IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Secured Android Mobile Authentication

G.Monisha[1] , B.R.N.Bharat Prabhu[2]and B.Bharath Kumar[3]

[1,2,3]Depatment of IT, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India

Abstract

Most commonly used user authentication has been the text passwords for quite few years on websites for its simplicity. As the user text password is simple to use it is also vulnerable for different threats and also it can be stolen. Most of all users tend to reuse the same password over a number of website they log into which cause a domino effect. When an unknown person gets the password from any one of the website, they try to use them across different websites to gain access. Nowadays the most common threat is typing the password in untrusted computers and sites. A hacker can launch many password stealing attacks' to snatch the password, such as phishing, keyloggers and malware. In this paper, we propose a system which involves a user cell phone and a short message service to prevent password stealing and password reuse attack. Here a telecommunication service provider is involved during the registration and the recovery phases. In the proposed system user has to just remember only the long-term password for login the websites. We believe that this proposed system may overcome the password stealing attacks by an unknown person

Keywords: *Password reuse attacks, domino effect, password stealing attacks, Network security, User authentication*

1. Introduction

In the recent years, text passwords have been the primary means of user authentication for logging in the websites. Fro logging in a website user must first register with a new username and its corresponding text password. If it is a valid username then the user is given authority to log in the website. In order to log in the website the user has to recall the text password that was registered during the registration phase. Generally this kind of password-based used authentication can resist to brute force and dictionary attacks if the user selects a strong password to provide sufficient entropy. No matter how strong the password is password-based user authentication has a major drawback as humans are not a great expert in memorizing the text strings. So the user tends to use easy-to-remember passwords for logging in the websites i.e. weak passwords, even if they know the password might be unsafe which are prone to many password stealing attacks [1]. Another important problem is that user tends to reuse the password around different website [2]. In 2007, Florencia and Herley [3] indicated that a user reuses a password across 3.9 different websites on average. There is a high possibility that the user may lose their sensitive or personal information stored in differ websites if the hacker compromises one of their passwords. This type of attack is referred to as password stealing attack. This password stealing attack is mainly due to negative influence of the human factors. So it is very important to take into consideration about these factors before designing any user authentication system.

Many researchers have been conducted to reduce the negative influence of the human factors in the user authentication system. According to the researchers humans are quite a good expert in remembering something which is represented in pictorial format, thus graphical password schemes were designed to overcome the text password schemes [4], [5] to address human recall problem. There is also a alternative method where password management tool is used [6]. These tools automatically generate strong passwords for the users for each websites, which eliminates password reuse and password recall problem. The advantage of this password management tools is that user has to remember only a master password for accessing the tool. Despite these two new technologies for user authentication i.e., graphical passwords and password management tools, the authentication tools still suffers a major drawback. Graphical password user authentication is still not yet matures and there are considerable amount of graphical password attacks [7]. Password management tool works well but still users have trouble in these tools due to their lack of knowledge of using it.

Password reuse attacks are not a means for getting sensitive information, another important effect to consider is the password stealing attacks. Adversaries steal the password to launch malicious attacks for collecting sensitive information, to perform unauthorized payments and also to leak our financial secrets [8]. Phishing is most commonly used and also a

efficient stealing attack for getting users password. According to a survey around 300 users in India have been affected by this phishing attack with in Jan 20th 2013.

Some researchers tend to focus on the three-factor authentication procedure rather than the password user authentication for more reliable user authentication. It is base on what you know (i.e., password), what you have (i.e., token), what you are (i.e., biometric). For this type of authentication the user has to input their password and provide a pass code generated by the token (e.g., RSA SecureID [9]), and scan their biometric feature usually their fingerprint or their pupil. Even though it gives security for the user authentication mechanism, it requires a high cost for applying it in practice. Thus two-factor authentication is more practical than the three- factor authentication.

Many support two-factor authentication which still suffers from negative influence of human factors and also the password stealing attacks. So as to overcome this user must remember another four-digit PIN code to work together with the token for authentication

In this paper, we propose a user authentication system [10] which uses users' cellphone and a short message service (SMS) to prevent password stealing and reuse attacks. In our opinion the main cause of password stealing is by entering the username and the password in untrusted computers or websites. Unlike other user authentication systems the user doesn't have to enter their password in the browser. Instead a new component is used, users cellphone for enter the password and a new communication channel SMS is used to transmit the authentication messages. This system has the following advantages.

2. Background

Here we describe about some of the secure features of the SMS channel and explain why SMS can be trusted and also discuss about the security of the 3G connection which is used in registration and recovery phases of the authentication system.

2.1. SMS Channel

SMS is a fundamental text based communication service provides by the telecommunication system which belongs to 3GPP standards. Also SMS is a successful data transmission techniques used by the telecom systems, hence it is widely spread across the world. This authentication system uses the SMS channel for a secure user authentication to provide password stealing attacks. We chose SMS channel because of its security reasons. Unlike TCP/IP, SMS is a closed platform, thus increasing the difficulties' for internal attacks like tampering and manipulating attacks. Therefore SMS channel is an out-of-band communication channel which is used to transmit secured messages between the users and the servers without entering the passwords in untrusted kiosks.

2.2. 3G Connection

In the 3G connection data confidentiality of users' data and signal data is provided and also provides data integrity of signal data for avoiding any tampering attacks. Algorithms f8 and f9 are used to provide confidentiality and integrity respectively. These two algorithms are based on a block cipher named KASUMI. Thus this proposed authentication system utilizes the security advantages of 3G connection for registration and recovery procedures.

2.3. One-Time Password

The one time password in this system is generated by one-way secure hash function. With a given input *c*, a set of passwords are generated through hash chain by multiple hashing. Assuming we need *N* one-time passwords, the first of these is produced by performing *n* hashes on input *c*.

$$\mu_0 = ℌ^N(c). \quad (1)$$

The next one time password is obtained by performing *n-1* hashes

$$\mu_1 = ℌ^{N-1}(c). \quad (2)$$

Hence, the general formula is given as follows:

$$\mu_i = ℌ^{N-i}(c). \quad (3)$$

For few security reasons the one-time passwords are used in reverse order i.e., μ_{N-1}, then μ_{N-2} and so on. Even if an old password is hacked, the attacker is unable to drive the next one. The input *c* is derived from a long-term password (L_P) and identity of server (ID_s) and a random seed (ϕ) generated by server.

3. Problem Definition and Assumption

In this part we first define the problems that are faced by the present user authentication techniques and systems and then we give a description of our proposed system architecture.

3.1 Problem Definition

Nowadays people more often tend to use Internet as a daily activity can easily be achieved through many web services. Web services provide many enriched application like online banking, e-commerce, social networking and many more. But the main problem is that all these web services provide user confidentiality only by providing a text password authentication which has many disadvantages.

The main cause for intruders to use our accounts is because users generate their own passwords. To make them easy to remember users usually tend to use a weak password for all websites that will be easily remembered by them so that they can easily be recalled. Due to this there is a relative chance of causing a domino effect [2]. Any intruder who gets hold of a user's password from any weak website, they tend to use them around different websites for revealing sensitive information like financial or bank accounts guessing that the user may have reused the password for different websites.

Another problem which is faced is that human are not great in memorizing complex and meaningless passwords. Even though many websites provide sufficient password management system by generating a complex password with sufficient high entropy users still change those passwords with a weak password which can be recalled.

In addition to this entire problem phishing attacks and malware are causing a threat for maintaining the user passwords a secret from the adversaries. Protecting a user password is inapplicable if keyloggers and backdoors are already installed in the kiosks. Now considering these threats for managing the passwords, user authentication via text passwords through browser is not a safe option.

Therefore we propose a system where the user is allowed to enter their password using a new component, the user cellphone and a new communication channel SMS channel is used for transmitting the secret information's between the user cellphone and the server. The security provided by the SMS channel is already mentioned in Section II. Based on this, user is authorized by the websites without entering their passwords in any untrusted kiosks. In this proposed system user just has to remember long-term password for accessing the cellphone. This is because to protect the information if the cellphone is lost.

3.2. Architecture

The basic architecture of the proposed user authentication system is describes in Fig. 1. In this system the components that are involved are the user cellphone, a browser on untrusted kiosks, and a web server that the user wants to interact with. The user interacts with the cellphone and the browser directly for a secure login purpose.

Fig. 1. Architecture of the proposed system

The communication between the user cellphone and the web server is maintained by the SMS channel. The web browser interacts with the web server via Internet. The user cellphone must interact directly with the web browser and this is accomplished by using a Bluetooth or a Wi-Fi connection interfaces which is present in the cellphone.

The assumptions 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. Hence, users can safely input the long-term passwords into cellphones.
3) The telecommunication service provider (TSP) will participate in the registration and recovery phases. The TSP is a bridge between subscribers and web servers. It provides a service for subscribers to perform the registration and recovery progress with each web service. For example, a subscriber inputs the id (ID_u) and a web server's id (ID_s) to start to execute the registration phase. Then, the

TSP forwards the request and the subscriber's phone number (T_u) to the corresponding web server based on the received ID_s.

4) Subscribers (i.e., users) connect to the TSP via 3G connections to protect the transmission.
5) 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 T_u sent from the subscriber.

If a user loses her cellphone, they can notify their TSP to disable the 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.

4. Overview

In Fig. 2. The operation flow overview is shown; the black rectangles indicate the extra steps that are different from other user authentication system. In this system there are mainly three phases that the user has to pass through- registration, login and a recovery phase.

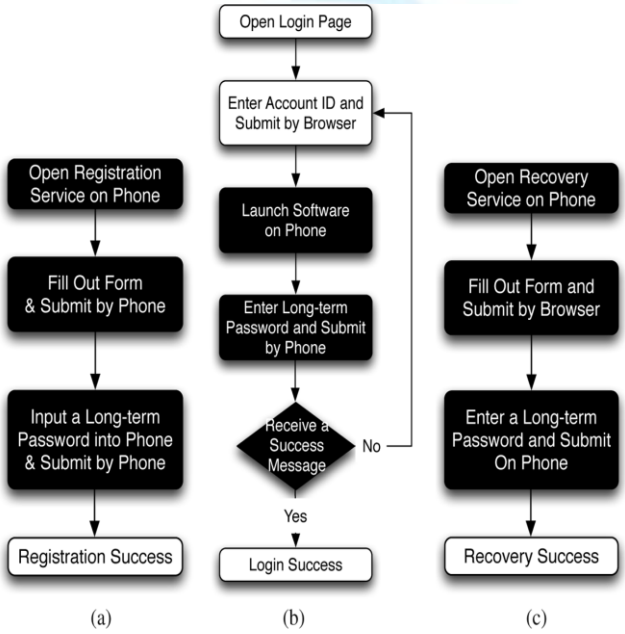

Fig. 2. Operation flow overview for user in each phase of the system respectively (a) registration (b) login (c) recovery

In the registration phase the subscriber (i.e., user) starts the program by registering a new account for a preferred web server. The difference in this system from other conventional registration system is that the server requests the user's id and the phone number, instead of the password. The registration form is filled up through the users' cellphone. After filling out the form the user is prompted to set a long-term password. This long-term password is used to generate a set of one-time passwords that are use for future login purposes. This registration message is sent to the server using a SMS channel. The information of the registration is encrypted to provide data confidentiality. The system also designed to enable the user to have a recovery phase, in some conditions where the user may lose their mobile and still need to login using the same user id from their new cellphone.

Unlike other systems in the login phase the user is not prompted to enter their password in the browser instead the user is enabled to enter their passwords in their cellphone. The only information the user has to enter in the browser is their username. The user enters the long-term password in the cellphone which in turn generates a chain of one-time passwords which are sent to the server securely to the server through SMS. The login SMS is also encrypted for providing security. Finally, the cellphone receives a confirmation message that the authentication is successful. This message is also used to ensure that the website is legal or a phishing website. Brief description of each phase is given below. Table 1 shows the notations that are use in the system design.

4.1. Registration Phase

The main goal of the registration phase is to provide the user and the server a shared secret authentication so that the server can authenticate the user in the future. The user starts the registration phase by entering the preferred user ID_u and the server ID_s (website URL) to the program. Then the program sends the ID_u and ID_s to the telecommunication service provider (TSP) for making a registration request. Once it receives the request the TSP traces the users' phone number T_u using the SIM number. It also plays a vital role in sharing a shared key between the user and the

server. This shared key K_{sd} is used to encrypt the SMS for registration with ABS-CBC now the TSP and the server *S* establishes a SSL tunnel for protecting the communication in-between. Then the TSP forwards the ID_u, T_u and K_{sd} to the server *S*. Then the server generates the corresponding information for the account and replies a response including its identity ID_s, random seed ϕ, and its phone number T_s. The TSP forwards these along with the shared key K_{sd} to the user cellphone. Now the user sets a long-term password L_P. Using this secret credential *c* is computed by the following way:

$$c = ℌ (L_P||ID_s||\phi) \quad (4)$$

To have a secure registration SMS, the cellphone encrypts the secret credential and the shared key K_{sd} and generates the corresponding MAC, i.e., $HMAC_1$. The cellphone sends the encrypted registration SMS to the server by its phone number T_s. The encrypted SMS contains the following:

$$\text{Cellphone} \rightarrow \text{S: } ID_u, \{c||\phi\}_{Ksd}, IV, HMAC_1 \quad (5)$$

Server *S* compares the source of received SMS with T_u to prevent SMS spoofing attacks. At the end of the registration the user cellphone stores all the information $\{ID_s, T_s, i, \phi\}$, except the long-term password L_P and the credential c. Variable *i* indicates the current index of the one-time passwords and is initially set to 0. With *i*, server can authenticate the valid user each time the login. After receiving the SMS (5) the serve stores $\{ID_s, T_s, c, i, \phi\}$ and then completes the registration.

TABLE 1: Notations

Notation	***Description***
ID_x	Identity of entity *x*.
T_Y	Entity *y*'s phone number.
K_{sd}	Shared secret key between user and the server.
L_P	User's long-term password.
c	Secret shared credential between user and the server.
μ_i	i^{th} one-time password.
Φ	Random seed.
N	Pre-defined length of hash chain.
n_z	Nonce generated by entity *z*.
ℌ(o)	Hash function with input o

4.2. Login Phase

The login phase begins when the user sends a request to the server *S* through an untrusted browser. The user uses the cellphone to produce a one-time password, e.g., μ_i, and deliver necessary information encrypted with μ_i to server *S* via an SMS message. Based on pre shared secret credential *c*, server *S* can verify and authenticate user based on μ_i.

The login procedure starts by accessing the desired website via a browser on an untrusted kiosk. The browser sends a request to with user's account ID_u. Next, server *S* supplies the ID_s and fresh nonce n_s to the browser. 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 like ϕ and *i*. The next step is promoting a dialog for the user to enter the long-term password L_P. Secret shared credential *c* can regenerate by inputting the correct L_P on the cellphone. The one-time password for current login is recomputed using the operations which are discussed in Section II.

μ_i is only used for this login (i^{th} 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 μ_i and generates the corresponding MAC, i.e., $HMAC_2$. The next action on the cellphone is sending the following SMS message to server:

$$\text{Cellphone} \rightarrow \text{S: } ID_u, \{n_d||n_s\}_{Ksd}, IV, HMAC_1 \quad (6)$$

After receiving the login SMS, the server recomputes μ_i 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, $\int (n_d \| \mu_i)$, 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 fails, the device would not increase the index *i*. If the user is successfully log into the server, index *i* 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 ϕ by the *recovery* phase to refresh the one-time password.

4.3. Recovery Phase

Recovery phase is designated for some specific conditions; for example, a user may lose their cellphone. The system will be still able to recover the setting in the new cellphone assuming the user still uses the same phone number (apply a new SIM card with old phone number).

Once user installs the program in the new cellphone, they can launch the program to send a recovery request with their account ID_u and requested server ID_s to predefined TSP through a 3G connection. As we mentioned before, ID_s can be the domain name or URL link of server *S*. Similar to registration, TSP can trace the phone number T_u based on the SIM card and forward the account ID_u and the T_u to server through an SSL tunnel. Once the server *S* receives the request, *S* 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 *S* generates a fresh nonce n_s 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.

When the mobile program receives the message, like registration, it forces the user to enter her long-term password L_P to reproduce the correct one-time password μ_{i+1} (assuming the last successful login before lost her cellphone is μ_i). During the last step, the user's cellphone encrypts the secret credential *c* and server nonce n_s to a cipher text. The recovery SMS message is delivered back to the server *S* for checking. Similarly, the server *S* computes μ_{i+1} and decrypts this message to ensure that user is already recovered. At this point, the new cellphone is recovered and ready to perform further logins. For the next login, one-time password μ_{i+2} will be used for user authentication.

5. Conclusion

In this paper, we have proposed a user authentication system that can be used to prevent from password stealing and password reuse attacks by using new components i.e., the user cell phone and SMS. This system is based on the assumption that each website posses a unique phone number like the user phone number and also that telecommunication service provider participates in the registration and the recovery phases of the system. The main principle of this user authentication system is that to eliminate the negative human factors as much as possible. By using this system, the user has to just remember the long-term password that they enter so as to protect the cell phone. This system eliminates the password entry by the user in any of the web browsers. Compared to other user authentication systems, our proposed system is first to prevent password stealing attacks and also reuse attacks simultaneously. There is a reason why one time password mechanism is used in this system, so as to ensure login independencies. This system also has a recovery procedure when a user loses the cell phone. They can still login into the accounts from new cell phone with reissued SIM card with the same phone number and also knowing the long-term password

References

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

[2] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of the password reuse" (APR 2004)

[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] I. 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] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient method for securely managing passwords," in WWW '05: Proc. 14th Int. Conf. World Wide Web, New York, 2005, pp. 471–479, ACM.

[7] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and thememorable space of graphical passwords," in SSYM'04: Proc. 13th Conf. USENIX Security Symp., Berkeley, CA, 2004, pp. 10–10, USENIX Associateion.

[8] R. Dhamija, J. D. Tygar, andM. Hearst, "Why phishing works," in CHI '06: Proc. SIGCHI Conf. Human Factors Computing Systems, New York, 2006, pp. 581–590, ACM.

[9] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters," in *Selected Areas Cryptography*, 2003, pp. 175–193, Springer.

[10] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin "oPass: A user authentication protocol resistant to password stealing and password reuse attacks" (APR 2012.