ProcurePass: A User Authentication Protocol to Resist Password Stealing and Password reuse Attacks

Mariam M. Kassim, A. Sujitha B.Tech., M.E.

Abstract— The most popular form of user authentication is the text password, which is the most convenient and the simplest. Users mostly choose weak passwords and reuse the same password across different websites and thus, a domino effect. ie., when an adversary compromises one password, she exploits, gaining access to more websites. Also typing passwords into public computers(kiosks) suffers password thief threat, thereby the adversary can launch several password stealing attacks, such as phishing, keyloggers and malware. Therefore user's passwords tends to be stolen and compromised under different threats and vulnerabilities. A user authentication protocol named ProcurePass, which benefits a user's cellphone and short message service to prevent password stealing and password reuse attacks. ProcurePass adopts the one-time password strategy, which free users from having to remember or type any passwords into conventional public computers for authentication.

Index Terms— encryption, hash function, network security, one-time password, password reuse attack, password stealing attack, user authentication.

1 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 these passwords. Generally, password based user authentication can resist brute-force and dictionary attacks if users select strong passwords. 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 those passwords might be unsafe. Another crucial problem is that users tend to reuse passwords across various websites. Password reuse causes users to lose sensitive information stored in different websites if a hacker compromises one of their passwords. This attack is referred to as the password reuse attack. The above problems are caused by the negative influence of human factors. Therefore, it is important to take human factors into consideration when designing a user authentication protocol.

Researchers have investigated a variety of technology to reduce the negative influence of human factors in the user authentication procedure. Since humans are more adept in remembering graphical passwords than text passwords many graphical password schemes were designed to address human's password recall problem. Using password management tools is an alternative. These tools automatically generate strong passwords for each website, which addresses password reuse and password recall problems. The advantage is that users only have to remember a master password to access the management tool.

Despite the assistance of these two technologies—graphical password and password management tool—the user authentication system still suffers from some considerable drawbacks.

Although graphical password is a great idea, it is not yet mature enough to be widely implemented in practice and is still vulnerable to several attacks. Password management tools work well; however, general users doubt its security and thus feel uncomfortable about using it. Furthermore, they have trouble using these tools due to the lack of security knowledge.

Besides the password reuse attack, it is also important to consider the effects of password stealing attacks. Adversaries steal or compromise passwords and impersonate users' identities to launch malicious attacks, collect sensitive information, perform unauthorized payment actions, or leak financial secrets. Phishing is the most common and efficient password stealing attack. Many previous studies have proposed schemes to defend against password stealing attacks.

Some researches focus on three-factor authentication rather than password-based authentication to provide more reliable user authentication. Three-factor authentication depends on what you know (e.g., password), what you have (e.g., token), and who you are (e.g., biometric). To pass the authentication, the user must input a password and provide a pass code generated by the, and scan her biometric features (e.g., fingerprint or pupil). Three-factor authentication is a comprehensive defense mechanism against password stealing attacks, but it requires comparative high cost.

Thus, two-factor authentication is more attractive and practical than three-factor authentication. Although many banks support two-factor authentication, it still suffers from the negative influence of human factors, such as the password reuse attack. Users have to memorize another four-digit PIN code to work together with the token.

A user authentication protocol named Procurepass which leverages a user's cellphone and short message service (SMS) to prevent password stealing and password reuse attacks. It is difficult to thwart password reuse attacks from any scheme where the users have to remember something. The main cause of stealing password attacks is when users type passwords to untrusted public computers.

Therefore, the main concept of Procurepass is free users from having to remember or type any passwords into conventional computers for authentication. Unlike generic user authentication, procurepass 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.

Procureass presents the following advantages:

- *Mariam M. Kassim is currently pursuing masters degree program in computer scince & engineering in Anna University, Chennai, India, E-mail: mehakassim@gmail.com.*
- *A. Sujitha, B.Tech., M.E. is currently Assistant Professor in computer science & engineering department of Sasurie College of Engineering, Tirupur,TN, India.*

1) Anti-malware—Users are able to log into web services without entering passwords on their com- puters. Thus, malware cannot obtain a user's password from untrusted computers.
2) Phishing Protection—Allows users to successfully log in- to websites without revealing passwords to computers.
3) Secure Registration and Recovery—SMS aids procurepass in establishing a secure channel for message exchange in the registration and recovery phases.
4) Password Reuse Prevention and Weak Password Avoidance—Users do not need to re- member any password for log- in. They only keep a long- term password for accessing their cellphones, and leave the rest of the work to procurepass.
5) Cellphone Protection—An adversary can steal users' cellphones and try to pass through user authentication. However, the cellphones are protected by a long-term password. The adversary cannot impersonate a legal user to login without being detected.

2 PROBLEM DEFINITION AND ASSUMPTIONS

2.1 Problem Definition

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 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.

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. Phishing attacks and malware are threats against password protection. Protecting a user's password on a kiosk is infeasible when keyloggers or backdoors are already installed on it. Considering the current mechanisms, authenticating users via passwords is not a best solution.

Therefore, a user authentication, called ProcurePass, to thwart the above attacks. The goal of 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, ProcurePass leverages SMS and user's cellphones to avoid password stealing attacks. SMS is a suitable and secure medium to transmit important information between cellphones 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 cellphone. In ProcurePass, each user simply memorizes a long-term password for access her cellphone. The long-term password is used to protect the information on the cellphone from a thief.

2.2 Architecture and Assumption

Fig. 1 describes the architecture (and environment) of the ProcurePass system. The assumptions in ProcurePass system are as follows:

1) Each web server possesses a unique phone number. Via the phone number, users can interact with each website through an SMS channel.
2) The users' cellphones are malware-free.
3) The telecommunication service provider (TSP) is a bridge between subscribers and web servers. It provides a service for subscribers to perform the registration and recovery process with eachweb service. For example, a subscriber inputs her id ID and a web server's id ID to start to execute the registration phase. Then, the TSP forwards the request and the subscriber's phone number to the corresponding web server based on the received ID .
4) 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. With the aid of TSP, the server can receive the correct sent from the subscriber.
6)If a user loses her cellphone, she can notify her TSP to disable her lost SIM card and apply a new card with the same phone number. Therefore, the user can perform the recovery phase using a new cellphone.

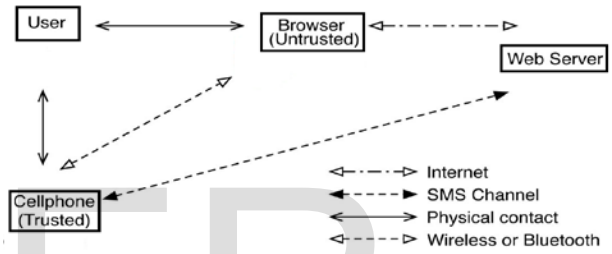

Fig 1: Architecture of ProcurePass System

2.3 ProcurePass

ProcurePass consists of registration, login, and recovery phases.

2.3.1 Overview

Fig. 2 describes the operation flows of users during each phase of ProcurePass. ProcurePass utilizes a user's cellphone as an authentication token and SMS as a secure channel. ProcurePass and are marked in black rectangles in Fig. 2, to show difference of additional steps with regular login process.

Contrasting with general cases, *login* procedure in ProcurePass does not require users to type passwords into an untrusted web browser. The user name is the only information input to the browser. Next, the user opens the ProcurePass 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. Finally, the cellphone receives a response message from the server and shows a success message on her screen if the server is able to verify her identity. The message is used to ensure that the website is a legal website, and not a phishing one.

2.3.2 Registration Phase

Fig. 3 depicts the *registration* phase. This 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 ProcurePass program installed on her cellphone. She enters ID_u (account id she prefers) and ID_s (usually the website url or domain name) to the program.

The mobile program sends ID_u and ID_s to the telecommunication service provider (TSP) through a 3G connection to make a request of registration. Once the TSP received the ID_u and ID_s, it can trace the user's phone number T_u based on user's SIM card. The TSP also plays the role of third-party to distribute a shared key K_{sd} between the user and the server. The shared key K_{sd} is used to encrypt the registration SMS with AES-CBC. The TSP and the server S will establish an SSL tunnel to protect the communication. Then the TSP forwards ID_u, T_u, and K_{sd} to the assigned server S.

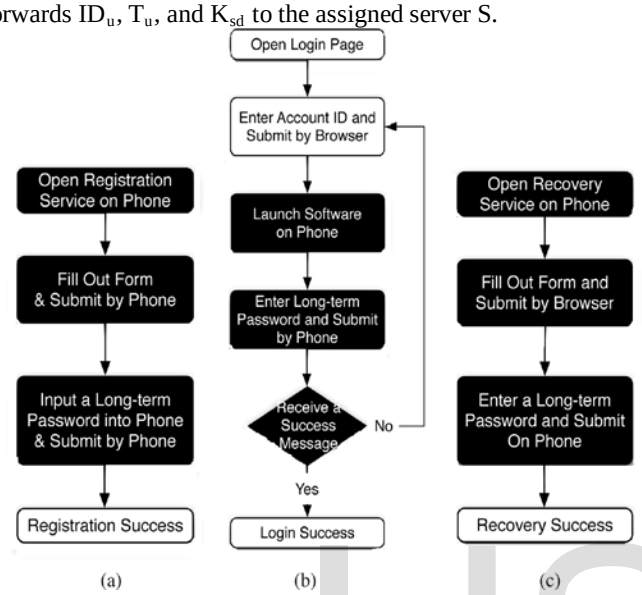

Fig. 2. Operation flows for user in each phase of ProcurePass system respectively. Black rectangles indicate extra steps contrasted with the generic authentication system: (a) registration, (b) login, and (c) recovery.

Server will generate the corresponding information for this account and reply a response, including server's identity ID_s, a random seed ϕ, and server's phone number T_s. The TSP then forwards ID_s, ϕ, T_s, and a shared key K_{sd} to the user's cellphone. Once reception of the response is finished, the user continues to setup a long-term password P_u with her cellphone. The cellphone computes a secret credential by the following operation:

$$c = \mathcal{H}(P_u||ID_s||\phi) \quad (5)$$

To prepare a secure registration SMS, the cellphone encrypts the computed credential c with the key and generates the corresponding MAC, i.e., $HMAC_1$. HMAC-SHA1 takes input user's identity, cipher text, and IV to output the MAC. Then, the cellphone sends an encrypted registration SMS to the server by phone number T_s as follows:

$$\text{Cellphone} \xrightarrow{\text{sms}} \text{S: } ID_u, \{c||\phi\}\mathbf{K}_{sd}, IV, HMAC_1. \quad (6)$$

Server S can decrypt and verify the authenticity of the registration SMS and then obtain c with the shared key K_{sd}. Server S also compares the source of received SMS with T_u to prevent SMS spoofing attacks. At the end of registration, the cellphone stores all information $\{ID_s, T_s, \phi, i\}$, except for the longterm password P_u and the secret c. Variable i indicates the current index of the one-time password and is initially set to 0. With i, the server can authenticate the user device during each login. After receiving the message (6), the server stores $\{ID_u, T_u, c, \phi, i\}$ and then completes the registration.

2.3.3 Login Phase

The *login* phase begins when the user sends a request to the server S through an untrusted browser (on a kiosk). The user uses her cellphone to produce a one-time password, e.g., δ_i, and deliver necessary information encrypted with δ_i to server S via an SMS message. Based on preshared secret credential c, server S can verify and authenticate user based on δ_i. Fig. 4 shows the detail flows of the login phase. The protocol starts when user u wishes to log into her favorite web server (already registered). However, u begins the login procedure by accessing the desired website via a browser on an untrusted kiosk. The browser sends a request to S with u's account ID_u. Next, server S supplies the ID_s and a fresh nonce n_s to the browser.

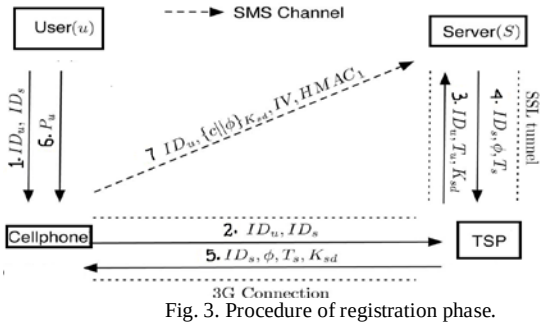

Fig. 3. Procedure of registration phase.

Meanwhile, this message is forwarded to the cellphone through bluetooth or wireless interfaces. After reception of the message, the cellphone inquires related information from its database via ID_s, which includes server's phone number T_s and other parameters $\{\phi, i\}$. The next promoting a dialog for her long-term password P_u. Secret shared credential c can be regenerated by inputting the correct P_u on the cellphone.

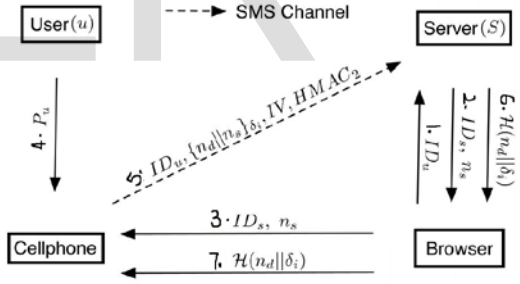

Fig. 4. Procedure of login phase.

The one-time password δ_i for current login is recomputed using the following operations:

$$c = \mathcal{H}(P_u||ID_s||\phi). \quad (7)$$

$$\delta_i = \mathcal{H}^{N-i}(c). \quad (8)$$

δ_i is only used for this login (ith login after user registered) and is regarded as a secret key with AES-CBC. The cellphone generates a fresh nonce n_d . To prepare a secure login SMS, the cellphone encrypts n_d and n_s with and generates the corresponding MAC, i.e., $HMAC_2$. The next action on the cellphone is sending the following SMS message to server S:

$$\text{Cellphone} \xrightarrow{\text{sms}} \text{S : } ID_u, \{\eta_d||\eta_s\}\delta_i, IV, HMAC_2. \quad (9)$$

After receiving the login SMS, the server recomputes δ_i (i.e., $\delta_i = H^{N-i}(c)$)) to decrypt and verify the authenticity of the login SMS. If the received n_s equals the previously generated n_s

, the user is legitimate; otherwise, the server will reject this login request. Upon successful verification, the server sends back a success message through the Internet, $H(n_d||\delta_i)$, to the user device. The cellphone will verify the received message to ensure the completion of the login procedure. The last verification on the cellphone is used to prevent the phishing attacks and the man-in-the-middle attacks. If the verification failed, the user knows the failure of login, and the device would not increase the index *i*. If the user is successfully log into the server, index is able to automatically increased, *i=i+1*, in both the device and the server for synchronization of one-time password. After N-1 rounds, the user and the server can reset their random seed by the *recovery* phase to refresh the one-time password.

Table I shows the notations used in the ProcurePass system.

TABLE I
NOTATIONS

Name	Description
ID_x	Identity of x.
T_y	Entity y's phone number.
ϕ	Random seed.
N	Predefined length of hash chain({}).
n_z	Nonce generated by entity z.
P_u	User u's longterm password.
K_{sd}	Shared secret key between cellphone and the server.
c	Secret shared credential between cellphone and the server.
δ_i	i^{th} one-time password.
$\|$	Concatenate operation.
$\{\}_k$	Symmetric encryption [1] with key k.
H(o)	Hash function H^2 with input o.
IV	Initialization vector of AES-CBC.
$HMAC_1$	The HMAC-SHA1 digest of $ID_u\|\|IV\|\|\{c\|\|\phi\}K_{sd}$ under the K_{sd}.
$HMAC_2$	The HMAC-SHA1 digest of $ID_u\|\|IV\|\|\{n_d\|\|n_s\}\ \delta_i$ under the δ_i .
$HMAC_3$	The HMAC-SHA1 digest of $ID_u\|\|IV\|\|\{c\|\|n_s\}\ \delta_{i+i}$ under the δ_{i+i}.

[1]Symmetric encryption algorithm in ProcurePass is AES-256.
[2]Hash function is SHA-256.

2.3.4 Recovery Phase

Recovery phase is designated for some specific conditions; for example, a user *u* may lose her cellphone. The protocol is able to recover ProcurePass setting on her new cellphone assuming she still uses the same phone number (apply a new SIM card with old phone number).

Once user installs the ProcurePass program on her new cellphone, she can launch the program to send a recovery request with her account ID_u and requested server ID_s to predefined TSP through a 3G connection. ID_s can be the domain name or URL link of server S. Once server receives the request, probes the account information in its database to confirm if account is registered or not. If account ID_u exists, the information used to compute the secret credential *c* will be fetched and be sent back to the user. The server generates a fresh nonce and replies a message which consists of ID_s, ϕ, T_s, *i*, and n_s. This message includes all necessary elements for generating the next one-time passwords to the user *u*.

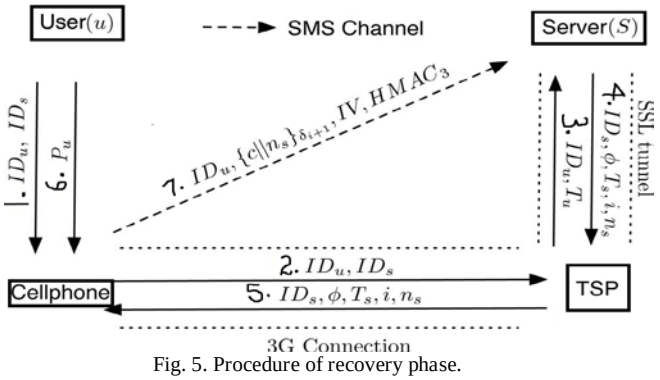

Fig. 5. Procedure of recovery phase.

When the mobile program receives the message, it forces the user *u* to enter her long-term password to reproduce the correct one-time password δ_{i+1}. During the last step, the user's cellphone encrypts the secret credential and server nonce to a ciphertext. The recovery SMS message is delivered back to the server for checking.

3 Conclusion

ProcurePass which leverages cellphones 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 ProcurePass is to eliminate the negative influence of human factors as much as possible. Through ProcurePass, each user only needs to remember a long-term password which has been used to protect her cellphone. Users are free from typing any passwords into untrusted computers for login on all websites. Compared with previous schemes, ProcurePass is the first user authentication protocol to prevent password stealing (i.e., phishing, keylogger, and malware) and password reuse attacks simultaneously. The reason is that ProcurePass adopts the one-time password approach to ensure independence between each login. To make ProcurePass fully functional, password recovery is also considered and supported when users lose their cellphones. They can recover our ProcurePass system with reissued SIM cards and long-term passwords. A prototype of ProcurePass is also implemented to measure its performance. The average time spent on registration and login is 21.8 and 21.6 s, respectively. Besides, the performance of login of ProcurePass is better than graphical password schemes, for example, Passfaces. Therefore, we believe ProcurePass is acceptable and reliable for users.

References

[1] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks" ieee transactions on information forensics and security, vol. 7, no. 2, April 2012 651

[2] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in CHI '09: Proc. 27th Int. Conf. Human Factors Computing Systems, New York, 2009, pp. 889–898, ACM.

[3] P. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Information Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[4] T. Holz, M. Engelberth, and F. Freiling, “Learning more about the underground economy:Acase-study of keyloggers and dropzones,” Proc. Computer Security ESORICS 2009, pp. 1–18, 2010.

[5] Phishing Activity Trends Rep., 2nd Quarter/2010 Anti-Phishing Working Group [Online]. Available: http://www.antiphishing.org/

[6] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X. Zhang, “Trustworthy and personalized computing on public kiosks,” in Proc. 6th Int. Conf. Mobile Systems, Applications Services, 2008, pp. 199–210, ACM.

[7] M. Weir, S. Aggarwal, M. Collins, and H. Stern, “Testing metrics for password creation policies by attacking large sets of revealed passwords,” in Proc. 17th ACM Conf. Computer Communications Security, New York, 2010, pp. 162–175, ACM.

[8] C. Yue and H. Wang, “SessionMagnifier: A simple approach to secure and convenient kiosk browsing,” in Proc. 11th Int. Conf. Ubiquitous Computing, 2009, pp. 125–134, ACM.

[9] R. Biddle, S. Chiasson, and P. van Oorschot, “Graphical passwords: Learning from the first twelve years,” in ACM Computing Surveys, Carleton Univ., 2010.

[10] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot. User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords. International Journal of Information Security, 8(6):387–398, 2009.