ANDROID SECURITY MECHANISM USING PRE-SHARED NUMBER, GPS LOCATION AND TIME SLICE

Vaibhav Kamble[1], Nupoor Deshpande[2], Omkar Patil[3], Ankush Pawar[4]

[1] *Student, Computer Engineering, Dilkap Research institute of engineering & Management, Maharashtra, India*
[2] *Student, Computer Engineering, Dilkap Research institute of engineering & Management, Maharashtra, India*
[3] *Student, Computer Engineering, Dilkap Research institute of engineering & Management, Maharashtra, India*
[4] *Professor, Computer Engineering, Dilkap Research institute of engineering & Management, Maharashtra, India*

ABSTRACT

Many web accounts are getting hacked everyday even though the public web servers like Gmail, Yahoo and Hotmail utilizes the well-known security techniques. However, attacks usually happen due to personal faults such as users do use a password or PIN that can be easily determined or bypassed, such as 1234 or 0000, birth date, name, mobile number. Traditional authentication system involves the use of a secret key or password of which user must memorize and recall during authentication, however due to user's careless, password can be forgotten or read by someone or simply intercepted during communication. Many approaches have been proposed for proper strategies of securing and using passwords. However, this can only reduce the problem of a static password authentication to some certain degree as it still has a lot of shortcomings. So we are proposing Multi-factor authentication to be an improved authentication scheme to overcome personal faults. It increases security by generating a secret hash code using a pre-shared number and user's current GPS location.

Keyword : - *GPS, hashing algorithm, multi-factor authentication, web security.*

1. INTRODUCTION

Now a days, various application servers like GMAIL, FACEBOOK has been secured due to security mechanisms so that it is difficult for attacker to hack such type of systems, as attacks normally happens from the user end.

Authentication is a process by which a system checks the identity of a user who wishes to access it.

- Existing system involves login id and password of a user, which user must memorize for login purpose.
- Due to user personal fault such as pswrd can be read by someone or simply shared during communication.
- Multi-factor authentication is proposed to be an improved authentication scheme using three factors: preshared number, GPS, time slice.

- An approach of multi-factor authentication is widely used in SMS based authentication, where a One Time Password is randomly generated and then sent to the user's mobile phone through an SMS message.

- Another proposed method is SecureID which is based on a security device.

- Each device has a unique seed used to generate a pseudo-random number (One Time Password) used to authenticate the user along with his other credentials.

- The device is timely synchronized with the server and its seed is also loaded into the server in order to validate the sent OTP.

- This approach has an advantage over the SMS based as it is free and worldwide accessible.

- A new mobile-based multi-factor authentication scheme is based on a pre-shared number, GPS location and Time slice (PGT).

- Multi-factor authentication is proposed to be an improved authentication scheme using three factors: preshared number, GPS location, Time slice.

2. LITERATURE REVIEW

Many approaches have been proposed for securing password, Weber and Frank proposed authentication by using PIN sent to Email as a knowledge factor of two factor authentication [2]. Bhargav and Abhilasha proposed a method by using Biometrics as the additional factor of authentication [4]. Sabzevar, Allreza and Angelos three of them stated a method of using a graphical method to represent a password in such a way that the password is entered by pointing on appropriate points of an image which the user receives through his portable device such as mobile phone running Android OS from the service providers [3].Another group of researchers Liou, Jing, and Sujith proposed a method identical to SecureID called SofToken that produces a pseudo-random number as an OTP based on seed shared between the authentication server and the user device [1].

3. EXISTING SYSTEM

Existing system for providing security to any data includes generating One Time Password (OTP); a normal password provided himself by the user, or a key generated automatically by encryption algorithms. These have become some of the traditional methods which makes it easy for a hacker to hack a profile or any data. These traditional methods require some changes, to make the security check more effective. One Time Password (OTP) are used to check that the registered user is genuine or fake. For all these reasons of security concerns we are building this application which would have a different way of generating a new password each time we login. This would have a lot more advantages than the existing way of security checks.

4. PROPOSED SYSTEM

This paper presents a new mobile-based multi-factor authentication scheme based on a pre-shared number, GPS location and Time slice (PGT). Unlike SMS based multifactor authentication, PGT does not have any additional cost for SMS. Compared to SecureID, PGT is considered to be more secure as SecureID is based on a fixed seed while PGT is based on a modifiable pre-shared number.

Moreover, PGT uses GPS location as an extra security parameter; PGT is also cost-free as it does not require a specific security device like SecureID. This makes PGT more secure and less expensive to be adopted. A bit similar work has been proposed before. It uses IMEI and IMSI numbers as the seed to generate the OTP. However, IMEI number is not very safe as it is already known to the mobile service provider; also IMSI is a cellular network identifier which makes the method not valid worldwide. Also their mechanism does not incorporate GPS location as a security parameter.

Steps:

1. User request for a required URL.

2. To open a site firstly users have to register on register page.

3. After registration request for login page.

4. During the process of login one code will be send to user mobile through OTP as shown in Fig 1.

5. Enter that code on login page. If user enters code correctly, then login will be successful else it will again return to login page.

6. User will get token (T1) if and only if login gets successful which he has to enter in the token block of requested URL.

7.

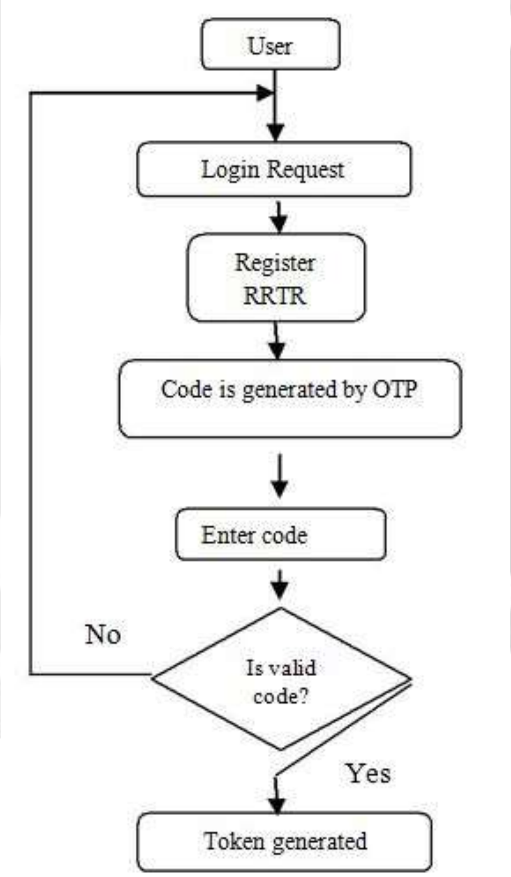

Fig -1: Flowchart for OTP

4.1 PGT System

This section discusses the steps involved in PGT multifactor authentication scheme. PGT requires a GPS server to synchronize the current GPS location of the user with the authentication server.

It also requires a pre-shared number between the authentication server and the user's mobile device to be set during registration and can be reset whenever it is necessary.

Three stages are involved in PGT multi-factor authentication (Fig 3) the first stage authenticates the user using the traditional method (username/password). In the second stage, the security token is generated. Finally the third stage verifies the given token by the authentication server.

Stage 1: Traditional Log in

In this stage, the user requests his personal web page URL through any Internet enabled device D1. The web portal server S1 has to respond back to D1 with the authentication page asking the user to provide his traditional credentials (username/password). The user provides his credentials to D1 which sends them to S1 for verification. If the user is verified, S1 asks for the security token.

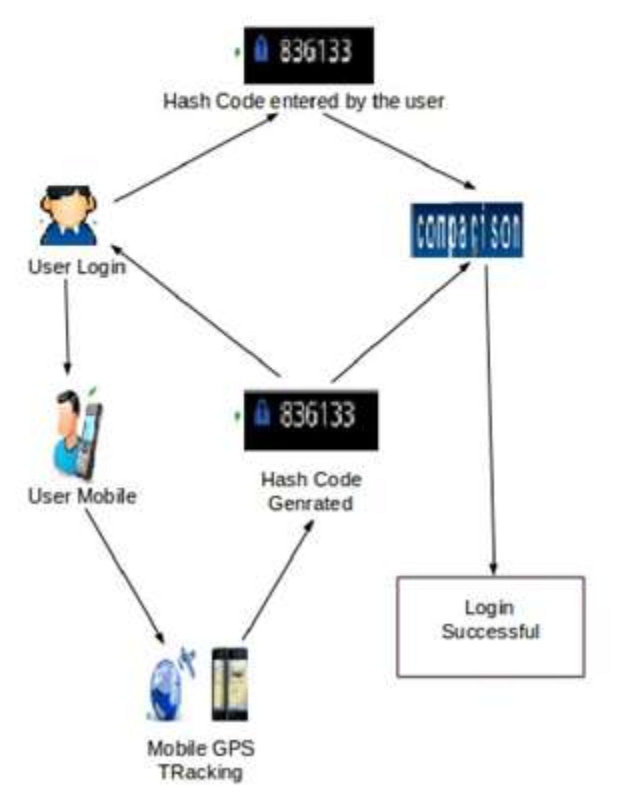

Fig -2: PGT System

Stage 2: Generation of Token T1

The PGT phone app is installed on the user mobile device D2 (GPS enabled), this app is responsible for generating the security token T1 according to the following equation where TS1 is the current time slice:

T1=hash (Pre-Shared Number + GPS + TS1);

At the same time D2 updates the GPS server (S2) with the user's GPS location and time slice (TS1) through a secured channel.

Stage 3: Verification of Token

S1 receives the security token *T1* and gets the GPS updates and time slice of the corresponding user from S2. Following that, it generates a security token T2 using equation (1). Then it compares *T1* with *T2* (Fig. 3), if they match, the user is authenticated and his personal web page is sent back to D1.

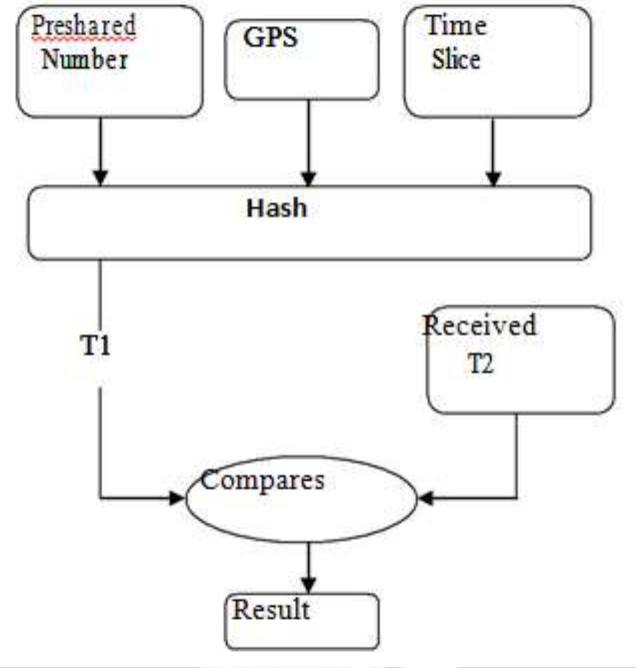

Fig -3: Token Verification

This section discusses various threats to the PGT multifactor authentication scheme and how it0 can thwart them:

Scenario 1: An intruder gains access to the user system and obtain information about his username/password. Here, the intruder would not be able to log in to the server as he does not have the enough information to generate the PGT token.

Scenario 2: An intruder obtained information about user's username/password and he was also able to intercept the communication between the Android Phone and the authentication server to capture the sent token. With the token being made to get expired either by time (let's say 60 sec) or by use (valid to be used for one time), the intruder won't be able to use the captured token even within its time limit as it has already under use by the user.

Scenario 3: The intruder has the user's fixed username/password and assuming that he was able to know the user's current GPS location. Still he cannot generate a valid/correct token as he does not hold the preshared number. The pre-shared number has never been transmitted over any channel during authentication. Thus, as far as the hash function is a one-way function, there is no way for the intruder to get the pre-shared number out of a sniffed token.

Scenario 4: An intruder has stolen the user's mobile phone and has already obtained the user's fixed username/password. For this scenario we made the PGT Android phone app as a PIN protected app. Thus the intruder would not be able to use the app as far as he does not possess its PIN.

Scenario 5: If the user has lost his Android mobile then he can no longer access his web page. To encounter this issue, PGT should provide an option to pre-register an alternative mobile device or backup mobile number that can be used in this case.

4. CONCLUSION

Multi-factor authentication utilizes the user's mobile device to generate an OTP. PGT uses a pre-shared number that is not transmitted through any channel and also makes it very difficult for the intruder to guess. Hence system becomes more secure.

5. REFERENCES

[1]. Perrig, Adrina. "Shortcomings of Password-Based Authentication" (2000).

[2]. Lamport, Leslie. "Password authentication with insecure communication"Communications of the ACM 24.11 (1981).

[3]. Ross, Blake, et al. "Stronger password authentication using browser extensions" Proceedings of the 14th Usenix Security Symposium. Vol.1998. 2005.

[4]. Nystrom, M. "The SecurID (r) SASL Mechanism", 2000.

[5]. Bauckman, Dena Terry, Nigel Paul Johnson, and David Joseph Robertson. "Multi-Factor Authentication" U.S.

[6]. Dispensa, Steven. "Multi factor authentication" U.S. Patent Application 11/862,173.

[7]. Weber, Frank. "Multi-factor authentication" U.S. Patent No. 7,770,002. 3 Aug. 2010.

[8]. Bhargav Spantzel, Abhilasha, et al. "Privacy preserving multifactor authentication with biometrics." Journal of Computer Security 15.5 (2007).

[9]. Sabzevar, Alireza Pirayesh, and Angelos Stavrou. "Universal multi-factor authentication using graphical passwords." Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on. IEEE, 2008.

[10]. Aloul, Fadi, Syed Zahidi, and Wassim El-Hajj. "Two factor authentication using mobile phones." Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on. IEEE, 2009