Importance of Authentication in Cyber Security

By Isha Gaur

ABSTRACT

In the time when people are not satisfied with their own personality and try to place the mask of other person by capturing their identity, technology is also not spared from that. This human behavior is creating a tremendous number of security threats in the advancement of technology. Every great innovation and the fast development of the technology comes with the great threat and now a days capturing the unauthorized access is the major concern in the cyber security.

The purpose of this report is to discuss briefly about the importance of authentication in cyber security and cyber environment. We will also discuss about the types of authentication, technologies used for authentication, authentication protocols, explanation on OAuth in the security of a web application.

KEY WORDS

Authentication, Authorization, Passwords, OAuth, Tokens, Web application, Cyber security.

1. INTRODUCTION

Authentication is a process of declaring and proving the identity of the actual user. It is an important step in maintaining the security of a system, network or web application by confirming that the person who has applied for the access is the actual user or not. For confirming this access control systems are used to check the credentials of the user. The very first a user has to do for gaining the access of anything on cyber environment is to get himself authenticate by providing his correct credentials to the system.Credentials can be in the form of username, password, pin, cards, biometric etc. System will check his/her credentials by matching them in the system database or on the authentication server. After checking it validates the identity of the authentic users. If the credentials provided by the user do not match in the system database then it prohibits the user for allowing the access.

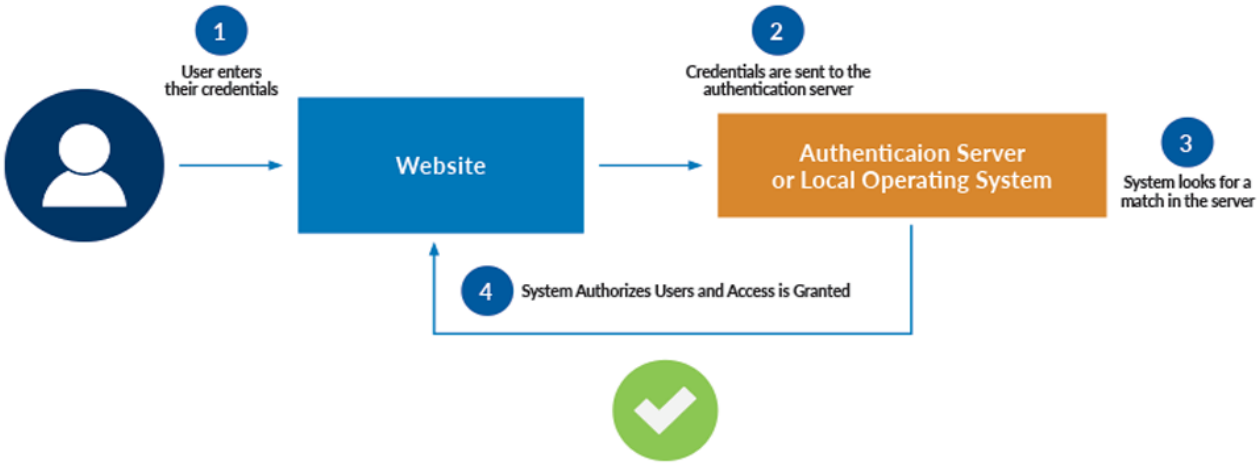

Figure1: Basic depiction of an Authentication process[1]

1.1 Key aspects of Authentication

[1] Available at https://www.tst.co.za/news/2019/3/1/understanding-user-authentication-3-basics-you-should-know

There are three main aspects of the authentication technology to enhanced the techniques of validating the authenticated user.

a. **What you have -** This contain the aspects that you have and by which you can do the process of authentication. For example smart cards, tokens,electronic cards,physical keys. This is something like a physical item. A smart card has the structure similar to the credit card which is attached with the certificate that identifies the person who is holding it and trying to get the access. That card holder has to insert the smart card into the card reader system for the authentication. Every smart card is associated with a pin with the technique of multi-factor authentication[2].A token which is widely used for authentication is a physical device which can be carried in hands. it is attached with a LED that shows a number. That number is validated by the authentication server.

b. **What you know -** This is the most factor used in authentication process. The information which a user uses to identify himself to get the access.This information can be password and personal identification number(PIN)[3]. User enters this information related to what he has with himself whether a smart card or a token.This is also something which has a high chance to get attacked first by the attacker to stole the authenticated user.They can be compromised very easily by social engineering.

c. **What you are -** This is related to something which is a part of human body. Biometric methods are covered into this factor. Biometric methods uses the user's finger prints, voice modules, eye's retina / iris ,palm geometry, hand prints and face recognition etc related to the human body to identify the user uniquely.This factor provides the best authentication because such things are only unique to the authenticated user's body and other can not copy that. But by technology advancement people are also trying to copy the finger prints or finding techniques to control the facial recognition systems. Still this the best in every security perspective.

2. Types of Authentication Methods

Authentication process in cyber security has a very high importance So the methods which are used in this process has to be very secure that the unauthorized person should not get

[2] Multi-factor authentication uses any two or more authentication factors. A key part of this is that the authentication factors must be in at least two of the categories..

[3] The Personal Identification Number (PIN) is created by the card holder and is never stored on the card itself. It is used to verify the user's identity at ATMs and other computer systems that can access the account at the issuer.Short for personal identification number, PIN is a set of personal numbers used to prove positive identification. It is often used with automated bank teller machines, telephone calling cards, and accessing Wireless networks. Available at https://www.sciencedirect.com/topics/computer-science/personal-identification-number

the access any how unless the whole system will face the consequence. There are few method mentioned below that are used in authentication :

2.1 **Password -** Passwords are the most commonly used method in authentication. Passwords are the simplest form for providing authenticity as compared to the other methods. The user needs to provide the password with respect to the users id , a smart card or a token.For maintaining the security in this method a user should use a strong password mechanism. A password is considered to be strong when it is an combination of alphabets (Upper and lower case), numbers and special characters. Many websites and organizations suggests to keep a long password. All these things increases the strength of a password. It is recommended not to keep any of the user's personal details like users name, date of birth or users id , also not to keep the word which are available commonly and can be find in dictionary.

2.2 **One Time Password (OTP) -** An one time password (OTP) technique is a method in which a password is generated only for one time which is valid for a certain restricted period of time. This OTP password can be a number or an alpha numeric value which is valid to login the session only for one time. Now a days OTPs are widely used to perform the financial transactions on a daily basis. There is one more use of OTP that is if a person forget/lost his or her password then he can use this method to validate himself and then he can change the password. SMS services are used to send the OTPs. For this user's phone number should be registered with the service provider so that service provider can send the OTP on the correct phone number. OTPs are considered as to be the most popular method for authentication in web based service to validate the user. The overall process of generating OTP for any financial transaction between a user and banking service, when a user initiated the transaction can be understand from the below figure 2.2.1.

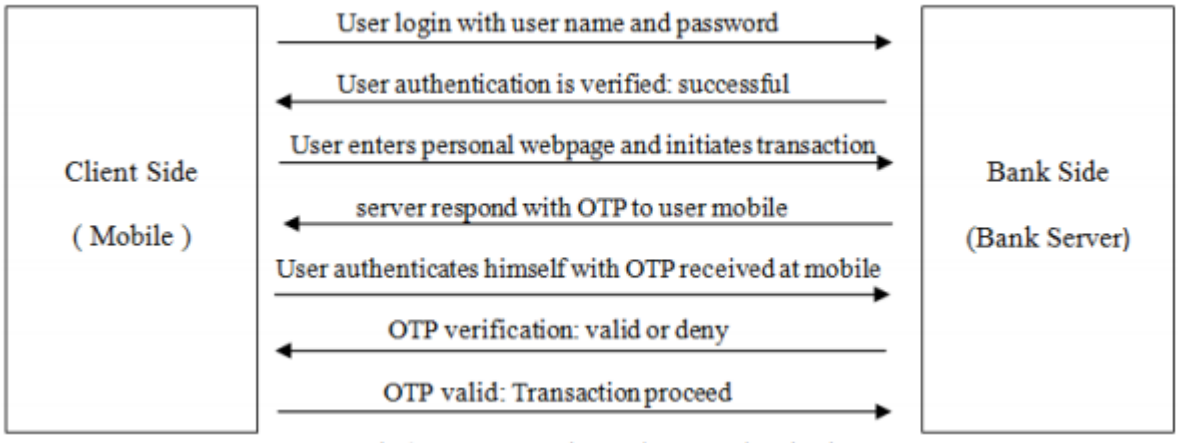

Figure 2: OTP generation and user authentication.

2.2.1 Techniques involve in generation of OTP

The method of generating OTP, Whenever a user start an procedure of authentication can be perform by the below techniques-

i. Time-synchronized OTP - In this an OTP is generated for a time period only after that it will get expire. In this case another OTP must be generated.

ii. Counter-synchronized OTP - There will be a counter synchronization between the server and client device.

An OTP can be delivered in two modes. One by text message service and other by email. This technique is very cost effective.

2.3 Biometrics- Biometrics technique is the best authentication technique with respect to the security parameters. It provides the higher level of secrecy to validate the user. It is based on the characteristics of identifying through the human body parts. There are two types of which uses biometrics, one which uses biometric as a single authenticating factor and other one is which uses biometrics as a second or third party system.

2.3.1 Types of Biometrics

a) Retina Scanner - This uses the retina pattern of a user's eye to scan and then identify.

b) Iris Scanning - In iris scanning biometrics system, a digital camera took photograph of the reflection from the cornea of the eye with the use of infrared light.

c) Finger Print Scanner- Human finger print patterns are the most reliable graphical patterns to recognize a person as they as unique and cannot change the whole life until and unless any accident occurs.

d) Facial Biometrics- These biometric systems use facial structure of the users to identify him/her. In this technique the gaps between the eyebrows, placing of nose, facial structure, shape of face, forehead pattern, width of nose and other facial elements are used to examine the uniqueness of the user.

e) Voice Recognition- It uses the voice modulation and pattern to recognize the user. Voice recognition programming is used in these types of biometrics. These biometrics records the contrast of voice in different moments and create a unique pattern to recognize it for identification.

f) Hand/Palm Print Pattern- The biometric which asks for your palm to scan for identification uses your hand line geometry. By scanning the geometry of palm lines makes the system to validate user.

2.4 API Authentication- An API authentication is a process when a server requests for the information of the user such as user ID and password from the client to validate from the database. HTTP basic authentication method, API keys and OAuth are used as a standard authentication methods. We are going to discuss the OAuth method in this paper.

3. Requirement of Authentication

The answer to the question that why should we use authentication is that authentication is required to prevent the data, system or web application from the attacks. An attacker can pretend to be a valid user to perform any sort of attack but if there is a barrier of authentication which is essential will help the system to stop the attacker to do so. An attacker may get to know your User ID but without entering the correct sequence of string i.e. a password he will not be allowed to get access of the system.

An attacker after capturing the identity of of valid user can

- Steal the confidential information of an organization
- Misuse the sensitive data of a user
- Perform financial transactions
- Stop the services of a product
- Defame the user
- Send false emails
- Corrupt the system etc.

4. Authentication Protocols -

We have gone through the various methods and the requirement of authentication, now we will discuss the various protocols used in the process of authentication.

4.1 **SSL/TLS -** The secure socket layer and transport layer security both are important protocols. TLS is a successor of SSL. Using these protocols, the client and server both authenticate each other using digital certificate before establishing the connection between each other. They exchange certificate to verify the authenticity. This protocol is built in most of the web browsers. It does not require software.

- **Working of SSL/TLS -** In SSL/TLS, the client and server initiated their communication by sharing their public keys this is known as TLS handshake[4].After

[4] A TLS handshake is the process that kicks off a communication session that uses TLS encryption. During a TLS handshake, the two communicating sides exchange messages to acknowledge each other, verify each other, establish the encryption algorithms they will use, and agree on session keys. Available at https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/

this both parties create their session keys. These sessions keys are used after the TLS handshake. Session keys are used for encryption and decryption. In each session different session keys are used after this the SSL/TLS make sure that both the communicating parties are the same who they claim to be.

4.2 **Kerberos -** This protocol was developed for checking the authentication of UNIX networks. Now a days Kerberos is used in windows authentication as a default authentication mechanism. This is also used in MAC OS and Linux also. It depends upon tickets which are the temporary security certificate used to authenticate the client and server over an unsecured network.

- **Working of Kerberos** - A user sends a ticket request to KDC, which sends an encrypted ticket to the user by encrypting it with the password of the user. The user then decrypts the ticket with his password. The authentication of the user is now validated if he successfully decrypts the ticket with his password.

4.3 **OAuth -** This is known as Open Authorization. It is an open standard which is used to grand the access of a website or an application to access their data and service without providing them the password. This protocol is based on the token-based authentication[5] and authorization[6] .

5. What is OAuth

In which paper we will briefly discuss about OAuth. The OAuth is an example of the better management of identity, confidentiality and privacy of users on internet. OAuth version 1.0 was published in April 2010 and after two years its latest version has be been released in October 2012. By using the OAuth framework, a primary website can allow the user to share its photographs or other such content to a third party[7] web application to use the permitted content. OAuth is a secure mechanism for authorizing the third party application without showing the user's credentials. Many big organizations like Facebook, Amazon, Google, Microsoft and Twitter allows its users to share information of their account with the third party web applications.

[5] Authentication determines the user's identity to grant access to the system.

[6] Authorization determines whether the particular user is authorized to access the resources.

[7] A third-party application is created by a developer that isn't the manufacturer of the device the app runs on or the owner of the website that offers it.

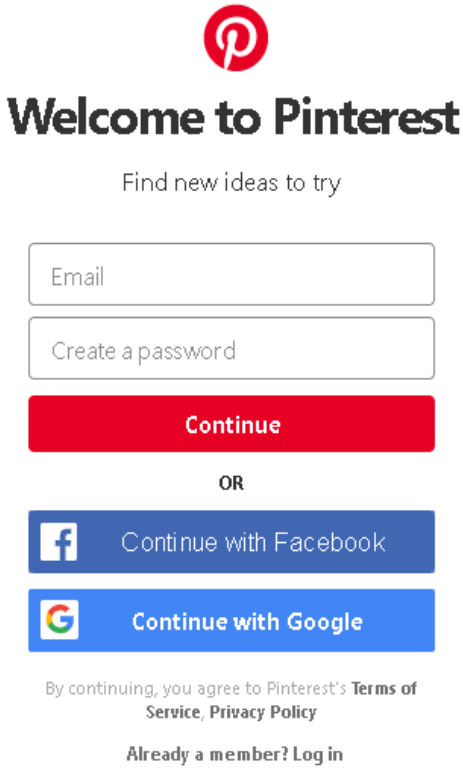

Figure 3: Website using OAuth

5.1 Features of OAuth

5.1.1 Delegate Access - In earlier version of OAuth the third party applications required the user credentials to access the social site on behalf of the users which is highly insecure. But now with OAuth2.0 Access Tokens[8] are used in place of user credentials.

5.1.2 Selective Access - OAuth2.0 gives an access control to the users that a user can make decision on the information that which website can use which data and for how much time period.

[8] Access tokens are the thing that applications use to make API requests on behalf of a user. The access token represents the authorization of a specific application to access specific parts of a user's data..

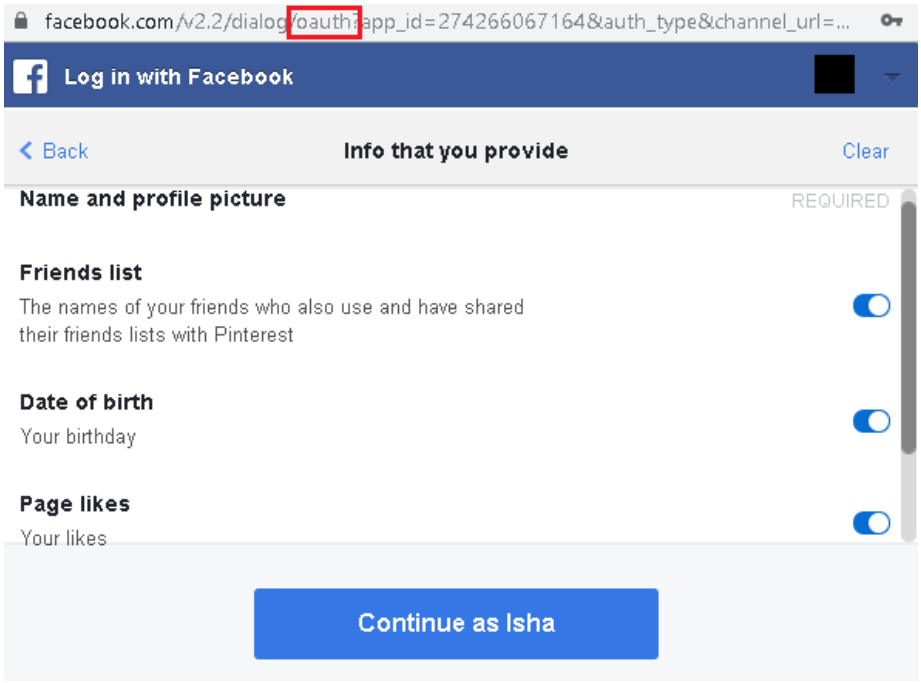

Figure 4: OAuth Selective Access

5.1.3 Access Tokens - They are used on behalf of user's credential to make an api request. They are generated randomly.They have replaced the passwords mechanism to provide better security.

5.1.4 Revoke Access - At any time user has the control to revoke the access permission which he gave to the third party application. In case of lost or stolen mobile devices this gives the security to the personal information to the user.

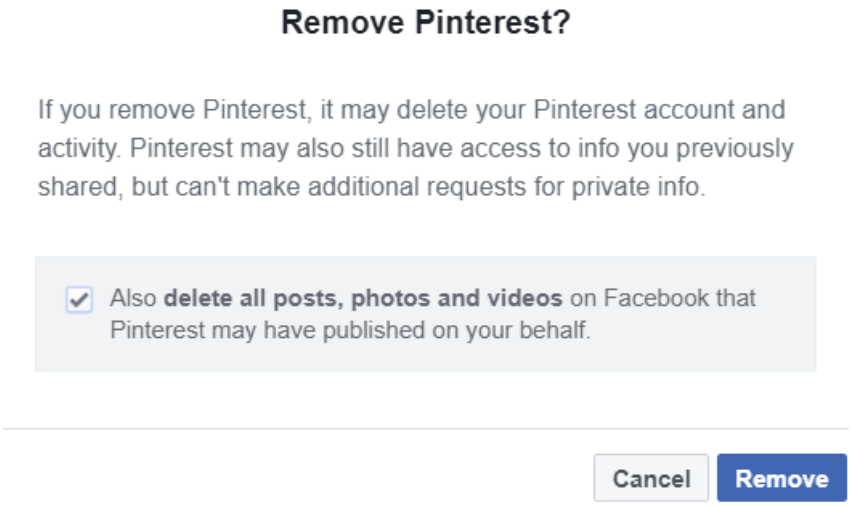

Figure 5: Revocation of Access token

5.1.5 Better Security - The standard model OAuth 2.0 transfers the data on the SSL to ensure the security on the basis of cryptographic protocols to secure the data.

5.2 Protocol Flow of OAuth

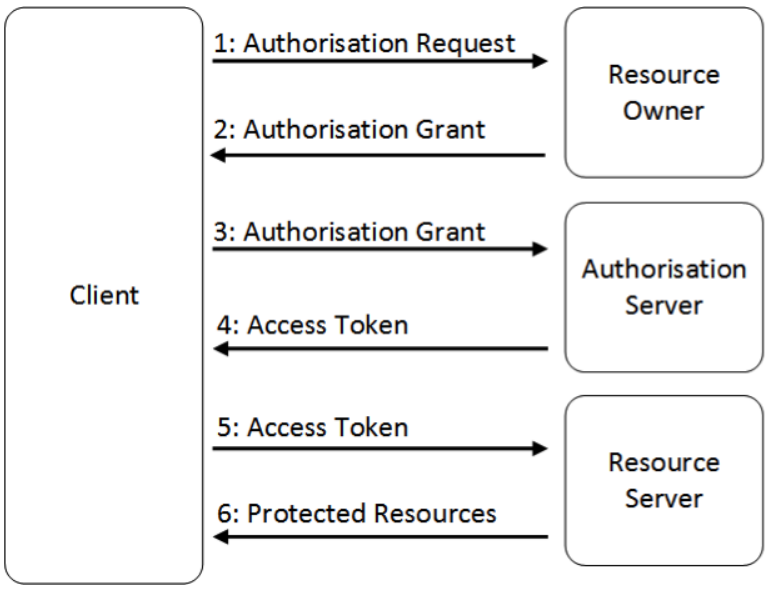

Figure 6: Protocol flow of OAuth[9]

a) The client directly makes the authorization request to the resource owner.

b) The resource owner the give the grant to the client. It depends on which method the client is using for requesting the authorization and the type which authorization sever is using.

c) The access token is requested by the client by providing the authorization grant which the client received from the resource owner.

d) By validating the authorization grant, the authorization server[10] validates the client. If the user gets validated from the server then it issues the access token to the valid client.

e) Now the client requests for the resources from the resource server[11] and authenticate himself by providing the access token.

[9] Available at https://www.researchgate.net/figure/OAuth-20-Protocol-Flow_fig1_290478841 Accessed on 2019-08-28

[10] Authorization sever is responsible for authenticating user's identity and gives an authorization token. This token is accepted by resource server and validate your identity.

f) If the resource server finds the access token valid then it provides the resources to the client.

5.3 Advantages of using OAuth

a) This protocol is easier to implement and also flexible as it relies on SSL.

b) It provides the stronger authentication.

c) A limited access is given to the user's data.

d) To make sure the security of data it uses the cryptographic protocols.

5.4 Disadvantages of using OAuth

a) If your primary website gets hacked then it may lead to the insecurity to the other third party websites.

b) If you want to increase the number of specifications for giving the access to the third party then it can create interoperable problems in implementation So you need to write the code for the website.

6. Conclusion and suggestions

Every system on the network is under the threat of being compromised. Most of the attacks are performed by initiation of the unauthenticated access on the system or on the web application. This is being done with the bad intentions. The strong authentication mechanism brings the feasibility of accessing the data as well as the security to the whole system. Authentication is very important whether for an organization, a system, application or for the website. Some authentication methods are easy to implement like password but somewhere they have fear of being compromised by the means of getting them or by social engineering. Some are very reliable and strong mechanisms like Biometrics but they are very costly to implement. Now a days there is a very effective technique of OTP is getting popular. It is very secure as well as easy to implement. It has brought revolutionary changes in the day to day transactions system and bring the new era of authentication.

The selection of authentication technique has the most important role in building the security of the data on the internet as well as on the physical devices. The authentication methods increase the security to make the system so that it can work effectively without the fear of not being able to dissolve the attack by the unauthenticated user. The user should use strong passwords with big length. Passwords should be change on the weekly basis.

[11] Resource server store user's data and http services which can return user data to authenticated clients.

7. References

- Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005
- Network Security: History, Importance, and Future?, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.
- Data Communication and Networking by Behrouz.A.Forouzan 4th edition
- San-Tsai Sun , “Simple But Not Secure: An Empirical Security Analysis of OAuth 2.0-Based Single Sign-On Systems” , http://blogs.ubc.ca/computersecurity/files/2012/04/San-Tsai.pdf
- Barry Leiba, " OAuth Web Authorization Protocol ", www.computer.org/internet computing, Vol. 16, No. 1. January/February, 2012
- http://www.iosrjournals.org/iosr-jce/papers/conf.15013/Volume%207/1.%2001-06.pdf?id=7556
- https://www.ijcsmc.com/docs/papers/May2015/V4I5201599a46.pdf
- https://www.oauth.com/oauth2-servers/differences-between-oauth-1-2/
- https://www.oauth.com/oauth2-servers/access-tokens