. **Security Realm:-**In Application, the place(small file/small DB) where username,password and roles are maintained is called security realm or Authentication information provider.



Examples:

1. Xml file

2. Property file

3. DB s/w

4. LDAP(Leight weight Directory Access Protocol) server.

In xml file,Property file, and DB s/w we encrypt the password manually and if we forget password , we can get back the old password.

Where as in LDAP Server, Password is automatically encrypted. If we forget the password then we can not get old password and we can reset the password.

Tomcat server is giving support only for xml file by default.

Spring/spring boot security support all types authentication info providers.

* 1. **Authentication Manager:-**  It is component that performs both authentication and authorization activities by taking the security realm.

Move over , it gives error page with error number accordingly.

ErrorCode 401 : authentication Failed.

ErrorCode 403 : authorization Failed.

Types of Authentication Managers:

=======================

1. Programatic Auth Manager:- we need to develop the authentication manager manually to perform authentication and authorization activities.
2. Declarative Auth Manager:- By adding entries in .xml file, web application uses underlying server supplied ready made authentication manager to perform authentication and authorization activities.

The declarative Auth Manager can perform Authentication activities in four modes.

1. BASIC
2. DIGEST
3. FORM
4. CLIENT-CERT
5. Basic:-

-------

* Interanlly uses the base64 algorithm to encode the username and password in travelling(client machine –to-Server )
* Makes the browser to generate dialog box for collecting username, password from endusers.
* It is supported by all browsers.

b.DIGEST:-

---------------

* Same as BASIC , but uses MD5(Message Digestive) algorithm to encode and decode.

c.FORM:

----------

* Same as Basic but allows the programmer to design his choice form page for gathering credentials(username,password) from endusers.
* Also allows to cfg error pages of programmer choice for authentication and authorization failure.

d.CLIENT-CERT:

-----------------------

* It is not related to Authentication and authorization.
* It is all about configuring Digital certificates in server by enabling “https” protocol.. and bring those digital certificates at client side and using them for encoding and decoding activities.