IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 4, Aug-Sept, 2013
ISSN: 2320 - 8791
www.ijreat.org

A Survey Paper On User Authentication

ArunKumar.Kasa[1], Sai Ashritha.K[2]

[1,2] **Department of Computer Science and Engineering,**
CMR Institute of Technology, Hyderabad, Andhra Pradesh.

Abstract

The password is used to spot the valid user for a specific system. Text password is the most popular form of user authentication. Today user passwords square measure taken from the third party that causes totally different threats and vulnerabilities. Typing the passwords intountrusted computers suffers password thief threat and selecting a weak password, reusing it across totally different websites may also cause threat. This paper focuses on numerous authentication techniques available and their performances and offersa brief information on an authentication protocol that authenticates the user employing a one-time password generated randomly and communicated to the user either as a mail service or by exploitation short electronic communication system.

Keywords:*Authentication, public and private keys and security.*

1.Introduction

Authentication could be a Greek word which suggests the act of conforming an act of truth of a knowledge or an entity. The aim of the user authentication is to secure their information from separation by the third party. Authentication is any protocol or method that allows one individual to ascertain the identity of another individual.

Generally authenticated fall into three categories, based on what is known as the factors of authentication: (i)Onething the user is aware of (knowledge) (ii) Onething the user has (ownership) and (iii) Onething the user is (inherence). Now let us see a basic login authentication processstep as follows:

1. A client requests access to a protected resource.
2. The web server returns a dialog box that requests the user name and password.
3. The client submits the user name and password to the server.
4. The server validates the identifications and, if successful, returns the requested resource.

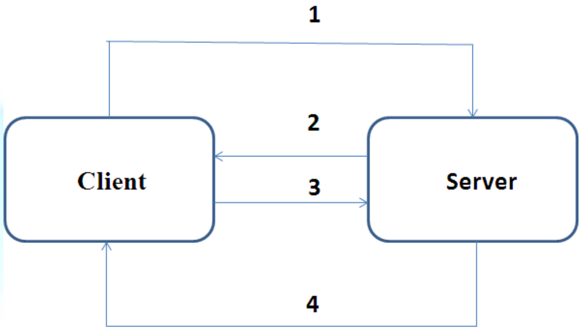

Figure: 1 One Basic login authentication process

Authentication is a fundamental aspect of system security. It confirms the identity of any user trying to log on to a domain or access network resources. Text password is the most popular form of user authentication on websites due to its convenience and simplicity. Passwords are prone to be stolen under different threats and vulnerabilities. Hence an authentication protocol which protects the user(s) password from various threats has been used. There are two basic authentication types they are non-repeatable (proof of origin cannot be denied arebiometrics, retinal images) and reputable.

1.1 Different methods of Authentication

(i) Digital signatures:A digital signature is associate degree electronic signature that can be used to authenticate the identity of the sender of a message and probably to make sure that the initial content of the message or document that has been sent is unchanged. Digitalsignatures are simplytransferable, cannot be imitated by someother person, and might can be mechanically time-stamped.

(i) One-Time Password: One-Time Password (OTP) system is a Two-Factor Authentication system where the password constantly alternates. This greatly reduces the risk of an unauthorized intruder gaining access to the account.

(ii) Public Key Cryptography: Refers to a cryptographic system requires two separate keys, one amongst that is secret and the other public. One key lock or encrypts the plaintext, and also the different unlocks or decrypts the cipher text.

There are different protocols used by the authentication are secure remote password protocol(SRP),authentication and key agreement(AKA),extensible authentication protocol(EAP) and Kerberos. Day by day the usage of net is increasing quickly and also the number of threats or attacks are increasing to avoid several new techniques for authentication have been introduced one among them is one time password method.During this survey on user authentication we tend to discuss totally different authentication techniques and how to protect our passwords from stealing to some extent using an authentication method called one time password.

This paper is organized as follows In section 1 Different methods of Authentication. In section 2 related literature surveys on existing research paper. Final conclusion in section 3.

2. Literature Survey

B. Ives et al. [1]Proposed an alternative security scheme.This can be done by both public and private keys In public-key encryption (PKE) the user is authenticated by the private key used to encrypt a message to the server. While similar to a password, the private key has two structures that increase its security.

1. The private key is stored on a client computer or smart card and can be of considerable length, thus eliminating the need for the user to memorize the code while also avoiding the possibility of the user generating an easy to guess the code.

2. The server verifies the code by correctly decrypting certain information sent by the client rather than comparing to a password file thus eliminating any server-side storage of password(s), encrypted or not. However, a user's private key must be protected on the client side, thus changing the location of a potential theft.Public-key infrastructure (PKI) uses PKE to authenticate users across a number of different applications or systems and also it allow a user to have a single private key that can be used across some or all of the user's needs, simplifying key management for the user. In this situation, loss of the user's private key can make several or all of the users' systems vulnerable in a similar way as when a user chooses the same password to enter for multiple systems. On the other hand, during this case, largerprominencecould also be placed on ensuring the system is tuf to penetrate with responsibility for the key remaining within the hands of the user. Further, a technique of centrally revoking a key will be place insituation so a stolen key can be quickly disabled for all systems. And it eliminates the necessity for the user to memorize the code whereas additionally avoiding the likelihood of the user generating a straight forward to guess code and also the PKI systems are thus tuf to use so poorly enforced, they are sometimes viewed as vain.

S. Gawandet al. [2] discussed a survey of how users manage passwords for online account(s), password practice(s), quantifying password reuse and also surveying the contributing factors to this reuse. Technical solutions for online password management wil improve observe and while not considerably ever changing user behavior. This can be in distinction to alternatives for ancient authentication systems. These alternatives would possibly place confidence in the user having a specific device like a cellullar phone or a physical token like a smart card. Once users access website accounts, they have alreadygot their hands on a computer. We able to develop systems at the appliance level or at the browsers particularly rather than at the device level. Theyprincipally claim that from a sensible purpose of read is that the extent of password reuse and its doubtless to become a lot of problematic over time as people accumulate more accounts and having a lot of accounts implies more password reuse.

D. Florencio et al.[3] Approach could be a higher means that to handle bulk attacks. Here the combined size of the user ID plus password key-space is considered rather than the password key-space alone that protects massive establishments against bulk estimationattacks.It reduces the quantity of break-ins that an attacker with fixed resources can expect, and reduces the burden on users however there is selection bias: we have information solely from users who downloaded the toolbar. These users will be expected to be much more active than the general web using population.

Jermyn et al. [4] Planned a replacement new graphical password scheme that exploits features of graphical input displays to relizehigher security than text based passwords. Here we tend to area unit primarily intended by devices like personal digital assistants (PDAs) that supply graphical input capabilities via a stylus, and prototype implementation of our password schemes on such a PDA, specifically the Palm PilotTM. Therefore, it is safer compared to text based passwords.However, here during this technique it needs extra space and also the server must store the seeds of the portfolio images of every user in plain text. Also, the method of choosing a set of images from the picture database may be tedious and time intense for the user.

S. Chiasson et al. [5] Outlined on multiple passwords using text and also click based graphical passwords. However, individuals usually have difficulty in remembering multiple passwords and additionally there is an oppourtunityof users reuses the equivalent password for various systems or reveals alternative passwords as they struggle to log in. Thus multiple click based passwords are used in order to avoid the problems of multiple text based passwords which are easy to remember or recall and click-based graphical passwords were significantly less prone to multiple password interference within the short, whereas having comparable usability to text passwords in most alternative respects. During this methodology there is associateoffset of the graphical passwords' inbuilt memory cue, that may be a safer memory aid than others.

Perrig et al. [6] Planned a completely unique methodology to use hash visual image to boost the real-world security of root key validation and user authentication. So as to boost the protection of the systems is to use hash visual image, a method that replaces pointless strings with structured pictures. Here we analyze two human limitations: Firstly difficulties people have with remembering strong passwords and personal identification numbers (PIN).Second with examination unimpoatant strings. We tend to use hash visual image to getpictures from the strings, and also the user will merely compare the photographsrather than the strings. This can beimage recognition that is simple compared to actual string recall and all the images generated by Random Art are regular, is firm.

H. Krawczyk[7] presents how cryptography is employed in today(s)web for implementing a secured channel between two end points and so exchange data over that channel. Typical implementations initial call a key-exchange protocol for establishing a shared key between the parties, and so use this key to authenticate and encrypt the transmitted data exploitation (efficient) symmetric-key algorithms. The three most popular protocols that follow this approachsquare measures SSL, IPsec and SSH. So its Straight forward and quick to implement and it has too many keys, a new shared key has got to be generated for communication with each completely different party. This creates a drag with managing and ensuring the security of these keys and loss of the private key is irreparable.

S. Garfinkel et al. [8] Discusses a novel strategywherever individuals more and more have faith in public computers doing business over the net. However accessing today's web-based email, on-line auctions, or banking sites invariably needs writing a username and password to prove one's identity to the remote service. This creates significant security vulnerability since the user's password may be captured by the computer and later reused by a hostile party. So as to avoid this we tend to use a portable as a handheld authentication token, and a security proxy that permits the system to be used with unmodified third-party net services.

Firstly, a user (U) that needs to use a Internetkiosk (K) to access a remote service (R) requiring authentication would instead connect with sure security proxy (P). The proxy mediates all aspects of the user(s) communication with the remote service, stores username and password and may use credentials to log in to R. P additionally stores a portable range for every user. And it creates a system that is both secure and highly usable.

3. Conclusion

This paper offers the detailed analysis of password authentication. From this detail literature survey we have a tendancy to feel that there is a necessity to possess a secured password authentication technique to avoid from password stealing and use attacks, that we would be attempting in our future dissertation work.

4.References:

[1] B. Ives, K. R. Walsh, and H. Schneider "The dominoeffect of password reuse,"commun.ACM,vol.47,no.4,pp.75-78,2004.

[2]S.Gaw and E.W.Felten,"password management strategies for online accounts," in SOUPS '06':proc.2symp.usable privacy. security, new york,2006,PP.44-55 ACM

[3]D.Florencio and C. Herley,"A large scale study of web wide web New York, 2007 pp.657-666, acm.

[4] I.jermyn,a.Mayer,f.monrose,m.k.reiter and a.dRubin, "The design and analysis of graphical passwords," in ssym'99':proc.8thconf.USENIXsecuritysymp.,Berkeley,ca, 1999,pp.1-1,usenix association.

[5]S.Chiasson,A.forget,E.stobert,A.c.vanOorschot and R.biddle "multiple password inference 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.

[6]A.Perrig and D.Song "hash visualization: a new technique to improve real world security," in proc .int.workshop cryptographic techniques E-commerce, citeseer, 1999 pp.131-138.

[7]H.karwczyk "The older of encryption and authentication of protecting communications (or: how secure is ssl?)," in advances cryptology—CRYPTO 2001, 2001, PP.310-331.

[8]M.wu,S.Garfinkel,andR.Miller "secure web authentication with mobile phones," in DIMACS workshop usable privacy security software ,citeseer,2004.