International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Web Based Security & Authentication Using Opass Mobile Application

Nikhil Ramrao Bhuktar, Mahesh D Ghodke
Department of Computer Engineering
SKN college of Engineering
Pune, India

Harsh Vaibhav, Swapnil P Kothawade
Department of Computer Engineering
SKN College of Engineering
Pune, India

***Abstract*— In this paper, we design a user authentication protocol named oPass which leverages a user's cellphone and short message service to thwart password stealing and password reuse attacks. 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—web security; user authentication; password stealing attacks;

I. INTRODUCTION

Text password is the most popular form of user authentication on websites due to its convenience and simplicity. However, user 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 untrusted computers suffers password thief threat. An adversary can launch several password stealing attacks to snatch passwords, such as phishing, key loggers and malware.

Today's world is rapidly shifting to the internet. All the transactions of many big companies as well as small companies are to being conducted on the internet. People are also making shopping online, so people are getting more exposure in the internet world. This ultimately increases the risk of getting attacked. So there is need of introducing a new secure system that will be easy to use and the user can securely and confidently can perform their transactions online.

II. BACKGROUND

In the proposed system there are various components that play important role in adding up security layers. Whenever the user will go online, instead of the regular steps for logging in, he/ she will have to perform few more easy steps. In the oPass user authentications system, the extra components will be One time Passwords, SMS channel & 3G connection.

A. One Time Password

oPass adopts the one-time password strategy therefore, the strategy is given later.We also describe the secure features of SMS channel and explain why SMS can be trusted. Finally, we introduce the security of 3G connection used in the registration and recovery phases of oPass.

B. SMS Channel

SMS is a text-based communication service of telecommunication systems. oPass leverages SMS to construct a secure user authentication protocol against password stealing attacks. SMS represents the most successful data transmission of telecom systems; hence, it is the most widespread mobile service in the world. The SMS channel is chosen because of its security benefits. As SMS network is closed as compared to the TCP/IP network. By introducing SMS channel for performing online transaction such as logging in to the gmail, facebook accounts, the risk of getting your password hacked will be reduced.

C. 3G Connection

3G connection provides data confidentiality of user data and signal data to prevent eavesdropping attacks. It also provides data integrity of signal data to avoid tampering attacks

III. 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 untrusted computers suffers password thief threat. An adversary can launch several password stealing attacks to snatch passwords, such as phishing, key loggers and malware. To prevent users from such kind of attacks a new system with extra secured layers should be introduced.

A. *Abbreviations and Acronyms*

Here are some of the abbreviations that are used in this paper along with their illustrations provided.

ABBREVIATION	ILLUSTRATION
SMS	Short Message Service
TSP	Telecommunication Service Provider
PKI	Public Key Infrastructure
3G	Third Generation
TPM	Trusted Platform Module
SSL	Secure Socket Layer
MITM	Man in The Middle Attack

B. *Assumptions*

- Each web server possesses a unique phone number. Via the phone number, users can interact with each website through an SMS channel.
- The users' cellphones are malware-free. Hence, users can safely input the long-term passwords into cellphones.
- The telecommunication service provider (TSP) will participate in the registration and recovery phases. The TSP is a bridge between subscribers and web servers.
- The TSP and the web server establish a secure sockets layer (SSL) tunnel. Via SSL protocol, the TSP can verify the server by its certificate to prevent phishing attacks.

IV. OPASS

oPass consists of registration, login, and recovery phases. We introduce the details of these three phases respectively..

A. *System Overview*

The main Objective of oPass is free users from having to remember or type any passwords into conventional computers for authentication.

Unlike generic user authentication, oPass involves a new component, the cellphone, which is used to generate one-time passwords and a new communication channel, SMS, which is used to transmit authentication messages.

After filling out the registration form, the program asks the user to setup a long-term password. This long-term password is used to generate a chain of one-time passwords for further logins on the target server. Then, the program automatically sends a registration SMS message to the server for completing the registration procedure.

B. *Registration Phase*

The aim of this phase is to allow a user and a server to negotiate a shared secret to authenticate succeeding logins for this user. The user begins by opening the oPass program installed on their cellphone. User enters his/her ID and usually the website url or domain name to the program. The mobile program sends both IDs to the telecommunication service provider (TSP) through a 3G connection to make a request of registration. Once the TSP receives the IDs, it can trace the user's phone number based on user's SIM card.

C. *Login Phase*

The login phase begins when the user sends a request to the server through an untrusted browser (on a kiosk). The user uses his/ her cellphone to produce a one-time password, e.g., and deliver necessary information encrypted with to server via an SMS message. The server can verify and authenticate user Fig. 1 shows the detail flows of the login phase.

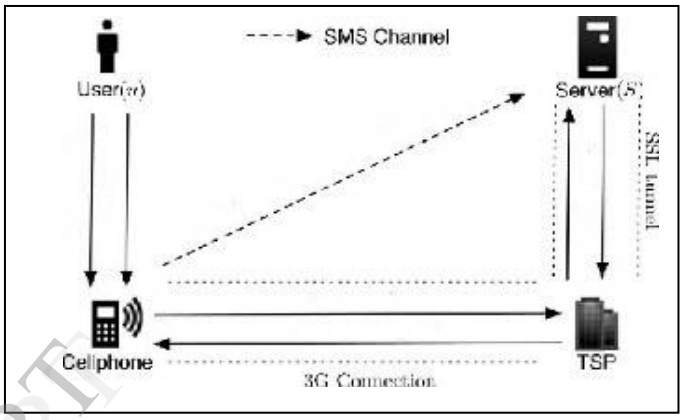

Fig. 1. *Flow of Login Phase*

D. *Recovery Phase*

Recovery phase is most important step as in some specific cases; for example, a user may lose his/ her cellphone. So in such case user will be able to recover oPass setting on their new cellphone assuming he/ she still uses the same phone number (apply a new SIM card with old phone number). Once user installs the oPass program on his/ her new cellphone, user can launch the program to send a recovery request with his/ her account ID and request. As we mentioned before, ID can be the domain name or URL link of server . Similar to registration, TSP can trace her phone number based on her SIM card and forward her account ID and the to server through an SSL tunnel. Once server receives the request, probes the account information in its database to confirm if account is registered or not. If account ID exists, the information used to compute the secret credential will be fetched and be sent back to the user.

ACKNOWLEDGMENT

We feel great pleasure in submitting this preliminary project report on "Web Based Security & Authentication Using Opass Mobile Application". We wish to express true sense of gratitude towards our internal project guide Prof. Mr. V.V. JOG, Computer Department, Smt.Kashibai Navale College of Engineering who is contributing his valuable guidance to this project. We sincerely thank our project committee and review committee members Prof.Kimbahune, Prof. P.N. Mahalle and for sparing their precious time and giving us valuable suggestions. We wish to thank our H.O.D. Prof.

P.N.MAHALLE for opening the doors of department towards the realization of the preliminary project report. We would also like to extend our sincere thanks to Principal Prof. A.V. Deshpande for his encouragement.

REFERENCES

[1] oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks by Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin, 2012. (*references*)

[2] An Empirical Study on the Web Password Strength in Greece by Artemios G.Voyiatzis, Christos A. Fidas, Dimitrios N. Serpanos and Nikolaos M. Avouris, 2011.

[3] A Large-Scale Study of Web Password Habits by Dinei Florencio and Cormac Herley WA, 2007

[4] Password Management Strategies for Online Accounts by Shirley Gaw & Edward W. Felten, 2006.