NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 4, ISSUE 2, Feb.-2017

WEB AUTHENTICATION PASSWORD DETECTION OF NETWORK SECURITY ATTACK USING S-PASS

BABASAHEB WAGHMODE
Department of Computer Engineering, A.C.Patil College of Engineering, Kharghar, Navi Mumbai Mumbai University, babasaheb27@gmail.com

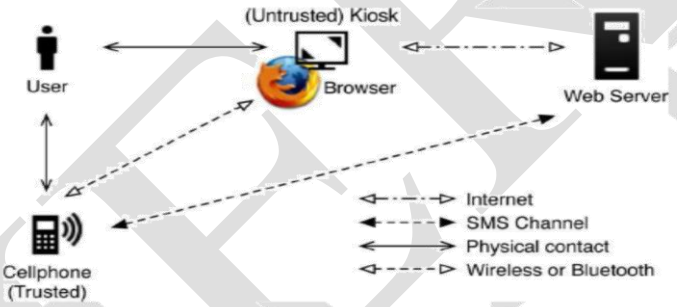
ABSTRACT
In Today's digital world all information and data is kept safe by passwords. The simple and convenient format of password is in the form of text. But, text passwords are not always strong enough and under different vulnerabilities they are very easily stolen and changed. When a person creates a weak password or same password is reused in many sites it may be possible that others can acquire that password. If one password is stolen, then it is possible that it can be used for all the websites. This phenomenon is known as the Domino Effect. Other possible risky attacks are related to phishing, malware and key loggers etc.
A protocol is designed which makes use of the user's customer's mobile i.e. cellular phone and SMS (short message service) to ensure protection against password stealing attacks. This user authentication protocol is named as S-Pass. The unique phone number is required which will be possessed by each participating website. The telecommunication service provider plays important role in the registration and the recovery phases. The main theme is to reduce the password reuse attack. It works with one time password technology, and results in reduction of the password validity time. The results show improvement in performance of the security.

INTRODUCTION
Internet and network services play vital role in today's digital world. The various web services are like online banking, social networks, cloud computing. For the security and authentication purpose of user needs a password. Mostly text based password is used. While registering accounts on a website, user selects his username and text password. In order to log into the website successfully, user must recall the selected passwords. To provide sufficient entropy, if users select strong passwords, then user authentication based on password can resist attacks like brute force attack and dictionary attack. However, a major problem is, password based user authentication involves humans and they are not experts in memorizing text strings. So the weak passwords (i.e. easy-to-remember passwords) would be chosen by most users even if they know the passwords might be unsafe. It is found that, the users tend to reuse passwords across various websites. This is another crucial problem. Reuse of Password causes users to lose sensitive information stored in different websites, if a hacker compromises one of their passwords. This attack is said to be the password reuse attack. Such problems are caused by the negative influence of the human factors. The various technologies are invented to reduce the negative impact of the human factors in the user authentication procedure. Since humans have adept nature in remembering graphical passwords than text passwords, there were many techniques related to graphical password designed to notify human's problem of password recalling . Making use of password management tools is an alternative approach. These tools can be used to automatically generation of the strong passwords for each website. It points out problems of password reuse and password recall problems. Due to this, users have to remember only one master password to access the management tool; this is an advantage .The another attack is related to the password stealing.
Adversaries steal or compromise passwords. They may impersonate users' identities to collect sensitive information, to launch malicious attacks, perform unauthorized payment actions and they may leak financial secrets. The most common and efficient password stealing attack is Phishing. Some researches focus on three-factor authentication rather than password-based authentication to provide more reliable user authentication. The previously three-factor authentication system depends on what user knows i.e. password, what user have i.e., token, and who user is i.e., biometric). To pass on the authentication function, the user must have to input a password and provide a pass code generated by the token (e.g., RSA), and scan his biometric features (e.g.,

fingerprint or pupil). Three-factor authentication is a comprehensive defence mechanism against the attacks like password stealing, however it requires comparative high cost. Compared to three-factor authentication, two-factor authentication is more attractive and practical. Although two-factor authentication is supported by many banks, it still suffers from the bad influence of human factors, like the password reuse attack. Another factor is, users have to memorize another four-digit PIN code to work together with the token, for example RSA Secure ID. The proposed system gives a Password authentication Security protocol (S-Pass) which combines the user's cell phone and short message service (SMS) to prevent the password reuse and password stealing attacks. The proposed system state that the main cause of stealing password attacks is when users type passwords to un-trusted public computers. The main concept of S-Pass is to free users from having to remember or type any passwords into conventional computers for authentication. The authentication system i.e. S-Pass involves a new instrument, i.e. the cell phone, which is used to generate one-time passwords. It has a new communication channel, i.e. SMS, which is used to transmit authentication messages.

EXISTING SYSTEM FRAMEWORK

People now a day's 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.



FOLLOWING ARE THE DISADVANTAGES OF EXISTING SYSTEM

1. First, users create their passwords by themselves. For easy memorization, users tend to choose relatively weak passwords for all websites . This behavior 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.
2. Humans have difficulty remembering complex or meaningless passwords.
3. Phishing attacks and malware are threats against password protection.
4. key loggers or backdoors Attacks on Password of login user

PROPOSED SYSTEM

Considering the above disadvantages of web authenticating users via passwords Therefore, we proposed a user authentication Protocol called S-Pass.to protect the above attacks. The goal of S-Pass 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, S-Pass leverages SMS and user's cell-phones to avoid password stealing attacks.

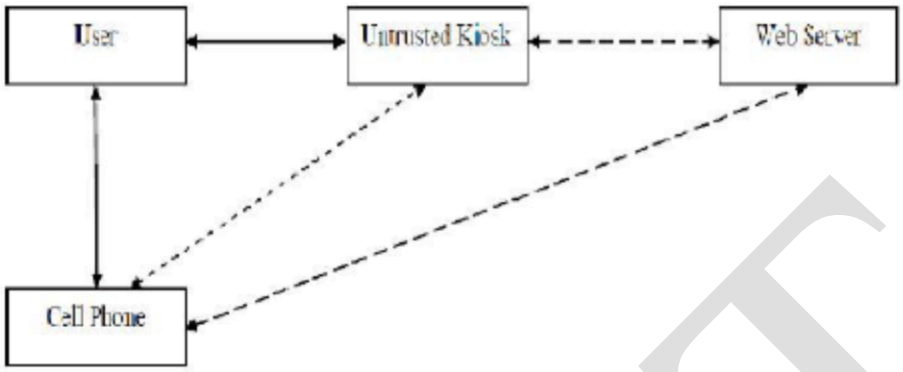


Fig. S-Password protocol Architecture

Above Figure describes the architecture (and environment) of the S-Pass system. To perform secure login on an un trusted computer (kiosk), S-Pass consists of a trusted cell phone, a browser on the kiosk, and a web server that users wish to access. To accomplish secure logins to the web server, the user operates his cell phone and the un trusted computer directly. The communication is possible through the SMS channel. The web browser interacts with the web server via the Internet. In our protocol design, it requires the cell phone interact directly with the kiosk. The basic way is to select available interfaces on the cell phone, SMS.

FOLLOWING ARE THE ADVANTAGES OF S-PASS SYSTEM:

1) Anti-malware—Malware (e.g., key logger) gathers sensitive information from users, like their password. In m-Pass, users are able to log into web services without entering passwords on their computers. Due to this change, malware is not able to obtain a user's information like password from un trusted computers.

2) Phishing Protection— Phishing attacks are launched by adversaries to steal users' passwords by cheating users when they connect to forged websites. S-Pass successfully allows users to log into the websites without disclosing or revealing passwords to computers. Users who adopt S-Pass are guaranteed to prevention of phishing attacks.

3) Password Reuse Prevention and Weak Password Avoidance— S-Pass achieves one-time password approach. For each login, the cell phone automatically derives different passwords; i.e. the password is different during each login. In this approach, users do not need to remember any password for login. They only keep a long term password for accessing their cell phones, and leave the rest of the work to S-Pass.

4) Cell phone Protection—An adversary can breach user authentication by stealing user's cell phones. However, the cell phones are protected by a long-term password. The adversary cannot impersonate a legal user to login without being detected.

FOLLOWING PHASES OF S-PASS SYSTEM:

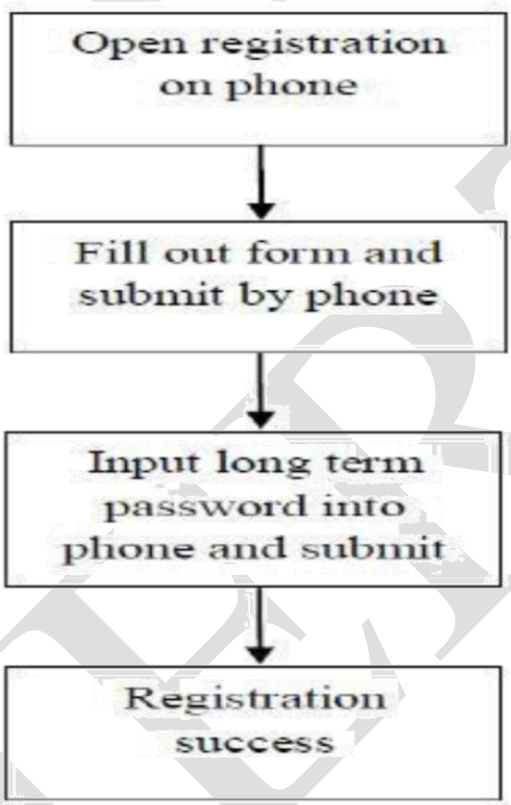
REGISTRATION PHASE:

In this phase, the user and a server negotiate a shared secret to authenticate succeeding logins for this user. The S-pass program installed on his cell phone is opened by the user. The user enters IDu (account id) and IDs to the program. The mobile program sends IDu and IDs to the telecommunication service provider (TSP). This is done through a 3G connection which makes a request of registration. Once the TSP received the IDu and the IDs, it can trace the user's phone number Tu based on SIM card used by user. After that TSP is used to distribute a shared key Ksd which plays the role of third-party between the user and the server. To encrypt the registration SMS with AES-CBC, the shared key is used. To protect the communication, the TSP and the server

S will establish an SSL tunnel. Then the TSP forwards IDu, Ksd, Tu , and to the assigned server S. Server will generate the corresponding information for this account a response, including server's identity IDs , a random seed ø, and server's phone number Ts . The TSP then forwards IDs , ø ,Ts , and a shared key Ksd to the user's cell phone. After reception of the response is finished, the user continues to setup a long-term password Pu with his cell phone. The cell phone computes a secret credential C by the following operation:

C= H(Pu ‖ IDs ‖ ø).

Fig. Registration Phase



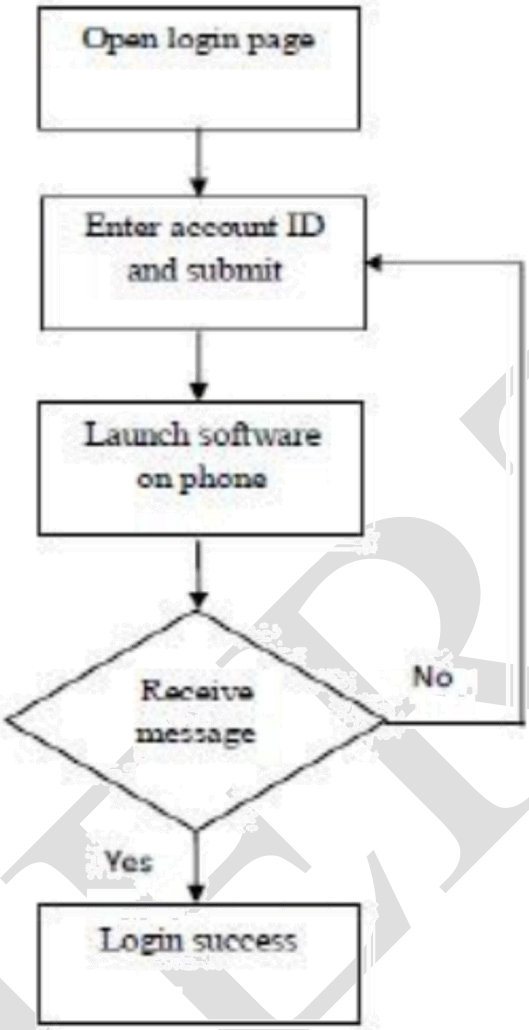
LOGIN PHASE:

The login begins when the user u sends a request to the server S through an un trusted browser (on a kiosk). The user uses his cell phone to produce a one-time password, e.g., δi. Then delivers necessary information encrypted with δi to server S via an SMS message. Server S can verify and authenticate user u based on δi, based on pre shared secret credential C, The protocol is started when the user u wishes to log into his already registered favorite web server S. However, user u begins with the login procedure by accessing the specific website via a browser on an un trusted kiosk. Then the browser sends a request to S with u's account IDu. Next, server S supplies the IDs and fresh nonce ns to the browser. Meanwhile, this message is forwarded to the cell phone through SMS or wireless interfaces. After receiving the message, the cell phone inquires related information from its database via IDs, which includes server's phone number and other parameters. The next step is promoting a dialog for the long-term password. Secret shared information can regenerate by providing the correct on the cell phone. The OTP i.e. one-time password for current login is recomputed using the following operations:

C= H(Pu ‖ IDs ‖ ø).

δi= Hn-i(c).

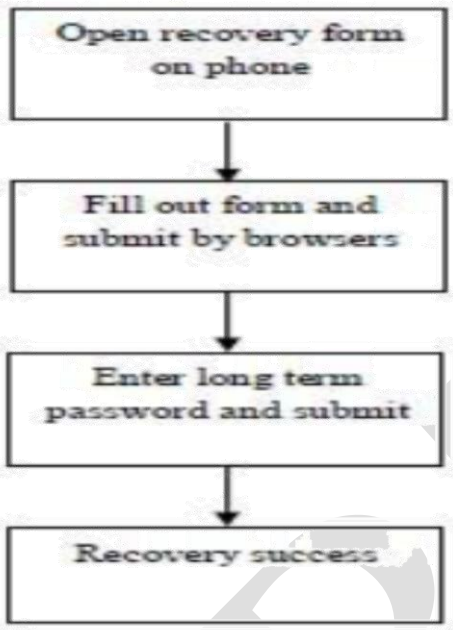
Fig: login phase



RECOVERY PHASE:

The recovery phase is designated for some specific conditions; for example, a user u may lose his cell phone. The protocol is able to recover S-Pass setting on his new cell phone assuming he still uses the same phone number (apply a new SIM card with old phone number).After the user u installs the S-Pass program on his new cell phone, he can launch the program to send a recovery request with his account IDs and requested server IDs through the 3G connection is to predefined TSP.As mentioned before, IDs can be the domain name or URL link of server. Similar to registration, TSP can trace his phone number Tu based on his SIM card and forward his account IDs and the Tu to server through an SSL tunnel. Once server S receives the request, S probes the account information in its database to confirm if account u is registered or not. If account IDu exists, the information used to compute the secret credential c will be fetched and be sent back to the user. The server S generates a fresh nonce ns and replies a message which consists of IDs, ø ,Ts , i , and S . The message includes all important fields for generating the next one-time passwords to the user u. When the mobile program receives the message, like registration, to reproduce the correct one-time password δi+1 , it forces the user u to enter his long-term password . During the final step, the user's cell phone encrypts the secret credential c and server nonce ns to a cipher text. The recovery SMS message is delivered back.

fig. Recovery phase



RESULT:

Below table evaluates our system with earlier systems indicating avoided attacks. Symbol ✓ " shows that the system avoids attacks, and - " represents "not applicable". Following comparison shows our system with different previous research approaches'.

System	Attack Prevention					
	Session hijacking	Phishing	Key-logging	Password reuse	DNS spoofing	Malware prevention
Our system	✓	✓	✓	✓	✓	✓
oPass [1]	✓	✓	✓	✓	✓	✓
MP-Auth [4]	✓	✓	✓	–	✓	✓
Phool Proof [2]	✓	✓	✓			✓
Secure Web[3]	✓	✓	✓		✓	✓
BitE [15]			✓		✓	✓
Garriss *et al.*[16]			✓			✓
Session Magnifier[14]	✓				✓	
Secure Pass [5]	✓	✓	✓	✓	✓	✓

CONCLUSION:

Web authentication protocol i.e. S-Pass leverages cell phones and SMS to prevent password stealing and password reuse attacks. The assumption it makes is that each website possesses a unique phone number. The important principle of the proposed system i.e. S-Pass is to eliminate the negative influence of human factors as

much as possible. Because of S-Pass, each user only needs to memorize the long-term password which has been used to protect his cell phone. Users are free from typing any passwords into un-trusted computers for the sake of login on all websites. Compared with previous schemes, S-Pass is the user authentication protocol to prevent password stealing and password reuse attacks simultaneously. The reason is that the S-Pass adopts the one-time password way to ensure independence between each and every login. Password recovery is also considered to make S-Pass fully functional. When users lose their cell phones password recovery plays it's very important role.

REFERENCES:

1) Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsin Lin "*O-pass : A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attack," in IEEE Transaction Vol 7, No.2, April 2012*.

2) B. Parno, C. Kuo, and A. Perrig, "*Phool proof phishing prevention," Financial Cryptography Data Security, pp. 1–19, 2006.*

3) M.Wu, S. Garfinkel, and R. Miller, "*Secure web authentication with mobile phones," in DIMACS Workshop Usable Privacy Security Software, 2004*

4) H. Krawczyk, "*The order of encryption and authentication for protecting communications (or: How secure is SSL?)," in Advances Cryptology— CRYPTO, pp. 310–331, 2001.*

5) C. Yue and H. Wang, "*Session Magnifier: A simple approach to secure and convenient kiosk browsing," in Proc. ACM 11th Int. Conf. Ubiquitous Computing, 2009, pp. 125– 134.*

6) M.Wu, S. Garfinkel, and R. Miller, "*Secure web authentication with mobile phones," in DIMACS Workshop Usable Privacy Security Software, 2004.*

7) Justin Martineau, Palanivel Kodeswaran, "*Secure Pass: Guarding sensitive information from un-trusted machines", www.csee.umbc.edu /~palanik1/ Secure PassPaper.pdf*

8) *Anti-Phishing Working Group. Phishing Activity Trends Report, July, 2006.*

9) *www.google.com*