International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Secure OTP Algorithm using Smartphone Application – Proposed Approach

Sonal N. Pannase[1], P. R. Pardhi[2]

[1]Student, M. Tech., Department of Computer Science and Engineering,
Shri Ramdeobaba College of Engineering and Management, Nagpur, M.H., India

[2]Professor, Department of Computer Science and Engineering,
Shri Ramdeobaba College of Engineering and Management, Nagpur, M.H., India

Abstract: ***OTP is considered as one of the most powerful authentication methods among several authentication protocols. But it has some security vulnerabilities. Like an unauthorized user could know a valid OTP value and be authenticated with this secret information. A secure OTP algorithm has been proposed to solve this type of problem. The proposed algorithm uses the IMSI number for registration of the user and captcha image along with OTP to it secure against MITM attack and MITPC/Phone attack.***

Keywords: OTP, Smartphone, Application, Authentication, Algorithm

1. Introduction

A user Authentication is a method to prove that whether a certain user is authorized to use a network source. There are different Authentication Methods such as follows.

1.1. Knowledge Based Authentication:

Knowledge-based authentication is a method of authentication which seeks to prove the identity of someone accessing a service. It requires the knowledge of private information of the individual to prove that the person providing the identity information is the owner of the identity.

1.2. Ownership Based Authentication:

Ownership Based Authentication relies on Something the user has e.g., wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token.

1.3. Attribute Based Authentication:

It is the inherence factor, something the user is or does e.g., fingerprint, retinal pattern, DNA sequence, signature, face, voice, unique bio-electric signals, or other biometric identifier.

1.4. Two Factor Authentication (TFA):

Knowledge Based Authentication is the most widely used Authentication method, in which ID/PASSWORD is used mostly. But PASSWORD is Vulnerable to *Brute Force Attack i.e.* as User keeps the password easy to memorize, therefore they can be cracked using trial and error method. This can be overcome with Two Factor Authentication (TFA). For TFA, OTP protocol is used widely along with user ID/PASSWORD.

1.5. One Time Password (OTP)

One-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication.

2. OTP Authentication Methods

2.1. Time Synchronization

A server and a Client are synchronized with time. In this method, a server and a client are synchronized with time after they share a secret key. When a user wants to be authenticated by the server, each of them uses the shared secret key and the time information to make an OTP value. When the client makes and sends OTP value to the server, the server makes OTP value by utilizing the same algorithm used in the client side and checks whether two OTP values are the same or not. If the two OTP values are the same, then the user can be successfully authenticated. The overall process is shown in Fig. 1.

Figure 1: Time Synchronization Authentication

2.2 Challenge Response Authentication

A Server authenticates user using Challenge values. A server and a client share a secret key prior to authentication. When a user wants to be authenticated, the server generates a

challenge value and sends it to the client. The server and the client then generate the OTP values at the same time by utilizing the same algorithm as an input of the challenge value and the shared secret key. The overall process is shown in Fig. 2.

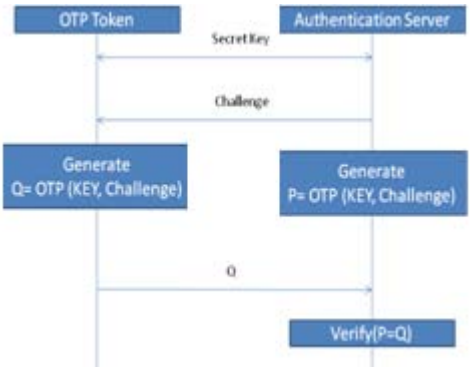

Figure 2: Challenge Response Authentication

2.3 S/Key Authentication

A S/Key authentication makes OTP values by using a hash function. The authentication process is as follows. First, a server and a client share a secret key. The shared secret key then becomes an input value to the hash function. The server and the client generate first hash value by using this secret key. The first hash value becomes an input value to second hash function. The algorithm repeats this procedure for N times. In the client side, the N hash values are stored in the client storage while the server just stores last Nth hash value. When the user tries to be authenticated, he sends (N-1)th hash value to the server. Then the server generates hash value with the received (N-1)th hash value. The server checks whether the Nth hash value which has been stored in the server side is the same as the generated hash value. If the authentication is successful, the server stores (N-1)th hash value and deletes the previous Nth hash value. And then he sends to the client a message indicating the client is successfully authenticated. When the user tries mth authentication, the client sends (N-m)th hash value among the N hash values stored in the client side. Then the server generates a hash value with the received hash value. The server checks whether the (N-(m- 1))th hash value which has been stored in server side is the same as the generated hash value. If two values are the same, the server stores the received hash value and deletes the previous (N-(m-1))th hash value. Then, the server sends to the client a message indicating the authentication is successful. If m equals to N, the server and client should initialize the process. The overall process is shown in Fig. 3.

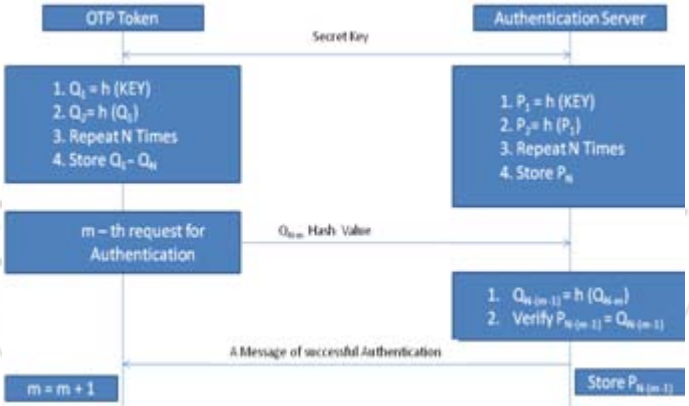

Figure 3: S/Key Authenticataion

2.4 Event Synchronization:

In event synchronization, a server and a client share a secret key and a count value in an initialization process. The count value is the number of the authentication. When a user wants to be authenticated, the client increases the count by 1 and generates OTP value with the count value and the shared secret key. The client sends the generated OTP value to the server thereafter. The server increases the count by 1 and generates an OTP value. Then he checks whether the received OTP value and generated OTP value are the same or not. The overall process is shown in Fig. 4.

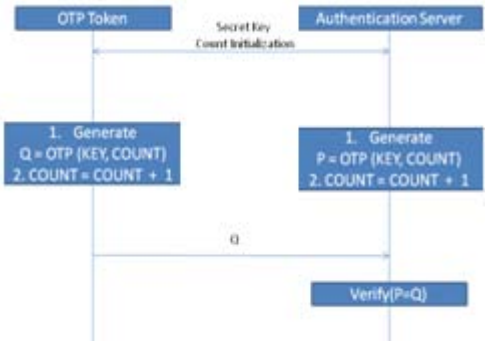

Figure 4: Event Synchronization Authentication

3. Threats to Present OTP System

OTP is especially vulnerable to MIT – X (Man - in – the – X) Attack:

3.1 MITM (Man in the Middle) Attack

An adversary can sit on Access Path/ Access channel pretend the receiver that he is authorized sender or he can pretend the server that he is the authorized user or receiver.

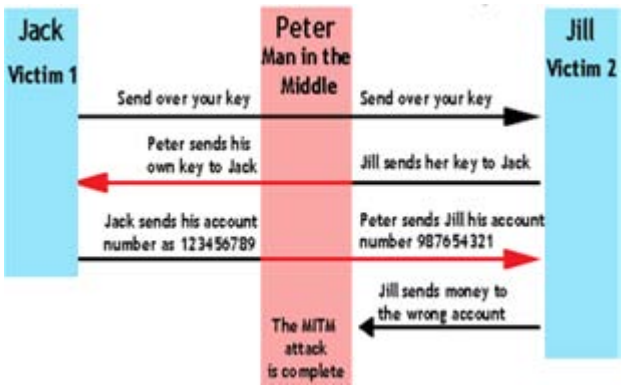

Figure 5: An example of Man in the Middle Attack

3.2 MITPC/Phone (Man in the PC/Phone) Attack

The desktop component of the MITPC/Phone attack requests victim‟s phone number and notifies them that a link for downloading the security application has been sent via SMS to their mobile device. Users are directed to install the fake application from this link and enter the activation code provided by the malware. Once installed, the mobile malware captures all SMS traffic, including transaction authorization codes sent by the bank to the victim, and forwards them to the fraudsters. This enables the criminals to initiate fraudulent transfers and capture the security codes.

4. Literature Review

A user authentication is a process to prove that whether a certain user is authorized to use a target service or system. There are various user authentication methods such as knowledge-based authentication, ownership-based authentication and attribute-based authentication. Among them, knowledge-based authentication is widely used these days, such as ID/PASSWORD in most websites or services. However, the password is maybe predictable because it should be easy for users to memorize. Thus, an adversary could get the passwords of users by brute-force attack in a short period of time. A Two-Factor Authentication (TFA) can be used as a countermeasure to this weakness. Especially, OTP (One Time Password) protocol is the most widely used for TFA with user‟s ID/PASSWORD [1].

4.1. In 2012, Hoyul Choi, Hyunsoo Kwon, Junbeom Hur, have presented a paper “A Secure OTP Algorithm using Smartphone application” [1]. In this paper, authors have proposed, An OTP Algorithm which uses Captcha Image, IMSI number, Limited Time availability to make it secure against Man in the Middle and Man in the Phone Attacks, using Smartphone Application.

4.2. In 2014, Dr. Ananthi Sheshashayee, D. Sumathy, have presented a paper “OTP Encryption Techniques in Mobiles for Authentication and Transaction Security” [2]. In this paper, authors have proposed Two Factor Authentication using PIN (Personal identification Number) and OTP (One Time Password. In 2013, Ms. Kalaikavitha, Mrs. Juliana Gnanaselvi, have presented a paper “Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology”. In this paper, the approach of using AES (Advanced Encryption Standard) Algorithm for Encrypting OTP has been proposed.

4.3. In 2010, Li Yinxiang, Lizhi Zhong presented paper titled “Research on S/Key One Time Password Authentication System” in which they propose the use of HASH function for generating OTP [4].

5. Proposed Architecture & Approach

5.1. IMSI Number

The **International Mobile Subscriber Identity** is used to identify the user of a cellular network. It is a unique identification associated with all cellular networks. To prevent eavesdroppers identifying and tracking the subscriber on the radio interface, the IMSI is sent as rarely as possible. An IMSI is usually presented as a 15 digit number, but can be shorter (14 digits). The first 3 digits are the Mobile Country code (MCC), which are followed by the Mobile Network Code (MNC), either 2 digits or 3 digits. The remaining digits are the Mobiles Subscription Identification Number (MSIN) within the network's customer base.

5.2. Proposed Algorithm

As OTP is vulnerable to Man in the Middle and Man in the Phone/ PC attacks. Ann efficient Challenge Response Authentication Methods has been proposed in the following Methodology:

5.2.1. An Authentication Server shares secret key with user's mobile application. IMSI number stored in user's Smartphone SIM card is used as the secret key.

5.2.2. When the server is requested to authenticate the user, the server generates a challenge value and delivers it to the user.

5.2.3. The user generates an OTP value using this challenge value and shared secret key.

5.2.4. Server also generates the OTP using same algorithm as in Client side.

5.2.5. Client sends the OTP value to the Server.

5.2.6. Server Compares the Received value with its own generated one. If both the values match, Authentication is Successful.

Fig. 5 shows the proposed architecture.

Figure 6: Proposed Architecture

5.3 Authenticating the User (OCRA: OATH Challenge Response Algorithm)

5.3.1 Authentication Server

Server sends a challenge value C to the user.

5.3.2 Mobile Application

- Generates OTP (P) using (Secret Key, C) using OCRA
- Sends the OTP (P) to Server

5.3.3 Authentication Server

- Also Generates OTP (Q) using (Secret Key, C) using OCRA
- Verifies P = Q
  - If „Yes" Authentication Successful
  - If „No" Authentication Fail

5.4 Server Database

The server database contains two tables one stores the user details and the other stores the captcha images to be sent to the user for authentication.

5.5 Mobile Application

Figure 7: An example of User Interface

6. Conclusion

As OTP authentication is generally used in Two Factor Authentication with ID/PASSWORD, but the PASSWORD authentication has some vulnerabilities like passwords are vulnerable to brute force attack. Also the OTP authentication is vulnerable to Man in the Middle and Man in the Phone/PC attack. The proposed scheme is secure against these attacks as it uses IMSI number as its secret key, which is stored in the SIM card and not in the memory.

References

[1] Hoyul Choi, Hyunsoo Kwon, Junbeom Hur, A Secure OTP algorithm using Smartphone Application, IEEE, 2015
[2] Dr. Ananthi Sheshashayee, D. Sumathy, OTP Encryption Techniques in Mobiles for Authentication and Transaction Security, 2014
[3] Ms. Kalaikavitha, Mrs. Juliana Gnanaselvi, Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology, 2013
[4] Li Yinxiang, Lizhi Zhong, Research on S/Key One Time Password Authentication Sysytem, Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on IEEE, 2010
[5] D.M'Raihi, J.Rydell,"OCRA: OATH Challenge-Response Algorithm", Internet Engineering Task Force RFC 6287, 2011
[6] Mohammad Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram Khan, OTP Based Two Factor Authentication Using mobile Phones, 2011Eight International Conference on Information Technology: New Generations, IEEE
[7] Derek L.Davis, Lionel smith, Authentication System Based on Periodic Challenge/Response Portocol, United states Patent, 2000
[8] Charles Fredrick AUSTIN, Xingsheng WAN, Two Factor Authentication, United states Patent, 2014, N – Dimension Solutions INC.