International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 2 Issue 3, March 2015

ISSN: 2394-4404

Secure Protocol Based Verification And Authentication For An Virtual Reality Environment

N. Saravanan
PG Scholar,
Prist University, Thanjavur, India

Dr. G. J. Joycemary
Asst Professor,
Prist University, Thanjavur, India

***Abstract:** In a user authentication protocol which involves user's cell phone and short message service to prevent password stealing and reuse attacks. Reusing passwords across different web sites may cause users to lose their information which is stored in web sites once the password hacked or compromised by attacker. Second, hackers can install malicious software to get the passwords, when user typing their username and password into unknown public computers. In this paper, developing web based security analysis of one Time password authentication schemes using mobile application. OPass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through OPass, users only need to remember a long-term password for login on all websites. After evaluating the OPass prototype, we believe OPass is efficient and affordable compared with the conventional web authentication mechanisms*

***Keywords:** LTP, STP, SOAP, Triple DES algorithm*

I. INTRODUCTION

Over the past few decades, text password has been adopted as the primary mean of user authentication for websites. People select their username and text passwords when registering accounts on a website. In order to log into the website successfully, users must recall the selected passwords. Generally, password-based user authentication can resist brute force and dictionary attacks if users select strong passwords to provide sufficient entropy. However, password-based user authentication has a major problem that humans are not experts in memorizing text strings. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might be unsafe. Another crucial problem is that users tend to reuse passwords across various websites.

A. ONE-TIME PASSWORD

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords they are not vulnerable to replay attacks This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology in order to work.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security token that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using a channel such as messaging (SMS). Finally, in some systems, OTPs are printed on paper that the user is required to carry.

a. MOBILE PHONES

A mobile phone keeps costs low because a large customer-base already owns a mobile phone for purposes other than generating OTPs. The computing power and storage required for OTPs is usually insignificant compared to that which modern camera-phones and smart phones typically use. Mobile phones additionally support any number of tokens within one installation of the application, allowing a user the ability to authenticate to multiple resources from one device. This solution also provides model-specific applications to the user's mobile phone. However, a cell phone used as a token can be lost, damaged, or stolen.

Figure 1: Mobile Phone

B. SCOPE

To develop web based security analysis of one Time password authentication schemes using mobile application.

C. PROBLEM DEFINITION

Text password is the most popular form of user authentication on websites due to its convenience and simplicity. However, users' passwords are prone to be stolen and compromised under different threats and vulnerabilities. Firstly, users often select weak passwords and reuse the same passwords across different websites. Routinely reusing passwords causes a domino effect; when an adversary compromises one password, she will exploit it to gain access to more websites. Second, typing passwords into untreated computers suffers password thief threat. An adversary can launch several password stealing attacks to snatch passwords, such as phishing, key loggers and malware**.** Smart-card-based password authentication is one of the most commonly used security mechanisms to determine the identity of a remote client, who must hold a valid smart card and the corresponding password to carry out a successful authentication with the server.

A user authentication protocol which involves user's cell phone and short message service to prevent password stealing and reuse attacks. Reusing passwords across different web sites may cause users to lose their information which is stored in web sites once the password hacked or compromised by attacker. Second, hackers can install malicious software to get the passwords, when user typing their username and password into unknown public computers. In this paper, developing web based security analysis of one Time password authentication schemes using mobile application. OPass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through OPass, users only need to remember a long-term password for login on all websites. After evaluating the OPass prototype, we believe OPass is efficient and affordable compared with the conventional web authentication mechanisms

II. REPRESENTATION OF OPASS STRUCTRUE

The representation of the OPASS is the conceptual design that defines the structure and/or behavior and more views of the system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system which comprises system components, the externally visible properties of those components, the relationships between them, and provides a plan from which products can be produced, and systems developed, that will work together to implement the overall system.

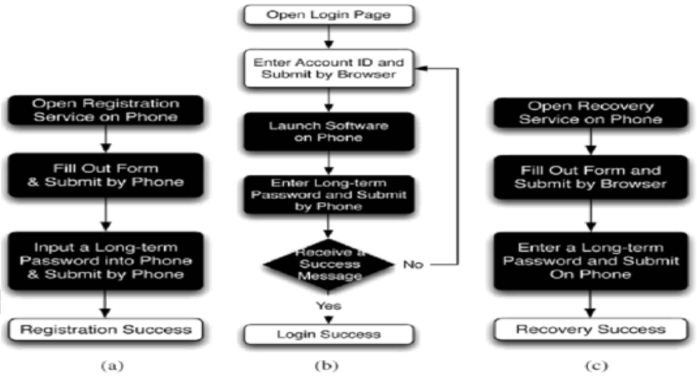
Open Registration Service on Phone
Fill Out Form & Submit by Phone
Input a Long-term Password into Phone & Submit by Phone
Registration Success
(a)
Open Login Page
Enter Account ID and Submit by Browser
Launch Software on Phone
Enter Long-term Password and Submit by Phone
Receive a Success Message
No
Yes
Login Success
(b)
Open Recovery Service on Phone
Fill Out Form and Submit by Browser
Enter a Long-term Password and Submit On Phone
Recovery Success
(c)

Figure 2: Representation of OPASS

III. MODULES DESIGN

A. LONG TERM PASSWORD GENERATION:

In our project, the long term password created by user. That is, in registration process the long term password given by user that stored in web server with encrypted format.

- ✓ We open a particular website from which we want to get the web services.
- ✓ New user has to register their personal details by entering into the new user mode.
- ✓ Now it will open the Registration Form. User has to fill up everything and submit.
- ✓ It will be stored on the Temporary table in server's database.

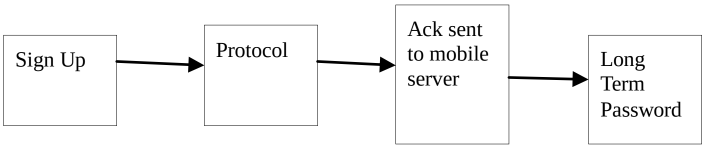

Figure 3: Long Term Password Generation

B. EMAIL VALIDATION & VERIFICATION

During registration process the email validation and verification will be processes. That is, first it checks our entered email id is valid or not. That time we use validation process. After validation we can verify that email for whether it is right or not. Instantly match email addresses to known dead domain names, malicious email addresses, and common typographical errors in email address submissions

- ✓ The server will generate Mobile and E-mail verification codes (OTP-One Time Passwords).
- ✓ These verification codes (OTPs) will be sent to the corresponding Mobile (through SMS) and Mail-ID.
- ✓ After getting these verification codes (OTPs), we should enter these codes in another webpage when registration which is called as OTP verification.
- ✓ Waiting for Accessing page will be in processing mode.

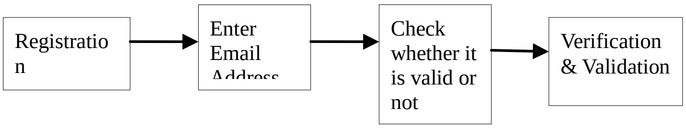

Figure 4: Email Validation & Verification

C. USER AUTHENTICATION

Online customers must have access to a computer and a method of payment. In our System, the user interactions are login, registration, communication, online payments and Transaction. User details are handled in backend common database.

In computer security, a login or logon is the process by which individual access to a Computer system is controlled by identifying and authenticating the user referring to Credentials presented by the user.

A user can log in to a system to obtain access and can then log out or log off when the access is no longer needed. To log out is to close off one's access to a computer system after having previously logged in.

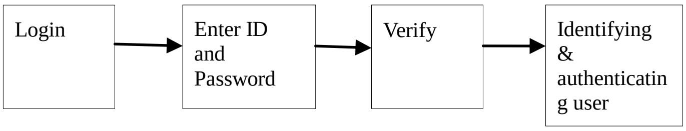

Figure 5: User Authentication

D. OTP ENCRYPTION

The main security for our system is one time password authentication. The one time Password created in web application and send to android application.

One-time pad (OTP) is a type of encryption which has been proven to be impossible to crack if used correctly. Each bit or character from the plaintext is encrypted by a modular addition with a bit or character from a secret random key (or pad) of the same length as the plaintext, resulting in a cipher text. If the key is truly random, as large as or greater than the plaintext, never reused in whole or part, and kept secret, the cipher text will be impossible to decrypt or break without knowing the key to use Triple DES algorithm for one time password encryption. This algorithm not only used for password encryptions but also used for use details encryptions.

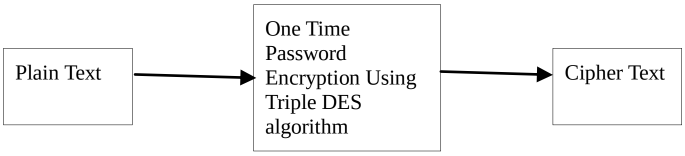

Figure 6: OTP Encryption

E. ANDROID APPLICATION LOGIN PROCESS

In Android application, a login is the process by which individual access to a mobile application is controlled by identifying and authenticating the user referring to credentials presented by the user.

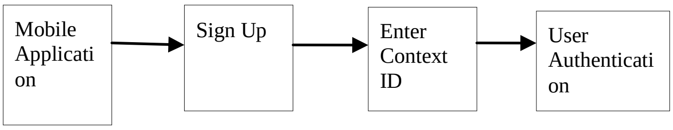

Figure 7: Android Application Login Process

F. OTP DECRYPTION

The One time password decryption process done in android application using same Triple DES algorithm and same key of encryption

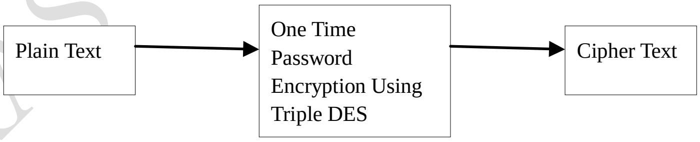

Figure 8: OTP DECRYPTION

G. OTP VALIDATION

Once the user got a onetime password in android application from mobile application That password entered to web application. In web application, the onetime password comparison is processes. That is compare sending OTP to user enterer OTP. If the comparison is true then it will go to application otherwise redirect to login page.

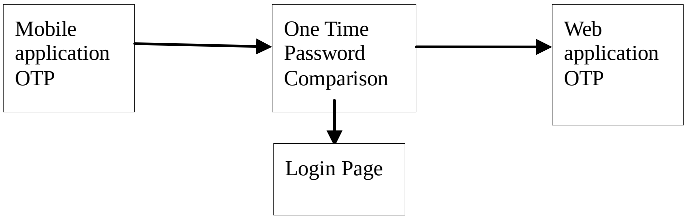

Figure 9: OTP Validation

H. APPLICATION MAINTENANCE

Application maintenance is a daunting task for enterprises. They are under pressure to Reduce spends on maintenance. While ensuring optimized performance of their IT systems and applications. Final module of our project as application maintenance. That is, to maintain our application with more and more security. Such as PIN code evaluation and OPASS verification

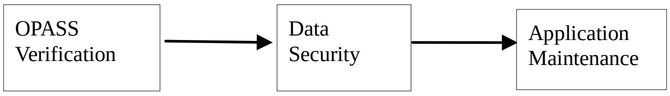

Figure 10: Application Maintenance

IV. CONCLUSION

The author of this paper proposed a user authentication protocol named OPass which leverages cell phones and SMS to thwart password stealing and password reuse attacks. We assume that each website possesses a unique phone number. We also assume that a telecommunication service provider participates in the registration and recovery phases. The design principle of OPass is to eliminate the negative influence of human factors as much as possible.

Through OPass, each user only needs to remember a long-term password which has been used to protect her cell phone. Users are free from typing any passwords into untreated computers for login on all websites. Compared with previous schemes, OPass is the first user authentication protocol to prevent password stealing (i.e., phishing, key logger, and malware) and password reuse attacks simultaneously. The reason is that oPass adopts the one-time password approach to ensure independence between each login.

REFERENCES

[1] K.-K.R. Choo, C. Boyd, and Y. Hitchcock, ‘‘The Importance of Proofs of Security for Key Establishment Protocols: Formal Analysis of Jan-Chen, Yang-Shen-Shieh, Kim-Huh-Hwang-Lee, Lin-Sun-Hwang, Yeh-Sun Protocols,’’ Comput. Commun., vol. 29, no. 15, pp. 2788-2797, Sept. 2006.

[2] H. Chien, J. Jan, and Y. Tseng, ‘‘An Efficient and Practical Solution to Remote Authentication: Smart Card,’’ Comput. Security, vol. 21, no. 4, pp. 372-375, Aug. 2002.

[3] T.F. Cheng, J.S. Lee, and C.C. Chang, ‘‘Security Enhancement of an IC-Card-Based Remote Login Mechanism,’’ Comput. Netw., vol. 51, no. 9, pp. 2280-2287, June 2007.

[4] C.-I. Fan, Y.-C. Chan, and Z.-K. Zhang, ‘‘Robust Remote Authentication Scheme with Smart Cards,’’ Comput. Security, vol. 24, no. 8, pp. 619-628, Nov. 2005.

[5] J.Hu, D. Gingrich, and A. Sentosa, ‘‘A k-NearestNeighbor Approach for User Authentication Through Biometric Keystroke Dynamics,’’ in Proc. IEEE ICC Conf., Beijing, China, May 2008, pp. 1556-1560.

[6] C.L. Hsu, ‘‘Security of Chien et al.’s Remote User Authentication Scheme Using Smart Cards,’’ Comput. Stand. Interfaces, vol. 26, no. 3, pp. 167-169, May 2004.

[7] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R.H. Deng, ‘‘A Generic Framework for Three-Factor Authentication: Preserving Security And Privacy in Distributed Systems,’’ IEEE Trans.Parallel Distrib. Syst., vol. 22, no. 8, pp. 1390-1397, Aug. 2011.

[8] W.S. Juang, S.T. Chen, and H.T. Liaw, ‘‘Robust and Efficient Password Authenticated Key Agreement Using Smart Cards,’’ IEEE Trans. Ind. Electron., vol. 55, no. 6, pp. 2551-2556, June 2008.

[9] W.C. Ku and S.M. Chen, ‘‘Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards,’’ IEEE Trans. Consum. Electron., vol. 50, no. 1, pp. 204-207, Feb. 2004.

[10] P.C. Kocher, J. Jaffe, and B. Jun, ‘‘Differential Power Analysis,’’ in Proc. Adv. CRYPTO, vol. LNCS 1666, M.J. Wiener, Ed., 1999, vol. LNCS 1666, pp. 388-397.