Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Enhanced Authentication Mechanism Against Untrusted Access and Phishing Attacks Using USSD

A Aswathy Nair [*]
Department of CSE,
SJCET ,Kottayam, Kerala, India

Saran Thampy D
Assistant Professor, Dept of CSE
KVM College of Engineering and IT, Alappuzha, Kerala, India

Abstract— Text passwords entered through personal computers is the most commonly used internet authentication for end user transactions such as online banking, e-commerce etc, due to its convenience and simplicity. Personal computers are preferred by most of the users than personal handheld devices for transactions, due to features like screen size and keyboards. However use of text passwords and typing them directly to computers are prone to be stolen and compromised under different threats and vulnerabilities like keylogging, phishing, and pharming. Such attack can extract user identity and sensitive account information allowing account access. In this paper, we propose a simple approach to overcome such attacks, which provides two modes of authentication. In low mode, normal text password is used and there by user indicates the server that user is in an untrusted environment which restricts the user's action. In high mode, the user's text password input is separated cryptographically from the client PC and the user has full access to all the services. The user's secret key is input through an independent personal trusted device such as a cellphone which makes it available to the PC using a telecommunication facility called Unstructured Supplementary Service Data (USSD). This proposal is intended to safeguard passwords from the attacks mentioned above, as well as to provide transaction security to foil session hijacking.

Keywords— Authentication, Keylogging, Pharming, Phishing

I. INTRODUCTION

Now a days most of the people rely heavily on internet since most of the activities are available on internet and the primary means of user authentication for websites is the text password. In this current Internet environment, most of the computers are infected with one or more forms of spyware or malware. Malicious administrators of such computers, and even users who are able to install rogue applications, can easily compromise a user's session and gain unauthorized access to private data. Along with common malware and spyware, software keyloggers are typically installed on a user PC. An increasing number of phishing sites also install keyloggers on user PCs, even when users do not explicitly download or click any link on those sites. Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even though many secure authentication protocols have been proposed, passwords are still the most commonly used technique for online authentication even in such an unsecure environment. The potential damage is worser in cases where passwords are used as authenticators, because the user's authenticator can be compromised and saved for later use. Thus passwords has become a prime target of attackers, who are economically motivated exploits including those targeting online bank accounts and identity theft.

Online banking is the service that is providing by the banks, using which users can access the financial services offered by the banks using a PC with an internet connection and without the need to visit the user's bank. This means of access to banking services through internet has gained popularity since its introduction and almost all commercial banks in the country have internet banking facilities offered to their customers. The Online banking requires only a userid and password for authentication. Users input these credentials to a bank website to access their accounts. An attacker can easily collect these long-term secrets by installing a keylogger program on a client PC, or embedding a JavaScript keylogger on a compromised website. As plaintext sensitive information is input to a client PC, malware on the PC has instant access to these long-term passwords. Reusable userid-password pairs can be collected by using phishing attack, even if a user's PC is malware-free. Besides text passwords, there are several other forms of authentication mechanisms which are either used alone or in combination with text passwords. A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface. It is easier than a text-based password for most people to remember. Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words. Even though graphical password is a better authentication mechanism, it is not yet mature enough to be widely implemented in practice and is still vulnerable to several attacks. Three-factor authentication is a more reliable user authentication mechanism than text passwords. 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 token, and scan his/her biometric features (e.g., fingerprint or pupil). Three-factor authentication is a comprehensive defence mechanism against password stealing, but it requires comparatively high cost. Another more attractive and practical approach than three-factor authentication is the two-factor authentication which is commonly used in banks. But it still suffers from the negative influence of human factors, such as the password reuse attack.

In this paper, we propose a user authentication protocol that utilizes the user's cell phone for logging in to websites, preventing the user from typing password directly into the computer. The system consists of two modes of authentication, a low mode and a high mode. In low mode, normal user id and text password is used. This mode indicates the server that user is logging in from an untrusted environment there by restricting the user's action. In this mode user is not allowed to enjoy the full services offered by the server. In high mode the text password is input by the user through user's cell phone using the telecommunication service called USSD. This mode is used in case where user needs to access all the services even in unsecure environments.

II. Related Work

The internet is a global network which is intrinsically insecure. Security threats arising from denial of service attacks, spoofing, sniffing, hacking, keylogging, phishing, virus, forms of malware etc causes risk to the internet users who perform the online transactions. It is imperative that strong security measures should be implemented which can adequately address and control these types of risks and security threats. The service providers like banks should provide the assurance that online login access and transactions performed over the internet are adequately protected and authenticated. Internet banking systems must authenticate users before granting access to particular services.

More precisely, the banking system must determine whether a user is, in fact, who he claims to be by asking the user to directly or indirectly prove knowledge of some sort of secret or credential. Based on the assumption that only an authentic user is able to do so, successful authentication eventually enables an authorized user to access his private information. The more security added to an authentication system, the lower will be the acceptance rate of users and the usability will decrease. It is a big challenge to find the most secure authentication system which is accepted by the users. Users always want new applications and features with easy to use interface. At the same time they are worried about the increasing dangers. Several authentication mechanisms were implemented and the most widely used authentication mechanism is the text password.

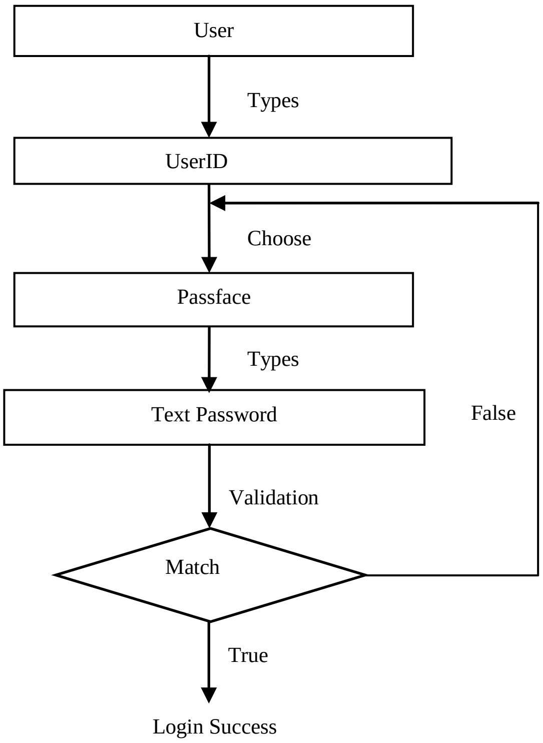

Fig 1: Graphical authentication using passfaces and text password

Alireza et al[2] proposed a graphical authentication system in combination with handheld devices like cellphone. In this system, the image and the click points in the corresponding image is selected during registration. The hint information such as the appropriate click points and their order which is selected during registration is sent to the handheld device like cellphone during the login phase. The hint information is transmitted to the device either through direct communication, photographic communication or indirect communications. This approach prevents the user from remembering the click points. But this approach has several disadvantages like shoulder surfing, pattern formation attack etc. Brickell et al[3] suggested an approach in which the server may be able to determine the trustworthiness of the client through remote attestation. The problem with these techniques is that they have not yet seen widespread deployment and also even if the server has determined that the remote platform is untrustworthy, it has no way of warning the user, thereby limiting the utility of these approaches.

Hung-Min et al[7] proposed an authentication system which leverages a user's cellphone and short message service to thwart password stealing and password reuse attacks. For users to perform secure logins to the web server on an untrusted computer, the user operates her cellphone and the untrusted computer directly. The communication between the cellphone and the web server is through the SMS channel. This approach prevents the password stealing attack, password reuse attack and the phishing attack. The problem with this approach is that the communication channel used here is the SMS, which is not reliable and the timely delivery cannot be guaranteed. Also even if the user need only less access privilege like checking the balance, the user have to follow all these security steps for the successful login.

Ahmed et al[8] introduced a graphical authentication system which include the combination of pass face and text based passwords as shown in fig:1. At the time of registration, a graphical password is created by the user by first entering a picture he or she chooses and selecting the click points for the corresponding picture. For each click point, the user types a word or phrase that would be associated with that click point. The problem with this approach is that the user need to remember both the click points and the text associated with each click points.

III. USSD: An Overview

USSD is a session oriented GSM service that is used to send messages between a mobile phone and an application server in the network. It is much faster and cost effective than SMS and is not based on store and forward concept. Since it is a session based protocol, the session is needed to be allocated for each interaction. In USSD, direct communication is established between the sender and the receiver, which results in a faster data transmission. USSD [6] is fast emerging as the communication protocol, which can replace the dependency on SMS for quick messaging services like spreading awareness about epidemics and fatal diseases to the users, mobile banking using USSD, updating mobile software etc.

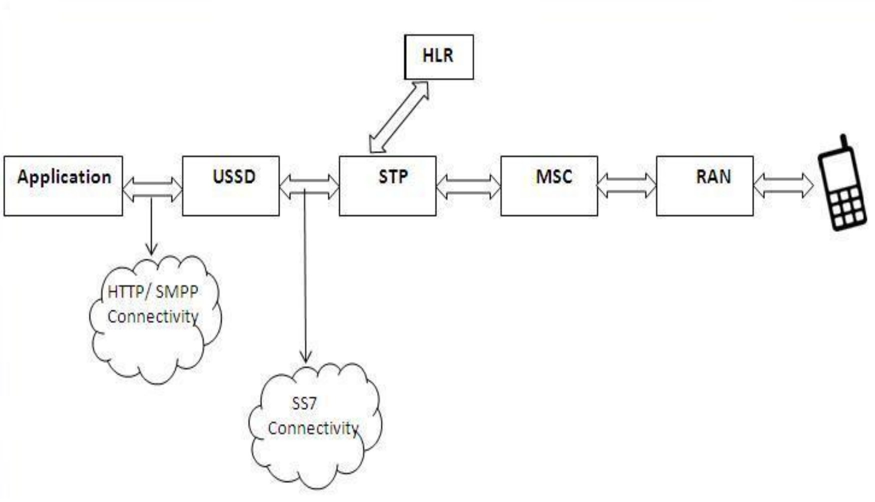

Fig 2: Network Architecture of USSD system

In USSD, a real time "session" is initiated between the mobile user and the USSD application platform when the service is invoked, allowing data to be sent back and forth between the mobile user and the USSD application platform until the USSD service is completed. The end-to-end data flow is across the encrypted GSM communication layer and the subscriber identity is also hidden. The data can also be encrypted as soon as it terminates at the USSD gateway sitting at the network operator, processor or bank, thus preventing any internal risk of misuse of data.

The first USSD services were called "Phase 1", or "MAP 1" and were only able to pass information from the handset to the USSD application with a confirmation. There was therefore no session held between the handset and the application. "Phase 2" (or "MAP 2") USSD added the capability for establishing a session instead of a once-off transaction. This meant that the handset and the USSD application could have the technical equivalent of a dialogue.

The network architecture for USSD system is as shown in fig2. USSD services reside as applications in the mobile network. These applications can reside in MSC, VLR, HLR, or an independent application server that is connected through a USSD Gateway (using SMPP). If a USSD message is not destined for an application in the MSC, VLR, or HLR, a USSD handler in these nodes routes the message to the USSD Gateway using the MAP protocol based on the service code. The gateway interprets the code and routes it to the specific USSD application server to fetch the necessary information requested by the user. In response, the application sends the relevant information to the USSD Gateway, which in turn converts the message to MAP format, and then sends to the mobile terminal. There are two modes of USSD implementation, the push service mode and the pull service mode. The Push Service Mode is the Network-initiated USSD service in which the network (MSC, VLR, or HLR) sends USSD message toward MS. The Pull Service Mode is MS-initiated USSD service with user sending USSD message toward MSC

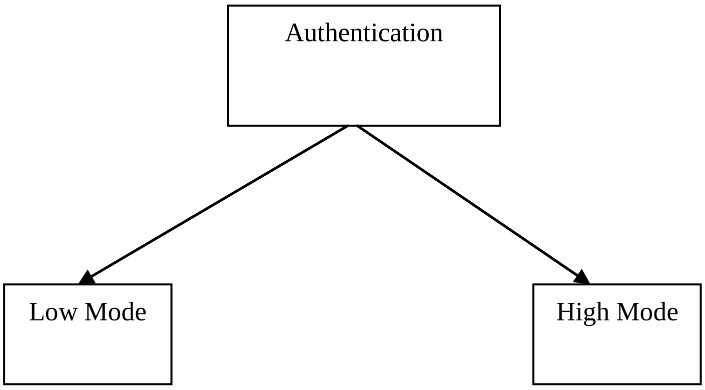

Fig 3: Authentication System

A USSD message can be up to 182 alphanumeric characters in length. Unstructured Supplementary Service Data allows interactive services between a MS and applications hosted by the Mobile Operator. These messages are composed of digits and the #, * keys, and allow users to easily and quickly get information/access services from the Operator. Another important fact about USSD is that messages from handsets always route to the home network. This means that in case of roaming in another network, then dialing a USSD string on the phone will always route to the application on the home network. Conversely, roaming subscribers from other networks cannot access USSD services on a host network.

IV. Proposed System

In this paper, we present a two type authentication system as shown in fig:3 for the same account of each user, a low mode and a high mode[4]. The first type which is the low mode, the user's privilege to access the services is restricted. This mode is used to login from unsecure environments. The authentication mechanism used in this mode is the normal text-based user name and password pairs. This mode does not prevents the session from hijacking. But it provides users with a convenient method that allows users to limit the capabilities of an authenticated session, thereby limiting the amount of damage that can be caused by session compromise.

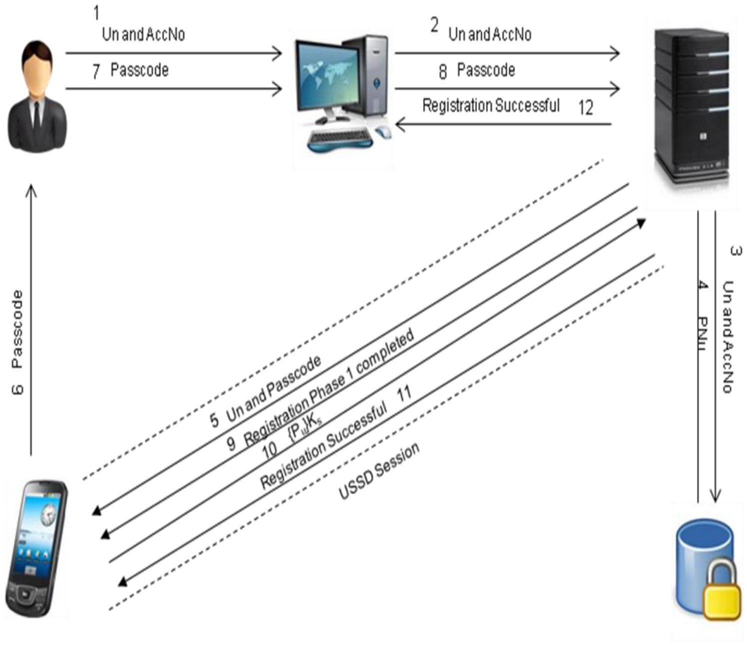

Fig 4: Registration Phase

In the second type which is the high mode, the user is privileged to access all the sevices and the user can login from both trusted and untrusted enviroments. The high mode adopts a more secure authentication system which prevents the user from typing the password directly in to the computer. This prevents the risk of password stealing, phishing attack etc. In this mode, the user's secret key is input through an independent personal trusted device such as a cellphone which makes it available to the PC using a telecommunication facility called Unstructured Supplementary Service Data (USSD). This proposal is intended to safeguard passwords from the attacks mentioned above, as well as to provide transaction security to foil session hijacking.

A. Low Mode

The users normally prefer the text passwords for authentication even in unsecure environments, due to the ease of use. In this authentication mechanism, each user registers with the system using a self declared or assigned username password pairs. Knowledge of the password corresponding to the username guarantees that the user is authentic. For each subsequent use, the user must know and use the previously declared password. The major drawback with the text password is that the password can often be stolen, accidentally revealed or forgotten. Hence text password authentication cannot be preferred for activities which need to be performed securely like bank transactions etc.

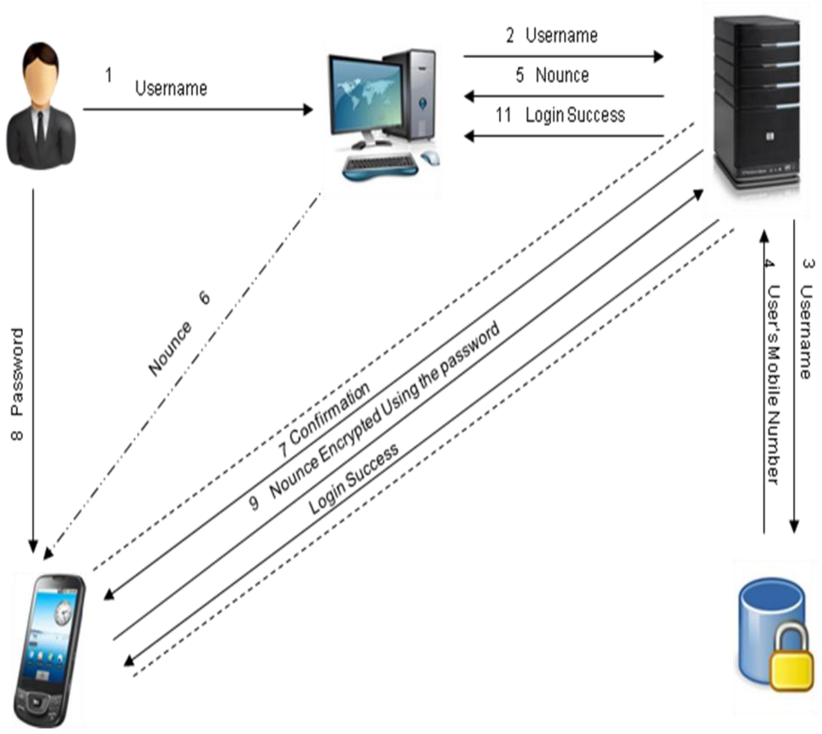

Fig 5: Login phase

In the proposed system, low mode is used for logging in from the untrusted environments like from internet café, public computers etc where computers may be infected with one or more forms of spyware or malware or may have key-loggers installed in it. The authentication mechanism used in this mode is the normal text passwords and the damage caused in case of password stealing etc is limited by restricting the user capabilities for the login session. For example, in a low mode associated with the email service, the user is allowed to access only the new unread mails and cannot access the read message, message saved in personal folders etc. In case of low mode associated with bank accounts, the financial transactions or access to financial records other than the account balance are restricted, there by restricting the damage caused to the user in case of password stealing or session hijacking. Login of user in this mode signals the server that the user is accessing the account from the insecure environment and there by limits the privileges of the user.

B. High Mode

When the user has to get full access to the services in both trusted and untrusted environment, the high mode is used. The authentication mechanism used here prevents the user from typing the password directly in to the computer by the use of cellphone[5].It is assumed that the user mobile number is registered with the bank during the opening of the account in the bank and a unique secret key is provided to user on request for netbanking. This mode consists of the following two phases:

1) Registration phase

During the registration phase as shown in fig4 the user selects the username (Un) and submits the account number and user's phone number (PNu) that is already registered with the bank to the server from the computer. The server after verification of the entered phone number and account number sends a passcode along with the username to the user's mobile through the push service mode of the USSD. The user types the passcode to the computer and the first phase of registration is completed if the typed passcode matches with the passcode send to the mobile. In the second phase the server request to provide the secret key provided by the bank and to setup a password(Pu). This password is encrypted with secret key (Ks) and is send back to the server. The registration is successful if the decryption of the password by the server is successful. A success message appears in the computer screen and in the mobile and the server exits the USSD session.The encryption and decryption is done using the AES algorithm. The AES algorithm which is a symmetric key cryptographic algorithm uses the secret key provided by the bank as the key for both encryption and decryption. \\

2) Login phase

In the login phase as shown in fig5, the user enters the username to the website from the computer through the browser. The server retrieves the user's phone number from the database and initiates an USSD session with the mobile. The server also generates a fresh nounce for the session and sends the nounce to the browser. The browser sends the nounce to the mobile phone through bluetooth or any wireless interfaces. The server prompts the user to confirm whether the user have a made a login attempt, through the initiated USSD session. The user confirms and sends the nounce encrypted with the password to the server. The encryption here is also done using the AES algorithm with the password provided by the user as the secret key. The server decrypts the received nounce and compares it with the previously generated nounce. If it matches, then the login is successful and the server terminates the USSD session with the mobile. The encryption and decryption used here is also done using the AES algorithm with the password provided by the user as the secret key.

V. CONCLUSION

In this paper we propose a user authentication protocol which includes two modes of authentication for the same account. In the first type which is the low mode, the user's privilege to access the services is restricted and is used to login from unsecure environments. In the second type which is the high mode, the user is privileged to access all the services and the user can login from both trusted and untrusted environments. The high mode leverages the cell phones and a communication mechanism, the USSD to prevent password stealing attack. This mode prevents user from typing any passwords into untrusted computers for login to websites. The USSD is a session oriented GSM service which is much faster than SMS, is used to send messages between a mobile phone and an application server in the network. The proposed approach safeguard password from the attacks such as password stealing attack, phishing attack as well as provides transaction security to foil session hijacking.

REFERENCES

[1] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla.*SWAtt: Software-based attestation for embedded devi*ces. In Proceedings of the IEEESymposium on Security and Privacy, May 2004.

[2] Alireza Pirayesh Sabzevar and Angelos Stavrou, "*Universal Multi-Factor Authentication Using Graphical Passwords*," in IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008

[3] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In CCS '04: Proceedings of the 11th ACM conference on Computer and communications security, pages 132–145, New York,NY, USA, 2004. ACM.M.

[4] K. Bailey, A. Kapadia, L. Vongsathorn, and S. W. Smith. *TwoKind authentication: Protecting private information in untrustworthy environments*. In ACM Workshop on Privacy in the Electronic Society (WPES'08),

[5] M. Mannan and P. van Oorschot, "*Using a personal device to strengthen password authentication from an untrusted computer*," Financial Cryptography Data Security, pp. 88-103, 2007.

[6] Janagoudar Sanganagouda, "*USSD: A Communication Technology To Potentially Oust Sms Dependency*," http://www.aricent.com/sites/www.aricent.com/files/pdf/Aricent_WhitePaper_USSD_0911.pdf

[7] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin," *oPass: A User Authentication Protocol Resistant toPassword Stealing and Password Reuse Attacks*", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012

[8] Ahmad Almulhem, "*A Graphical Password Authentication System*," in 978-0-9564263-7/6/$25.00 IEEE, 2011

[9] L. Lamport, "Password authentication with insecure communication,"

[10] *Commun. ACM*, vol. 24, pp. 770–772, Nov. 1981.

[11] USSD Demo for mobile banking, "*http://www.icicibank.com/Personal-Banking/onlineservice/mobile-banking/USSD-demo.html*"

[12] K. J. Hole and V. Moen and T. Tjostheim. Case Study: *Online banking Security*. IEEE Security & Privacy Magazine, 2006.

[13] M Zviran, WJ Haga, "*A comparison of password techniques for multilevel authentication mechanisms*", in Computer Journal v 36 no 3 (93) pp 227-237

[14] Mobile Banking Technology Options, "http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2012/06/finmark_mbt_aug_07.pdf, August 2007