ISSN:0975-9646

Two Way Authentication Scheme for Mobile Applications and Web Application

Md Jaleel Ahmed Ansari[#1], P. Subhadra[*2]

[#1]*M. Tech Student,*[*2] *Associate Professor*

Dept. of CSE, Vardhaman College of Engg.
Hyderabad, India.

***Abstract*- Text countersign is that the most typical kind of user authentication on websites thanks to its simplicity and convenience. User's passwords square measure simple to be purloined and compromised below totally different threats. Two sorts of mistakes square measure unremarkably done by the users. Firstly, users choose weak passwords and utilize identical passwords across totally different websites. second writing the countersigns into untrusting computers results in password threat and felony. During this paper, we tend to style a user authentication protocol named OPass that uses a user's telephone and short message service to thwart countersign stealing and utilize attacks. OPass solely needs every collaborating web site to possess a novel sign and involves a telecommunication service supplier in registration and recovery phases. Reusing countersigns across totally different internet sites might cause users to lose their data that is keep in internet sites once the password hacked or compromised by wrongdoer. Second, hackers will install malicious code to urge the passwords, once user writing their username and countersign into unknown public computers. During this paper, developing net primarily based security analysis of Time countersign authentication schemes victimization mobile application. A user authentication protocol that involves user's telephone and short message service to stop counter sign stealing and utilize attacks. User's solely got to keep in mind a protracted term countersign for login on totally different websites.**

Keywords: **Network security, password stealing, password reuse attack , User authentication**

I. INTRODUCTION

Text password has been adopted as the primary means of user authentication for websites. People select the username and text password when registering accounts on a Website. In order to login into the website successfully, user must recall the registered password. Generally password based user authentication can resist brute-force and dictionary attacks if user select strong passwords. Thus most users would choose an easy to remember password. Even if they know the password might be unsafe. Another crucial problem is the user tends to reuse the password across on various websites. Password reuse causes users to lose sensitive information stored in different websites if the hacker compromises one of the passwords. This attack is referred to as a password reuse attack. The advantage is those users only have to remember Master password to access the management tool. Adversaries can steal or compromise passwords and impersonate users identities to launch malicious attacks, collect sensitive information and performs unauthorized payments actions or leak financial secrets.

The main cause of password stealing and reuse attack is when user types the passwords into un trusted public computers. The main concept of OPass is free users from having to remember or type any passwords into conventional computers for authentication. OPass involves new component a cell phone which is used to generate one-time password and a new communication channel, SMS which is used to transmit authentication messages. Password-based user authentication has a problem that humans are not able to remember all passwords. Because, most users would choose easy-to-remember passwords even if they know the passwords might be unsafe. Another crucial problem is that users reuse passwords across various websites For online accounts, users are at the same machine but access many different accounts. The average user has 6.5 passwords, each of which is shared across 3.9 different websites. Each user has about 25 accounts that require passwords, and types an average of 8 passwords per day. Users would choose weak passwords to remember easily. Users forget passwords a lot: we estimate that at least 1.5% of Yahoo users forget their passwords each month.

Generally, authentication methods are classified into three categories:

A. ***Inherit Based Authentication***

The Inherent Based Authentication category which is also known as Biometric Authentication, as the name suggests, is the automated method/s of identity verification or identification based on measurable physiological or behavioural characteristics such as fingerprints, palm prints, hand geometry, face recognition, voice recognition and such other similar methods. Biometric characteristics are neither duplicable nor transferable. They are constant and immutable. Thus it is near impossible to alter such characteristics or fake them. Furthermore such characteristics cannot be transferred to other users nor be stolen as happens with tokens, keys and cards. Unlike the security of a user's password, biometric characteristics, for instance the user's fingerprint or iris pattern, are no secret. Hence there is no danger of a break in security.

B. ***Token Based Authentication***

The Token Based Method category is again as the name suggests authentication based on a TOKEN such as: a key, a magnetic card, a smart card, a badge and a passport. Just as when a person loses a key, he would not be able to open

the lock, a user who loses his token would not be able to login, as such the token based authentication category is quite vulnerable to fraud, theft or loss of the token itself.

C. ***Knowledge Based Authentication***

The concept of Knowledge Based Authentication is simply the use of conventional passwords, pins or images to gain access into most computer systems and networks. Textual (alphabetical) and graphical user authentications are two methods which are currently used. True textual authentication which uses a surname and password has inherent weaknesses and drawbacks

II. EXISTING SYSTEM

The existing login systems typically include text primarily based login systems, biometric primarily based login systems, catch primarily based login systems and alternative ways. However, they are doing not offer comprehensive solutions. Additionally, phishing attacks and malware ar threats against countersign protection. Protective user's countersign on associate degree shady laptop is impossible once key loggers or back door SAR already put in on that. The text countersign has been adopted because the primary mean of user authentication for websites. Individuals choose their username and text passwords once registering accounts on an internet site. So as to log into the web site with success, users should recall the chosen passwords. Generally, password-based user authentication will resist brute force and lexicon attacks if users choose sturdy passwords to supply ample entropy.

However, password-based user authentication features a major drawback that humans don't seem to be specialists in memorizing text strings. Thus, most users would opt for easy-to-remember passwords (i.e., Weak passwords) although they apprehend the passwords may well be unsafe. Another crucial drawback is that users tend to utilize passwords across numerous websites on the average. Countersign utilize causes users to lose sensitive data hold on in numerous websites if a hacker compromises one in all their passwords. This attack is brought up because the countersign utilize attack. The higher than issues ar caused by the negative influence of human factors. Graphical countersigns ar additional strong than text passwords against multiple password interference (assuming distinct background images).Users might additional simply keep in mind multiple graphical passwords than multiple text passwords. Graphical passwords is a minimum of a {part of} the rationale for higher user performance which cueing ought to be part of any recall primarily based authentication theme. strictly automatic attacks might be accustomed facilitate inform safer style selections in implementing Pass Points-style graphical passwords. Proactive checking rules for Pass Points vogue graphical passwords may well be created supported the press order pattern attacks. A user will perform the bulk of browsing interactions from the laptop and solely perform terribly sensitive interactions from the organizer. Session scientific instrument permits a user to completely cash in of the convenience of employing a laptop.

A. ***Strong Passwords***

Users are frequently reminded of the risks: the popular press often reports on the dangers of financial fraud and identity theft, and most financial institutions have security sections on their web-sites which offer advice on detecting fraud and good password practices. As to password practices traditionally users have been advised Choose strong passwords Change their passwords frequently Never write their passwords down. Unfortunately, these recommendations appear somewhat out of date. If we enumerate the principal threats to a user's credentials they would appear to be:

1. Phishing
2. Key logging
3. A brute-force attack on the user's account (i.e. an attacker knows the user ID and tries to guess the password)
4. A bulk guessing attack on all accounts at the institution
5. Special knowledge or access attacks:
   (a) Guessing based on information about the user
   (b) Shoulder surfing
   (c) Console access to a machine where password Auto fill is enabled or a password manager is in use. As can be seen none of the password \best practices offers any real protection against phishing or key logging, which appear to be the most prevalent attacks. Strong passwords are just as susceptible to being stolen by a phisher or key logger as weak ones, and changing the password frequently helps only if the attacker is extremely slow to exploit the harvested credentials.

People have access to a computer and the internet when logging into online accounts, able to show the technology they used did not help them with recalling their passwords. The nature of online accounts and tools for managing passwords in online accounts enable poor password practices rather than remembering them. The data allows us to measure for the first time average password habits for a large population of web users. A Large Scale Study of Web Password Habits able to estimate the number of accounts that users maintain the number of passwords they type per day, and the percent of phishing victims in the overall population. Graphical passwords are more robust than text passwords against multiple password interference (assuming distinct background images). Users could more easily remember multiple graphical passwords than multiple text passwords. Graphical passwords is at least part of the reason for better user performance and that cueing should be part of any recall based authentication scheme. Purely Automated attacks could be used to help inform more secure design choices in implementing Pass Points-style graphical passwords. Proactive checking rules for Pass Points style graphical passwords might be created based on the click order pattern attacks.

A user can perform the majority of browsing interactions from the PC and only perform very sensitive interactions from the PDA (Personal Digital Assistant). Session Magnifier enables a user to fully take advantage of the convenience of using a Pc.

- Captcha Based Login System
- Text Password Based Login
- System Cryptography based Login system
- Image based Login System
- Biometric Based Login System

III. PROPOSED SYSTEM

People nowadays rely heavily on the Internet since conventional activities or collaborations can be achieved with network services (e.g., web service). Widely deployed web services facilitate and enrich several applications, e.g., online banking, e-commerce, social networks, and cloud computing. But user authentication is only handled by text passwords for most websites. Applying text passwords has several critical disadvantages. First, users create their passwords by themselves. For easy memorization, users tend to choose relatively weak passwords for all websites. This behaviour causes a risk of a domino effect due to password reuse. To steal sensitive information on websites for a specific victim (user), an adversary can extract her password through compromising a weak website because she probably reused this password for other websites as well. Second, humans have difficulty remembering complex or meaningless passwords. Some websites generate user passwords as random strings to maintain high entropy, even though users still change their passwords to simple strings to help them recall it. These approaches could mitigate this problem, but they also make the system more complicated to use. In addition, phishing attacks and malware are threats against password protection. Protecting a user's password on a kiosk is infeasible when key loggers or backdoors are already installed on it. Considering the current mechanisms, authenticating users via passwords is not a comprehensive solution. Therefore, we proposed a user authentication, called OPass, to thwart the above attacks. The goal of OPass is to prevent users from typing their memorized passwords into kiosks. By adopting one-time passwords, password information is no longer important. A one-time password is expired when the user completes the current session. Different from using Internet channels, OPass leverages SMS and user's cell phones to avoid password stealing attacks. We believe SMS is a suitable and secure medium to transmit important information between cell phones and websites. Based on SMS, a user identity is authenticated by websites without inputting any passwords to untrusted kiosks. User password is only used to restrict access on the user's cell phone. In OPass, each user simply memorizes a long-term password for access her cell phone. The long-term password is used to protect the information on the cell phone from a thief.

IV. IMPLEMENTATION

The user operates her cell phone and the untrusted computer directly to accomplish secure logins to the web server. The communication between the cell phone and the web server is through the SMS channel. The web browser interacts with the web server via the Internet. In our protocol design, we require the cell phone interact directly with the kiosk. OPass consists of a trusted cell phone, a browser on the kiosk, and a web server that users wish to access. The user operates her cell phone and the un trusted computer directly to accomplish secure logins to the web server.

Fig. 1 describes the architecture (and environment) of the OPass system. For users to perform secure login on an untrusted computer (kiosk), OPass consists of a trusted cell phone, a browser on the kiosk, and a web server that users wish to access. The user operates her cell phone and the untrusted computer directly to accomplish secure logins to the web server. The communication between the cell phone and the web server is through the SMS channel.

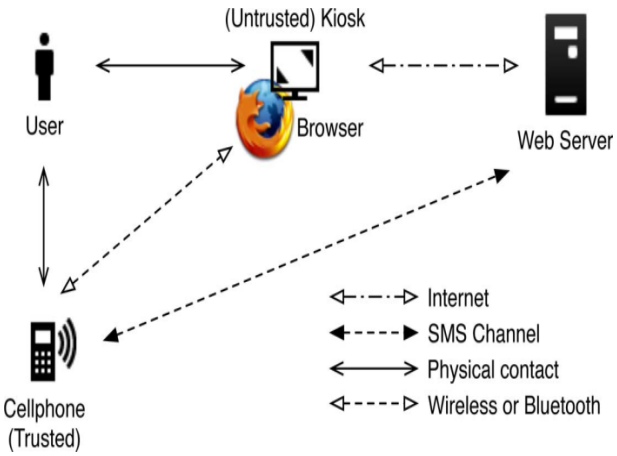


Fig. 1. Architecture of OPass system.

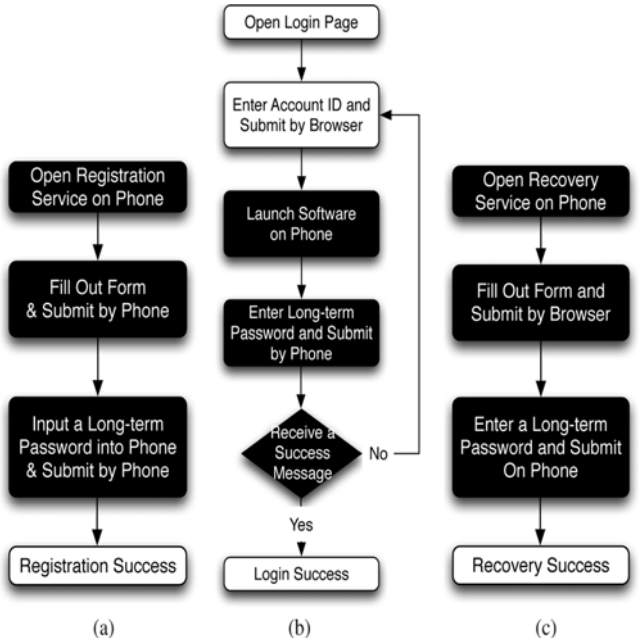
The web browser interacts with the web server via the Internet. In our protocol design, we require the cell phone interact directly with the kiosk. The general approach is to select available interfaces on the cell phone, Wi-Fi or Bluetooth. The cell phone that has the android application which is used to generate One Time Password (OTP) OPass has the following advantages:

OPass schemes achieve one-time password approach. The cell phone automatically derives different passwords for each login. The password is different during each login. Under one-time password approach, users do not need to remember any password for login. They only keep a long-term password for accessing their cell phones I design a user authentication protocol named OPass which leverages a user's cell phone and short message service to plan 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. This long term password is used to generate a chain of one-time introduced years before. Evaluated new graphical password schemes to achieve better security than text passwords.

When Graphical password users were creating passwords they were able to quickly and easily create a valid password, but to learn those passwords they had more difficulty than alphanumeric password users. However, the graphical users took longer time and made more invalid password as compared to alphanumeric users while practicing their passwords Biddle studied Multiple Password Interference and Click-Based Graphical Passwords. They concluded that graphical password users managed significantly better than text password users and they did not use similar passwords across multiple accounts. They also concluded that remembering multiple click-based graphical passwords is easier than remembering multiple text passwords. Text password users made comparatively more recall errors than graphical password which was based on two areas i.e. security and usability. 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. The user name is the only information input to the browser. Next, the user opens the OPass program on her phone and enters the long-term password, the program will generate a one-time password and send a login SMS securely to the server. The login SMS is encrypted by the one-time password.

Fig.2. Operation flows for user in each phase of OPass system respectively. Black rectangles indicate extra steps contrasted with the generic authentication system: (a) registration, (b) login, and (c) recovery.



V. CONCLUSION

In this paper, we 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 untrusted 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. To make OPass fully functional, password recovery is also considered and supported when users lose their cell phones. They can recover our OPass system with reissued SIM cards and long-term passwords.

REFERENCES

[1] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.

[2] S. Gawand E. W. Felten, "Password management strategies for online accounts," in SOUPS '06: Proc. 2nd Symp. Usable Privacy . Security, New York, 2006, pp. 44–55, ACM.

[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666, ACM.

[4] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords," in CCS '09: Proc. 16th ACM Conf. Computer Communications Security, New York, 2009, pp. 500–511, ACM.

[5] . Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in SSYM'99: Proc. 8th Conf. USENIX Security Symp., Berkeley, CA, 1999, pp. 1–1, USENIX Association.

[6] A. Perrig and D. Song, "Hash visualization: A new technique to improve real-world security," in Proc. Int.Workshop Cryptographic Techniques E-Commerce, Citeseer, 1999, pp. 131–138.

[7] J. Thorpe and P. van Oorschot, "Towards secure design choices for implementing graphical passwords," presented at the 20th. Annu. Computer Security Applicat. Conf., 2004.

[8] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," Int. J. Human-Computer Studies, vol. 63, no. 1–2, pp. 102–127, 2005.

[9] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in AVI '06: Proc. Working Conf. Advanced Visual Interfaces, New York, 2006, pp. 177–184, ACM.

[10] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in CCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170, ACM.