ISSN No:-2456-2165

Mobile Based Secure Authentication using TLS and Offline OTP

Abhishek Vijay Phalke, Bhagyshri S.Bhutawale
Institute and business management studies karjat

Abstract:- World Wide Web hosts (e.g. Yahoo, Gmail, etc.) deploy the best known security mechanisms to protect user important data from hackers. A large number of user they access their own account.Security purpose hacker are hacked their account but important that how to protect their account from hacker.

Still the personal information is compromised. Security lapse is at the user data, i.e. user's personal faults is responsible for the onslaughts. Accessing the web server is different. Every hacker attemptsadvance access to user's system to steal data. So in this paper, enhanced Authentication schema to maintain secure data and try to protect for the hacker also maintain confidentiality of information is proposed.

The purpose of the framework is to save pre-shared phone number and MAC address from the device current timestamp(PMT),required to also generate TOTP(Time-base One Time Password) which in turn will generate an offline secret hash code by using offline Token generation mobile app. Security Token based runtime interaction could extends the strength or authentication control.

When generated hash code is entered the user request in the website is transferred to the server using TLS.

Connection is established between servers or user system goes away with the usage for SMS based OTP applications which are strung-out on the cellular net.

Keyword:- *OTP,TLS, Authentication, attack, IMEI.*

I. INTRODUCTION

Data sharing and storing over cloud network using internet is becoming a movement. There is an increasing needfor securing the data over the internet. In order to keep data in the web as safe as possible, more clients and servers implements cryptographic techniques to encrypt sensitive data, as well as verify entities at the other end of the connection.

Use of smart phone has increased in the recent years. Mostly people like to exchange data over the internet using smart phones. Smartphone based on web applications developedprovide ease of access to the users. Hacking the web application servers is also complicated as compared to getting access to the user system in parliamentary procedure tosteal data. Hence, attacks attack normally happen at the user terminal device. The major goal of net security is to prevent unauthorized access to data and resources. Various cryptographic techniques are applied by clients and servers to keep the confidentiality of data.

Authentication is the heart of every security model. Every user wants secure Authentication with the server and also to maintain security so they do not lost message integrity. Authentication It is the process to confirm the user's identity (or a machine), attempting to gain access to a system or resource. Password based authentication is the most often utilized and trusted authentication mechanism. Because password are unique to every person but in the password also contain special symbol. There is lesser chance to hack their account. User needs to insert the required login credentials (username and password), to acquire access to a resource or computer, the supplied credentials are then matched against a database which contains the list of all authorized users and their passwords. Your email id and password are unique and when user is login they create unique session and when logout their account they session expired the session. Many advances have been suggested for proper strategies of securing and using passwords. The user is suggested to maintain strong passwords, however number of problems persists in password based authentication. Do not share your unique password with anyonee.g.: (friend, employee etc.). A better technique which overcomes the shortcomings of password authentication technique is known as multi-factor authentication. Multi-factor technique is considered to be much secure as it adds up extra layer(s) of protection over password authentication technique.

II. OVERVIEW OF EXISTING METHODOLOGIES AUTHENTICATION

Multifactor authentication has been introduced into the current scope of the project. Two factor authentication proposed in, the knowledge component is the email and the pin is sent to the registered electronic mail with the corresponding user account. An authentication scheme proposed in is using biometrics as one of the key elements for authentication. Granting to the suggested approach in the password is represented using a graphical icon, which is beamed from the service providers to the user on the mobile device and the user has to point appropriate points to insert the word.

ISSN No:-2456-2165

Biometric information required for recognition is called feature, and features appearing in fingerprints are especially called minutia. The minutia is divided into two types of ending and bifurcation. Ending refers to the place where the flow of ridges is cut, and bifurcation is the place where two ridges become one ridge. One fingerprint image has more than one ending and bifurcation.

A user is authenticated by using the place of this ending and bifurcation. Compared to the other user authentication methods, this user authentication method using users' physical characteristics has strong security.

However, the user authentication method using users' physical characteristics has critical security vulnerability such as the user authentication key cannot be changed. The fingerprint, or iris, and so forth are said to be users' own information but the user authentication key must be able to be changed because when leaked, all the authentication systems using all of their biometric information are hopeless. In authentication based on SMS, a random value is generated which is termed as OTP, is sent to the user registered mobile number by service providers through an SMS. Which is then submitted by the user for authentication; this is a widely used multi-factor authentication scheme. Every person has unique mobile number they already register with their email id. Proposed generating location based OTPs and encryption schemes. This One Time Password generated those who have register mobile number. Another person cannot access your own account.

Another suggested approach for multi-factor authentication is using Secure ID [10]. It utilizes a security device which generates an OTP which is then provided by the user along with other credentials for authentication. Each device uses a unique seed to generate OTP and the seed is also stored in the server's database in order to validate the OTP sent by the user. The device is timely synchronized with the host. Although the technique holds the benefit over SMS based authentication as it is free and worldwide accessible, but it will be really costly and infeasible for free service providers like Facebook.

The OTPs can also be generated by sharing the seed between both the communicating parties. if third person cannot access this OTP because its unique. On every successful login the seed is regenerated. d. Use of IMEI and IMSI numbers as the seed to generate OTPs is proposed in.the IMEI number is unique for each mobile it help to track current location of user and their mobile phone when its lost.

Time based OTP generation is proposed in but this technique is most usually employed for generating SMS based OTPs. Usage of TLS to exchange the seed for the generation of TOTP is proposed in.

If the OTP is sent to email of the user and the intruder hijacked the user email account, then he can easily generate and use OTPs to access the services pretending to be an authentic user if the intruder knows the user login credentials as well. This report gives an authentication framework which is more secure and trusted as compared to other systems. It utilizes the device hardware address, i.e. MAC address (something user possesses like a smart card) and number (pre-shared with the server) along with the current time (PMT) to authenticate the user. Compared to SMS based authentication schemes the technique uniquely authenticates the user using pre-shared MAC and number which helps in eliminating the dependency on other networks (like cellular networks in case of SMS based OTP scheme) to send the OTP. Hence, extra cost for sending OTP through SMS using additional network is reduced. If in some way the intruder gets physical access to the user registered number for SMS based OTP services, then he can easily get the OTP through SMS in SMS based approach. If the intruder intercepts the OTP message, then he may use the OTP to access the services before the user does. PMT mitigates the defects of SMS based multi-factor authentication system. A similar technique using the GPS location along with pre-shared number and timestamp is proposed in [14] to authenticate users. It will increase the communication overhead as each time the user logs in, the GPS coordinates need to be calculated and sent to the server side and the server fetch the user GPS coordinates information from GPS server and hence increasing the load on the server too. The GPS positioning of the user can easily be followed by the intruder as well as it will compromise the user's "DO NOT TRACK" feature. Also the intruders can social-engineer the user to get the pre-shared number. The location based OTP generation schemes possess the same problem. All the location based techniques are based on GPS coordinates which requires internet connectivity to the mobile device as well as in order to generate the OTP.

III. PROPOSED FRAMEWORK

T. The technique can substitute the existing SMS based authentication due to its security characteristics. Pre-shared number and hardware address helps in identifying the authenticity of the user and verification of the device used by the user. The device and number are registered with the server during the user registration phase. At the time of enrollment, a user is also commanded to select an image and a security question which is stored on the host. The number can be modified by the user anytime, but the hardware address is required to be identical. The multi-factor PMT authentication technique involves three phases: the first phase uses an older method of using username and password for authentication. In the second phase hash is calculated. Finally, in the third phase the authenticating party (server) verifies the hash sent to it by the PMT app. The notations used to describe the proposed work area:

ISSN No:-2456-2165

Notation	Description
Di	The device on which PMT app is installed by the user
Ws	Web-Server
Ts	Token-server
Uid	User unique id registered with the server
Pwd	User password registered with UID
Itu	Identity Token generated at User side
Its	Identity Token generated at Server side
Topt	Time Based OTP
MCAu	Mac address of the Di
Pno	The number registered with WS to corresponding UID
CRT	Current Time
H	One way hash function
Hu	Hash (one-time identity token) generated by the application
Hs	Hash (one-time identity token) generated by TS

Table 1. Notation Description

A. Phase Log-in using the password

In this phase, single user perform a main role enter the web page URL of the website need to gain access using any internet enable device.it is not necessary to a people stand in public and private place and access the internet they stands anywhere and access internet to access login e. The requested webpage server sends the authentication page to the user on which he needs to enter the login credentials (UID and PW) this is the unique for each user. The hash of entered credentials is sent to WS for verification. If the hash of credentials sent by user to WS is successfully verified, then the user is asked to provide ITU by WS.

B. Phase Generation of ITU and ITS

ITU is generated by the PMT app installed on the Di. The identity token ITU is generated using an equation:
ITU = hash (hash (Pre-shared number ⊕ Pre-shared MAC) ⊕ TOTP); (1). The TOTP is automatically generated by the application using CRT entered by the user which is displayed as a result of an ITU request by WS. Concurrently the current time used to generate TOTP is also sent to server by establishing a TLS connection between the user web accessing device and WS. The seed used to generate TOTP is changed every time the user logs-in to PMT application and the seed needs to be renewed after every 7days.

C. Phase Verification of Identity Token

ITU entered by the user is sent to WS using TLS connection. TS sends WS to ITS. If both ITU and ITS matches, the user successfully passed the authentication procedure and allowed to access the services offered by WS. To important if match data between ITU and ITS. When verification is done with identified by token also check to secure connection between client and server. Because this phase try to protect from the user and establish secure connection.

- *Algorithm 1: First time application registration with Tsinstalled Di*

It is used to exchange user device information and seed required for generation of TOTP,to generate and identity tokan.it is need exchange information for authentication purpose and see entire details. A TLS connection is establish between client and server for secure information exchanged. If information is exchange a hacker are confused and didn't know which user data information are exchanged and what is password of this user.it is less chance to hack the account from hacker. A user is required to log-in using tradition method, enters the username and password which are verified by the token server when user login their account they generate the unique token. Along with a user id and password hardware address of the device, i.e. MAC address is sent which is stored by token server. The token server generates a seed for generation of TOTP and stores it in the database and sends the seed to device too using TLS a token .A every time device ask user registration phone number with web server and PIN required to access application. Every time user access the application generate unique pin and ask the registered mobile number.

Step 1: User needs to login into the application using required credentials.

Step 2: TLS connection is established between the application and TS. A confirm the TLS connection and the session key is sent to an application by TS.

Step3: A seed generation request is generated and send to TS by application. The parameters of the request, i.e. login credentials along with MACU are encrypted and send to TS for verification

Encrypt [data = H (UID ⊕ PW); MACU; cipher= AES256CBC]

Step4: The server decrypts the data.

Decrypt [key=session key; cipher=AES256CBC; data=seed request

Step5: TS verifies the credentials of the user, stores the MACU in the database corresponding to UID and a unique 32-bit seed is generated for the user account.

Step6: The server uses the same TLS connection to send seed to the application. Encrypt [key = session key; cipher = AES256CBC; data = seed]

ISSN No:-2456-2165

Step7: PMT application decrypts the seed Decrypt [key = session key; cipher=AES256CBC; data = encryptedseed]

Step8: Application requires the user to enter PNO registered with the server and a PIN for opening the application to prevent unauthorized use.

Step9: Application generates a 32-bit hash string using MACU and PNO. HU= H (MACU ⊕PN)

Step10: Application encrypts HU and seed and stores them

When registration is successful of the device with server token, application is ready to generate one time identity offline without using mobile and internet connectivity. User is required update with server token after every week.TLS session need to exchange information is valid only for some time.to maintain specific time of session for user and server.

- *Algorithm 2: Generation of OTP offline at client side*

When successful registrations of application with token server the application to ready for generating one time token. A generate token user need to enter PIN required for open the application and request the application to generate identity token. This PIN is common for the specific user. If pin are send to user register mobile number. The user is then asked for the current time displayed on the PC when the web server requests PC to provide identity token. When user provide the current time displayed in the application,it is decrypt seeds and hash phone number and MAC address. Using seed and current time application generates a 32-bit TOTP and computes a 32-bit identity token, i.e. hash of user MAC and phone number hash and TOTP.

Step1: User opens the application in Di and enters a PIN to gain access to application services.

Step2: User requests the application for ITU generation

Step3: User needs to enter the CRT displayed on the device using which the user is communicating with WS in the application

Step4: Application decrypts the seed and HU.

Step5: Using seed and provided CRT a 32-bit TOTP (random number) is generated

Step6: The application generates a 32-bit token ITU by using HU and TOTP. ITU=H (HU⊕Totp)

After complete this step identity token is successfully generated and displayed to the user. The identity token valid specific period of time

- *Algorithm 3: Generation of OTP at server side*

When user register the application first time with token server its store generated seed by it and sent application in database and ask the web server to provide the register mobile phone number corresponding user and computer one way 32 bit using MAC and phone number store in to database. If a web server request t user for the token current time is sent by pc to the web server using TLS connection. The current time to provide to server its generate 32 bit TOTP seed store in database and database maintain all record to user and server and current time provide web server. The identity token for the user is generated by computing one way 32 bit hash of generating TOTP and hash of user MAC and phone number stored in a database of token server registered with the corresponding user.

Step1: During first time registration of application with TS, it stores the MACU of Di acquired from application and the generated seed associated with UID in the database.

Step2: After seed generation TS asks the WS for PNO registered with the UID.

Step3: TS generates a 32-bit hash string using MACU and PNO and store it in a database. HS= H (MACU⊕Pno)

Step4: When a user requires using the services provided by WS, an identity token request is sent by WS to the user. The user device asking to access the service displays and transmits CRT to WS using TLS

Encrypt [data = CRT; cipher = AES256CBC; key = session key]

Step5: WS decrypts CRT and transmits the decrypted CRT to TS. Decrypt [cipher=AES256CBC; data = EncryptedCRT; key = session key]

Setp6: TS extract seed and HS from the database associated with the UID.

Step7: Using seed and provided CRT a 32-bir TOTP (random number) is generated.

Step8: Then TS generates a 32-bit token ITS by using HS and TOTP. IDs=H (HS⊕ TOTP)

After this step identity token for the user is successfully generated at the token server without communicating directly with the client and thus ensuring security as the requests for token generation comes through the web server. The token server only communicates with the application and web server directly.

- *Algorithm 4: Verification of identity token*

After identity token is successful generated for the user at both end user and server they generated token both side and each and unique token generated. User need to provide generated token to the web server which sent to web browser through TLS connection. The web server matches both the tokens provided by the user and token server.

ISSN No:-2456-2165

Step1: User enters the ITU generated by the application.

Step2: User transmits ITU using TLS to WS. Encrypt [data = ITU; cipher = AES256CBC; key = session key]

Step3: WS decrypts CTR and transmits the decrypted CTR to TS. Decrypt [cipher=AES256CBC; data = EncryptedITU; key = session key]

Step4: WS requests TS to send ITS.

Step5: If ITU=ITS, the UID is allowed to access services provided by WS else denied.

If both token are match,then user is treated as authentic user and allow to access web server provided by web server and service denied to user and session with user is terminated.

IV. CONCLUSION

The framework uses the pre-shared number and MAC address of the device along with TOTP to.

Generate a hash known as the one-time identity token to successfully authenticate the user.

Attempting to access the services offered by the network host. Unlike SMS and location based.

Multi-factor authentication schemes, it does not require network services to transmit or to generate.

The OTP for authenticating the user. It never transmits the pre-shared number and the MAC address.

Of the device during the token generation process. MAC is only shared once through the channel at.

The time of application registration on token server, thus making the intruder difficult to guess and.

The number can also be modified by the user. The technique can easily be implemented in a vast.

Number of applications involving multi-factor authentication security. In future, the factors.

Required to identify and authenticate the device and user can be improved to enhance the security.
Level

REFERENCES

[1]. B. Ross, C. Jackson, N. Miyake, D. Boneh, J.C. Mitchell, "Stronger password authentication using browser extensions."Proceedings of the 14th Usenix Security Symposium. 2005.
[2]. L. Lamport, “Password authentication with insecure communication.” Communications of the ACM, pp. 770-772.1981.Vishal Gangwar, Ravishanker, Dr. Ashish and Kr. Luhach**5262.**
[3]. Bauckman, Dena, Terry, Nigel, Paul, Johnson, David, Joseph, Robertson, “Multi-Factor Authentication.” U.S. PatentNo. 20,130,055,368. 28 Feb. 2013.
[4]. Weber, Frank, “Multi-factor authentication.” U.S. Patent No.7, 770, 002, 3 Aug. 2010.