JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Volume-3, Issue-1 E-ISSN: 2347-2693

A Survey on User Authentication Protocols

Prajitha M V

Dept. of CSE, Royal College of Engineering and Technology, Akkikavu, Kerala, India
Prajitha.mv@gmail.com

www.ijcaonline.org

Received: Dec /16/2014 Revised: Dec/28/2014 Accepted: Jan/16/2015 Published: Jan/31/2015

Abstract---Passwords are the powerful tools that tend to keep all data and information digitally safe. It is frequently noticed that text password remains predominantly popular over the other formats of passwords, due to the fact that it is simple and expedient. However, text passwords are not always sturdy enough and are very easily stolen and misused under different vulnerabilities. Other persons can obtain a text password when a person creates a weak password or a password that is completely reused in many sites. In this condition if one password is hacked, it can be used for all the websites. This is called the Domino Effect. Another unsafe situation is when a person enters his/her password in a computer that is not trust-worthy; the password is prone to stealing attacks such as phishing, malware and key loggers etc. Among the most significant current threats to online banking are keylogging and phishing. These attacks extract user identity and account information to be used later for unauthorized access to user's financial accounts. This paper focuses on user authentication protocols which are used for secured online processing like online banking. During recent years numbers of authentication protocols are proposed in this area. For further researches, understanding of these approaches is essential.

Index Terms — Network Security, User Authentication, Password Reuse Attack, Password Stealing Attack

I. INTRODUCTION

One of the ancient ways to prove identity or gain access to a resource is passwords. A password is nothing that consists to be of any secret word or string of characters that is used for authentication purpose. A typical computer user may require passwords for many purposes: logging in to server accounts, retrieving the emails, accessing programming codes, databases, networks, web sites, and even reading the newspapers online. As humans are not experts in memorizing passwords they easily forget the passwords and these users firstly often select weak passwords and reuse the same passwords across different websites. Regularly reusing passwords causes a domino effect; when an adversary compromises one password, they will use it to gain access to more websites. Second, entering passwords into untrusted devices suffers password thief threat. An adversary can begin several password stealing attacks to snatch passwords, like malware, phishing, and keyloggers.

Password based user authentication has a major problem that humans are feel hard to keep those passwords in memory. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might not be secure. Another crucial problem is that users tend to reuse passwords across various websites. Reusing of password causes users to lose sensitive information stored in different websites if a hacker compromises one of their passwords. This attack is called as the password reuse attack. The above problems are occurred by the negative influence of human factors. Therefore, it is significant to take human factors into consideration when designing a user authentication protocol.

In order to reduce the negative influence of human factors in the user authentication procedure, the researchers have investigated a variety of technology. Since humans are more adept in remembering graphical passwords than text passwords, many graphical password technologies were designed to address human's password recollect problem. An alternative method is using password management tools. These tools automatically generate strong passwords for each website, which resists password reuse and password recall problems. The benefit is that users only have to remember a single 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 significant drawbacks. Although graphical password is a great idea, it is not mature enough to be widely implemented in practice and is still vulnerable to more attacks. Password management tools work well; however, general users have doubt about its security and thus feel uncomfortable about using it. Furthermore, they have problem using these tools due to the lack of security knowledge.

II. PASSWORD ATTACKS

A. Brute Force Attack

In this type of attack, all possible combinations of password apply to break the password. The brute force attack is generally applied to crack the encrypted passwords where the passwords are saved in the form of encrypted format. Early Linux systems were using MD5 hashing schemes for storing the password. There is a password file in the operating system which contains the user's passwords with user names. If the password file is stolen by the attacker then the password can be caught. The original form of password is not in the file but it is encrypted by MD5 hash. The encrypted password looks like safe but in fact it is also vulnerable to brute force attack. For this, the attacker first tries to convert all combinations of passwords into their MD5 hashes. In order to crack the password the attacker first extracts the MD5 hash of suspected password from the password file placed in the system. The hash is then matched with hashes individually. When the hashes are matched, the corresponding password is got.

B. Dictionary Attack

This type of Attack is relatively faster than brute force attack. Unlike checking all possibilities of words using brute force attack, the dictionary attack tries to a match the password with most going on words or words of daily life usage. Most users generally write passwords related to the names of birds, familiar places, famous actor's names etc. These passwords can be judged by the dictionary attack. The attacker create the dictionary of most commonly used words that might have been be used as a password. The attacker then applies all of these words to crack the password. Although the dictionary attack is faster than brute force attack, it has some drawbacks too. i.e. brute force attack contains limited words and sometimes it is unable to crack the password because it remains a possibility that password to be cracked may not be present in the dictionary itself

C. Shoulder Surfing

Shoulder Surfing is an alternative name of "spying" in which the attacker spies the user's movements to get his/her password. In this kind of attack, the attacker observes the user; how he enters the password i.e. which keys of keyboard the user has pressed.

D. Replay Attack

The replay attacks are also known as the reflection attacks. It is a method to attack challenge response user authentication mechanism (Same type of protocols by each sender and receiver side for challenge And response). The mode of this type of attack is that the attacker first enters his/her name in first login connection. To authenticate the user, the receiving device sends the challenge to the sender (in this case attacker). The attacker opens an alternative login at the same time with its own valid user name and replies the receiving device as challenge of previous connection. The receiver side accepts the challenge and responds to it. That response sends back by the attacker through the account to be hacked and thus it gets authenticated. Then the attacker gets the permission to access that account

E. Phishing Attack

It is a web based attack in which the attacker redirects the user to the fake website to get passwords/ Pin codes of the user. To explain Phishing, assume a user wants to open website say "www.yahoo.com". The attacker readdresses the user to a different web site e.g. "www.yaho0.com" whose interface is comparable to it of the initial web site to masquerade the user. The user then enters the login information which is retrieved by the attacker. The attacker then transmits the user to the original website and logins the user with the original website. Nowadays different phishing control filters are used, but still they are not much reliable.

F. Key Loggers

The attacks through key loggers are similar to the login spoofing attacks discussed above. They are also called as the key sniffers. The key loggers are software programs which monitors the user actions by recording each and every key pressed by the user.The attacker tries to put in the key logger software into the user system, either by putting in that computer code himself or by tricking out the user to click to install that file into his/her system. The key logger then makes the log file of the keys pressed by the user and then sends that log file to the attacker's e-mail address. The attacker then gets the user's password and can access to the target system.

G. Malware Attack

Malware, short for malicious software, is software used to disorder computer functinalities, gather secured information, or gain access to the private computer systems. It will seem within the kind of programming code, scripts, active content, and different software package. Malware is a general word used to refer to a variety of forms of aggressive or intrusive software. The greater part of active malware threats are usually worms or trojans rather than viruses.

H. Video Recording Attack

In such type of attack the attackers with the help of camera equipped mobile phone or miniature camera, analyzes the recorded video of authenticated users which enters password to their computer. In this user's password entry operations are recorded once or twice.

III. AUTHENTICATION METHODS BASED ON PASSWORD

A. One Factor Authentication

Inorder to reduce the negative influence of human factors in the user authentication procedure, there have a variety of technology. One method is *One factor authentication*, this is "something a user knows" (password)- not a secure method in the internet and banking world. Hackers have the option of using many techniques to steal this type of password.

B. Two Factor Authentication

To resolve the problem of one factor authentication a more attractive and practical approach *Two-factor authentication* (2FA) is adopted which requires the presentation of two or more of the three authentication factors: a knowledge factor ("something the user knows"), an owned factor ("something the user has"), and an inherence factor ("something the user is").Although there area unit range of banks that support two-factor authentication, however it still suffers from the negative influence of human characters, like the secret reusing attack. Users need to memorize another four digits PIN code to work together with the token, for example RSA SecureID. In this method also to remember the tokens are very difficult.

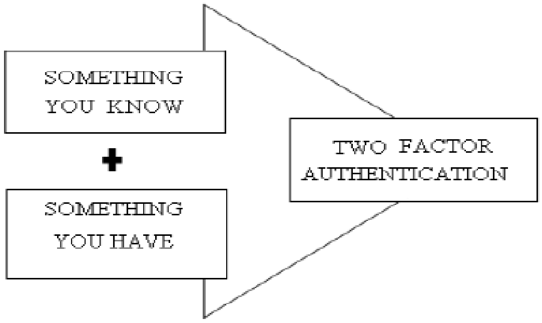

Figure 2.1: Two factor authentication

C. Three Factor Authentication

Three-factor authentication takes advantage of combination on three fators of authentication which includes what you know (password), what you have (ATM cards or tokens), what you are (biometrics). It is a comprehensive defense mechanism against password stealing attacks. 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. This provides superior security. The major drawback is though it provides high level security, because of its increased complexity and of comparatively high cost, this cannot be adopted in all environments.

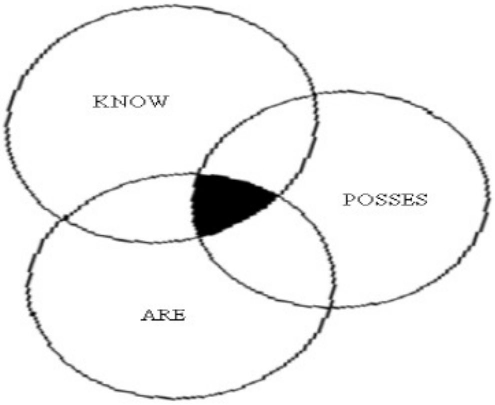

Figure 2.2: Three factor authentication

D. Biometrics

Biometrics is additionally used as authentication procedure during which the popularity is predicated upon image process. During this case to see a picture, it's first preprocessed to extract options from it so the image supported these extracted options is matched with the information. There are many sorts of biometry primarily based authentication i.e.

Finger print authentication
Face Recognition
Signature Verification
Speech Recognition
Iris recognition etc.

Advantages of such schemes embrace that it involves real and distinctive signatures and it cannot be purloined. The disadvantages includes that, it is pricey and tough to implement. It is still not mature and may be bypassed, also it's time taking method.

E. Graphical password

In this theme, the user first enters the user name to login. Afterward some graphical objects are displayed, that are necessary to be chosen by the user. These chosen objects are then drawn by the user mistreatment mouse, touch pad or stylus, touch screen etc. The system performs preprocessing on the user drawn objects and converts the sketches into hierarchal sort. Ultimately hierarchal matching is performed for user authentication.

Advantages enclosed reduced shoulder surfing and it is a safer authentication. Disadvantages embrace that the system verifies the user given that correct sketch is drawn by the user and touch sensitive screens are needed for sketching. Conjointly it depends upon the power of the user to draw sketches and its authentication time interval is far longer than alternative schemes.

F. Virtual password

This Novel password theme offers secure user's password in on-line environments . It will offer protection against totally different on-line attacks as phishing and password file compromise attacks.

G. One time password

To reduce the harm of phishing and spyware attacks, banks, governments, and alternative security-sensitive industries are deploying one-time password systems, wherever users have several passwords and use every password one time. A one-time password (OTP) may be a password that is valid for less than one login session or dealings. OTPs avoid variety of shortcomings that are related to ancient (static) passwords. The foremost necessary disadvantage that is self-addressed by OTPs is that, in distinction to static passwords, they aree not liable to replay attacks. this suggests that a possible intruder who manages to record an OTP that was already wont to log into a service or to conduct a dealings won't be ready to abuse it, since it 'll be now not valid. A reusable password is one that doesn't change for every authentication. a similar password travels across the network on every occasion the user authenticates. These passwords are liable to eavesdropping on the network. To combat these, one-time passwords (OTPs) were invented. These are passwords that are used precisely once. computer crackers utilize resources to get the data necessary to impersonate different users. sniffer programs that capture password data from packets from well-known services like telnet and ftp are found everywhere the internet.

IV. AUTHENTICATION PROTOCOLS

A. Secure web Authentication With Mobile Phones

Wu et al projected an authentication protocol [2] supported a trusted-proxy and user-mobile devices.

This protocol in the main thinks about two security threats:

1. kiosk remembers association data for replay attack at a later time
2. Security proxy receives two coincident association from completely different kiosks, every claiming to be a similar user

Secure login is with success attested by a token (mobile device) on the undependable computers, e.g., kiosks. A random session name is shipped by SMS to the mobile device from the proxy so as to stop phishing sites. it's declared by the authors that the safety of the projected system depends on SMS that are encrypted with A5/1. The algorithmic program A5/1, however, has with success been broken. The system can also be at risk of telephone thievery.

B. Mp-Auth Protocol

The primary goals of MP-Auth [3] are to safeguard user passwords from malware and fishing websites, and to produce group action integrity. There have some assumptions like, bank's correct public key's accessible to users and mobile devices are malware free. A browser on a laptop uses bank's SSL certificate to determine an SSL reference to the bank web site. The browser is also duped to travel to a spoofed web site, or have a wrong SSL certificate of the bank or the confirmative certificating authority. The protocol doesn't defend user privacy from an untrusted laptop; the PC will record all transactions, generate custom user profiles etc. Visual data flaunted to a user on a laptop screen is additionally not attested by MP-Auth.

MP-Auth, on the contrary, assumes that the account and password set is secure. Users got to setup the account and therefore the password through physical contact, like the banks that needs the shoppers to initialize their account in person or sending passwords though communication.

This protocol provides following benefits:

1. Keylogging Protection: A consumer laptop doesn't have access to future user secrets, which means keyloggers on the laptop cannot access vital passwords.
2. Phishing Protection: notwithstanding a user is directed to a spoofed web site, the web site are unable to decipher a user arcanum
3. Pharming Protection: within the unlikely event of name hijacking, MP-Auth doesn't reveal user's future arcanum to attackers.
4. group action Integrity: With the group action conformation step in MP-Auth, a user will sight any unauthorized group action throughout a login session, even once Associate in Nursing aggressor has complete management over the user laptop.
5. relevance to ATMs : MP-Auth is appropriate to be used in ATMs, if Associate in Nursing interface is provided to attach a mobile phone

C. Phoolproof Phishing interference

To build an anti-phishing mechanism [5], used mobile devices as authentication tokens, this was referred to as as Phoolproof. Phoolproof projected employing a sure device to perform mutual authentication that eliminates reliance on excellent user behavior, thwarts Man-in-the-Middle attacks when setup, and protects a user's account even within the presence of keyloggers and most varieties of spyware. To go online into the websites, a user needs to give the pre-issued public-key and therefore the username/password combination. A user who needs to access the account should always initiate the association victimization the secure bookmarker on the mobile phone. However, a mobile phone is unequipped to sight if the user visits a phishing website and so are unable to stop the user from revealing personal data to malicious parties. Again, Phoolproof is also still at risk of the human influential password apply downside and so wants physical contacts so as to confirm that the account setup is secure.

D. Sessionmagnifier

A user merely installs the SessionMagnifier [4] extension on a personal digital assistant browser; nothing must be put in or designed on a daily laptop browser, and no third-party proxy is needed. At the network layer, the laptop will access the personal digital assistant via communications protocol connections. At the appliance layer, the regular laptop browser communicates with the extended personal digital assistant browser victimization the HTTP protocol. A user directly uses the personal digital assistant browser to determine an internet session with a foreign net server. The SessionMagnifier extension is to blame for synchronizing the most recent markup language webpage document from the personal digital assistant browser to the laptop browser, and it's conjointly to blame for acceptive interactions initiated from the laptop browser and firmly playacting these interactions on the personal digital assistant browser.

The simple design of SessionMagnifier leverages two vital options of contemporary web browsers: end-user extensibility and Ajax (Asynchronous JavaScript and XML) technology. End-user extensibility permits the SessionMagnifier browser extension to maximise its capabilities and seamlessly integrate its functionalities with trendy browsers. Ajax technology allows a daily laptop browser to periodically send HTTP requests to SessionMagnifier and maintain the communication with the non-public digital assistant browser. End- user extensibility is well supported by common browsers like Firefox and internet explorer, and Ajax technology has received wide acceptance among all fashionable net browsers . Therefore, SessionMagnifier are often much enforced and deployed on fashionable web browsers. in a very booth browsing surroundings, establishing TCP connections between a PDA and a laptop is possible, and having net access for a PDA is additionally possible. UsingWi-Fi, a user will simply establish each forms of network connections. If Wi-Fi isn't accessible, a user will use USB or Bluetooth to modify TCP connections between a PDA and a PC; meantime, exploitation numerous net access over USB or net access over Bluetooth techniques (e.g., Microsoft ActiveSync), a user also can simply acquire net access for a PDA. Therefore, SessionMagnifier are often much employed in kiosks.

The SessionMagnifier extension consists of 4 main components: connection management, request authentication, request process, and response generation. in addition, it also contains an initial webpage, that is an markup language file to be sent to a daily laptop browser.

E. Opass: A User Authentication Protocol

The projected system OPass [9] that leverages a user's cell phone and short message service (SMS) so as to prevent many password stealing and password reuse attacks. it is quite tough to forestall the password reuse attacks from any of the schemes wherever within the users need to bear in mind one thing. the most reason behind stealing password attacks is solely once the users sort passwords to an undependable public computer. OPass additionally involves a brand new part, malware free mobile phone, which is able to be accustomed pass passwords and additionally a brand new communication, SMS, which is able to be used to transmit the specified authentication messages. the most conception of oPass is free users from having to recollect or sort any passwords into standard computers for authentication.

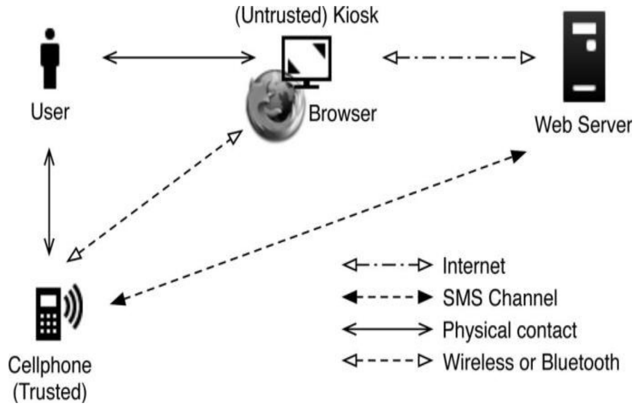

Figure 2.8: architecture of oPass system

Assumptions in oPass system are

Each web server posses a unique number.

Users mobile phone is malware free.

The telecommunication service provider (TSP) can participate in registration &amp; recovery phases.

Users hook up with the TSP via 3G connection to guard transmission.

The TSP &amp; web server establish a secure socket layer (SSL) tunnel to prevent phishing attacks.

If the user loses his mobile phone, he can get a brand new sim card from TSP having identical range. OPass authentication protocol includes three parts: Registration phase, Login phase, and Recovery phase. Registration phase is completed by the user solely initially time and therefore the recovery part is employed once the user lost his/her mobile. The login part is employed by the user after they wish to login to their websites. within the login part user creates a long term password and that is additionally employed in the recovery part. In every login user enter this long term password in his/her mobile.

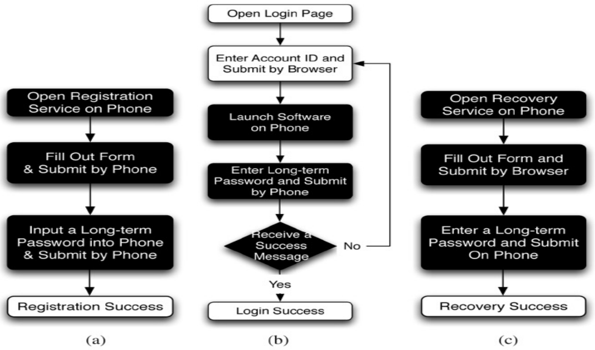
Open Login Page
Enter Account ID and Submit by Browser
Open Registration Service on Phone
Launch Software on Phone
Open Recovery Service on Phone
Fill Out Form & Submit by Phone
Enter Long-term Password and Submit by Phone
Fill Out Form and Submit by Browser
Input a Long-term Password into Phone & Submit by Phone
Receive a Success Message
No
Enter a Long-term Password and Submit On Phone
Yes
Registration Success
Login Success
Recovery Success
(a)
(b)
(c)

Figure 2.9: (a) registration (b) login and (c) recovery

The OPass has the subsequent benefits.

Anti-malware
Phishing Protection
Secure Registration and Recovery
Password reuse prevention
Weak password Avoidance
Cell phone Protection

V. CONCLUSION

Through this survey many things are terminated as before adopting any secret or authentication methodology, user should grasp the secret attack and so user ought to apply acceptable answer. The user ought to apply the authentication methodology per situation as a result of a number of the ways are applicable at stand alone system and a few are applicable at on-line environments as over ATM and several other net services. although many novel schemes delineated here give protection against dictionary attacks, brute force attacks, video recording attacks, spyware, shoulder surfing, phishing etc however so as to secure the system. additionally totally different secret themes are often incorporate along to create one and additional secured secret scheme. Such theme are often the mixtures of passwords schemes.

Authentication mechanisms give the cornerstone for security for several distributed systems, particularly for more and more fashionable on-line applications. for many years, widely used, ancient authentication ways enclosed passwords and PINs that ar currently inadequate to guard on-line users and organizations from ever additional sophisticated attacks. This study projected an improvement to ancient authentication mechanisms. the answer introduced here includes a one-time-password (OTP) and incorporates the conception of multiple levels and multiple channels. thus this paper projected close to secure user identity and user authentication.

REFERENCES

[1]. B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, **2004,** pp. **75–78.**.

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

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

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

[5]. B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," Financial Cryptography Data Security, **2006,** pp. **1–19.**

[6]. B. Schneier, "Two-Factor Authentication: Too Little, Too Late," in Inside Risks 178, Communications of the ACM, 48(4), April **2005**.

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

[8]. W.C. Kuo, Y.C. Lee, "Attack and improvement on the one-time password authentication protocol against theft attacks", Proc. of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, Aug. **2007**, pp.**19-22.**

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

[10]. Anand Sharma and Vibha Ojha. "Password based authentication" Philosophical Survey, IEEE. 2010.

[11]. 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,, ACM, **2007**, pp. **657–666**.

[12]. 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.**

[13]. 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, USENIX Association, **1999** pp. **1–1**.

[14]. B. Pinkas and T. Sander, “Securing passwords against dictionary at- tacks,” in CCS ’02: Proc. 9th ACM Conf. Computer Communications Security, New York, ACM, **2002,** pp. **161–170.**

[15]. H. Tian, X. Chen, and Y. Ding, “Analysis of Two Types Deniable Authentication Protocols,” I. J. Network Security, Jul. **2009**, pp. **242-246**.