Password-based Authentication in Computer Security: Why is it still there?

Shameer Mohammed*, Dr. L. Ramkumar** & V.R. Rajasekar***

*Lecturer, Department of Information Technology, Sur College of Applied Sciences, Ministry of Higher Education, Sur, Ash Sharqiah, SULTANATE OF OMAN. E-Mail: shameer.sur{at}cas{dot}edu{dot}om
**Lecturer, Department of Information Technology, Sur College of Applied Sciences, Ministry of Higher Education, Sur, Ash Sharqiah, SULTANATE OF OMAN. E-Mail: ramkumar.sur{at}cas{dot}edu{dot}om
***Lecturer, Department of Information Technology, Sur College of Applied Sciences, Ministry of Higher Education, Sur, Ash Sharqiah, SULTANATE OF OMAN. E-Mail: rajasekar.sur{at}cas{dot}edu{dot}om

***Abstract*—**Amongst today's methods of authentication, the old-fashioned technique which requires a username and password remains the prevailing measure of securing computers, email accounts, or online transactions. Besides the threats people are often exposed to if they don't change their passwords regularly, there is always a risk that passwords wipe out from human memory over a longer period of time. This research is exploring the flaws of the dominating username-password security measure, and focusing on the alternative authentication and authorization techniques. Furthermore, the classification of password usage is given and suitable authentication methods are suggested.

***Keywords*—**Authentication; Authorization; Password; Security Measure; Threats; Username.

***Abbreviations*—**Closed-Circuit Tele-Vision (CCTV); Challenge-Response Authentication Mechanism (CRAM); Encrypted Key Exchange (EKE); Public Key Infrastructure (PKI); Secure Sockets Layer (SSL); Universal Authentication Framework (UAF).

I. INTRODUCTION

WE all routinely use various applications in computer systems and other platforms. Commonly, every session starts with logging in into a system preceding any access to email servers or enterprise' applications. A simple, effective, and easy to implement approach known as Compatible Time-Sharing System at MIT was recorded first ever to deploy a password to secure the machine back in 1970, followed by MULTICS – Unix Systems that used a hashed form to protect sensitive data; finally, in 1979 password hashing and salting via crypt() was developed as a measure of security [Joseph Bonneau et al., 1]. The internet-based applications opted for password authentication with the arrival of SSL. Even with the adoption of new technologies in hardware and software, password authentication is still not completely replaced by the existing alternative authentication methods.

II. COMPUTER SECURITY

User authentication is the basic feature of protecting data from computer system intruders; it is the fundamental block of computer security. Authentication allows identity verification of any entity. Moreover, user identity is mapped with the process of granting privileges on access to a resource, known as authorization [Lampson, 2]. Authenticating users is carried out by the series of identification and verification stages. At the identification stage, access to a security system is defined, and the binding between an entity and an identifier is done during the verification step [William Stallings & Lawrie Brown, 3]. Authentication of an entity is usually done by verifying the following [Arvind Narayanan & Vitaly Shmatikov, 4]: (a) Something the entity knows; (b) Something the entity possess; (c) Something the entity is; and (d) Something the entity does. Something the individual knows includes traditional approach of entering identification details such as PIN and passwords, which permits user to login to the application or system and to gain access on the specific features based on the privilege. The second approach is achieved by the usage of the smart card or by physical keys. The third approach can be used with finger prints and eye retina scan. For the fourth approach, voice recognition and handwriting recognition can be used.

III. AUTHENTICATION AND AUTHORIZATION

Authentication and authorization is implemented to ensure confidentiality, integrity, availability, authenticity, and accountability in both local and remote systems. Authentication can be implemented in local and remote systems by password protocol, token-based protocol, static biometric protocol, or dynamic biometric protocol.

IV. PASSWORD AUTHENTICATION

Password Authentication is performed by accepting a key and password for letting a user into local and remote systems [Fujita & Hirakawa, 13]. Authentication is critical for sending our data over the internet, as well as for ensuring that authorizing is done properly allowing access to systems and services; especially now when data theft and information security threats are more advanced. Usually, server authentication is done by SSL with PKI certificates while the client authentication is done with passwords. Password authentication can be categorized depending on its strength as weak authentication, stronger authentication, and inconvenient authentication [5].

Weak Authentication	Strong Authentication	Inconvenient Authentication
Clear Text Passwords	EKE	One-time passwords
Hashed Passwords	DH-EKE, SPEKE	Kerberos
Challenge Response	A-EKE	SSH

V. PASSWORD RELATED THREATS

There are various kinds of attacks which can be attempted by an attacker in order to obtain a victim's password. Some of these attacks work by targeting password during transmission, such as eavesdropping, replay, and man-in-the-middle attacks [Xia, 6].

Other attacks, such as dictionary attacks are directed to passwords stored in the server end [Pinkas & Sander, 7]. Some tools required to launch these attacks are readily available on the Internet, although most of them require some level of technical knowledge. Examples include network sniffer (such as tcpdump [8] and wireshark [9]), tools to assess WiFi network security (such as aircrack-ng [10]) and password cracking utilities (such as John the Ripper [11] and RainbowCrack [12]). Service providers usually attempt to prevent these attacks by encrypting the communication between users and server (using SSL, for example), encrypting and limiting access to stored passwords, and blocking accounts which have too many incorrect login attempts.

Some other types of password attacks are as follows:

5.1. Brute Force Attack

In this type of attack combinations of password applies to break the password [10]. The passwords which are saved in encrypted format were attacked in brute force. Even though the passwords are in the encrypted form, sometimes it may get hacked or steal with the help of insiders. Brute force attack is time consuming.

5.2. Dictionary Attack

The passwords which are usually very simple to guess are matched against a file which contains all possible set of words. If there is a match then the password is hacked. This type of attack takes very faster than the brute force attack.

5.3. Shoulder Surfing

In this type of attack user is under close observation either through CCTV or listening to the beep sounds of key pressed or which keys has been pressed to crack the password.

5.4. Replay Attacks

Reflection attacks is the another name for replay attacks [11]. In CRAM (Challenge-Response Authentication Mechanism) attack user is getting authenticated in two levels. First level is basic authentication and the second level is digest authentication. This mechanism is called as. Here the server and client are involved in mechanism, usually client keys in his/her credentials as an authentication challenge to the server. Then server will receive the response from the client and if the password keyed in is correct then user is allowed to access the system else not. During this basic form of authentication password in the form of a clear text which is visible where as in the second authentication method i.e. digest, password is encrypted to be sent over a network. Even digest authentication method can also be hacked.

5.5. Phishing Attacks

This type of attack is a web based attack [Syverson, 14; Fahad Ikram et al., 15] which takes place during the web transactions where user will be redirected to the fake website and hacker can get access to the user credentials. For example user wants to login to website www.citibank.com. Then the hacker will redirect the user to the website www.ctibank.com, whose UI, look and feel will resembles same as the real website.

5.6. Key Loggers

Key Loggers attack is similar to the spoofing. Another name for this type of attack is key sniffers [Arvind Narayanan & Vitaly Shmatikov, 4; Baig & Mahmood, 17]. User activities are monitored by the key logger's software programs and make an entry in to the log file. This log file is submitted to attacker from which password of the user is traced out.

5.7. Video Recording Attack

In this type of attack hacker may steal the password with the help of miniature cameras or camera equipped mobile phones during the ATM transactions or E-Commerce transactions.

With all the possibility and issues, still password usage is the simplest of all for the purpose of authentication [18].

VI. CLASSIFICATION OF PASSWORD USAGE

Every user has to apply an effective strategy to manage the password depending on the category of usage. Based on its purpose, password usage is mainly classified as (i) Organization/University password (Classification A), (ii) Financial password (Classification B), (iii) Social Media password (Classification C) and (iv) Disposable password (Classification D).

First type, Classification A is related to access to IT Service inside an organization, and VPN password to access the organization from outside. Classification B is related to usage of password with multiple banks, insurance, credit card accounts, etc. Classification C is related to password usage in social networking websites like Facebook, twitter, etc. Finally, classification D represents the passwords used on the websites to access software drivers, clipart, perform opinion poll and surveys, etc.

VII. CATEGORY OF PASSWORD USAGE

Password Managers, Proxy, Graphical, Cognitive, Biometric and Recovery are common categories of using passwords [19]. Among the categories the new approach used additionally with passwords to support more security and better usability are Federated and without password are UAF and U2F.

7.1. Password Managers

Web browsers like Chrome and Firefox offers facility to remember password entered into the web page optionally by encrypting the passwords.

7.2. Proxy (URRSA Server)

In URRSA Server [Dinei Florencio & Cormac Herley, 20], the login server used by organization can be used and sensitive information is not displayed or compromised at the untrusted machine. The user will experience the same browser or client software environment.

7.3. Federated Single Sign-On

In this category, federated single sign-on servers' enable web applications to authenticate users by redirecting them to a trusted identity server to attest the users' identity. Based on the attestation, the user is allowed or declined to access the web application. Facebook Login [21], OAuth [22] and Single Sign-On (SSO) for Google Apps [23] are common examples for this category.

7.4. Graphical Password

In this category, the system displays a 4x4 panel of images containing 2 random pass-images out of the 4 previously chosen pass-images + 14 other decoy images [Alsaiari et al., 24]. The user needs to identify the two pass-images. Based on the selection, the authentication process is selected.

7.5. Cognitive Authentication

Challenge-Response scheme is commonly used in this category. We install [Markus Byström & Michael Palmgre, 25] proposed a scheme that requires a user to memorize a set of 30 assigned images. To login, the user is presented with a series of screens and at end of the completion the user enters the two bit number written on the margin at the exit point. Hoppe-Blum [Hopper & Blum, 26] proposed a challenge response scheme by involving the user calculation on a shared secret.

7.6. UAF and U2F

UAF authentication claims to be a password less authentication supported by the Universal Authentication Framework (UAF) protocol. In this category, as illustrated in Fig. 1, the user carries client device with UAF stack installed and then the user presents a local biometric or PIN. Based on the inputs, the web application chooses how to retain password.

In this category, the user registers their device to the online service by selecting a local authentication mechanism such as (1) swiping a finger, (2) looking at the camera, (3) speaking into the mic, (4) entering a PIN. The UAF protocol allows the service to select which mechanisms are presented to the user. Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms such as fingerprint + PIN.

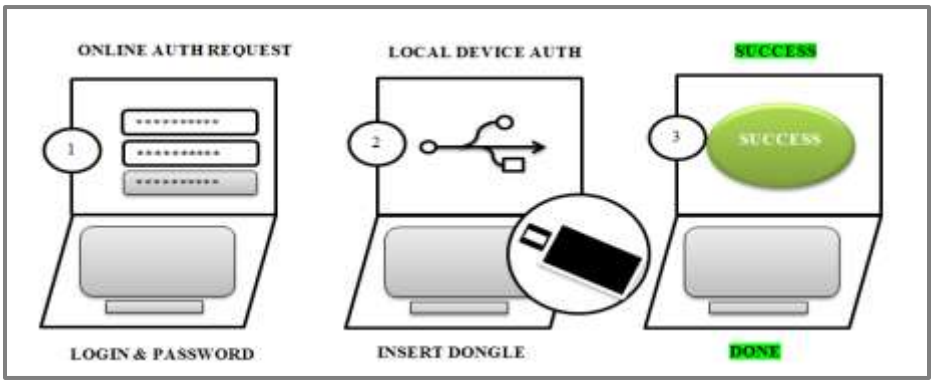

Figure 1: Working

The following section compares the applicability of categories in specific classifications.

Password Managers are suitable only for classification C and classification D as the web browsers supports the better usability.

Proxy (URRSA Server) is mainly suitable for multiple applications within a single organization. There is no proven record for its role in security improvement in online banking applications.

Regarding the usage of Federated Single Sign-on, in classification A, the organization can setup a federated server internally for all the application within an organization. This category is not suitable for classification B as the application has to verify the trust of another identity server, which is complex in process. This category is most suitable for classification C and classification D.

Graphical password will lead the user to remember the images for different applications which is not a solution for replacing the password. It will be an additional burden to the user. Not Suitable for all the classification.

Regarding the Cognitive Authentication, the memorization is beyond human limit. So this cannot be a replacement for the password authentication in all the classifications.

UAF and U2F category is suitable for all the classification. But there is an additional device cost involved in implementing this category [16].

Table I gives the comparative chart of common password category in different classification. From the table it is evident that, no category can completely replace the password authentication in all the classification, other than the UAF but it requires additional cost of implementation.

Table 1: Comparative Chart of Common Password Category in Different Classification

Category/ Classification	A	B	C	D
Password Managers	-	-	X	X
Proxy Server	X	-	X	X
Federated Single sign-on	-	-	X	X
Graphical	-	-	-	-
Cognitive	-	-	-	-
UAF	X	X	X	X

VIII. Conclusion

The past decade has seen growing interest in replacing username-password authentication with new methods. On the other hand, there is a tremendous growth in web based applications. Two factors are considered key elements in the usage of password authentication: usability and security. User authentication can be done by verifying a password, pin, smart card, physical key, finger print or eye retina scanning. Improper authentication or authorization allows the attackers of the system to get the right of the systems and intrude. From the comparative chart of password categories in different classification it is evident that except for UAF, no other category can replace password authentication. It is clear from the study, that the new techniques to replace the password need more time for adaptation.

References

[1] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot & Frank Stajano (2015), "Passwords and the Evolution of Imperfect Authentication", *Communications of the ACM*, Vol. 58, No. 7, Pp. 78–87.

[2] B.W. Lampson (2004), "Computer Security in the Real World", *IEEE Computer*, Vol. 37, Pp. 37–46.

[3] William Stallings & Lawrie Brown (2008), "Computer Security: Principles and Practice", *Pearson Education India*.

[4] Arvind Narayanan & Vitaly Shmatikov (2005) "Fast Dictionary Attacks on Passwords using Time-Space Tradeoff", *Proceedings of the 12th ACM Conference on Computer and Communications Security*, Pp. 364–372.

[5] http://srp.stanford.edu/ndss.html

[6] H. Xia (2005), "Hardening Web browsers Against Man-in-the-Middle and Eavesdropping Attacks", *Proceedings of the 14th international conference on World Wide Web*, Japan, Pp. 489–498

[7] B. Pinkas & T. Sander (2002), "Securing Passwords against Dictionary Attacks", *Proceedings of the 9th ACM Conference on Computer and Communications Security*, Washington, DC, USA, Pp. 161–170

[8] tcpdump. http://www.tcpdump.org/

[9] wireshark. http://www.wireshark.org/

[10] aircrack-ng http://www.aircrack-ng.org/

[11] John the Ripper. http://www.openwall.com/john/

[12] rainbowCrack. http://project-rainbowcrack.com/

[13] K. Fujita & Y. Hirakawa (2008), "A Study of Password Authentication Method against Observing Attacks", *6th International Symposium on Intelligent Systems and Informatics*.

[14] P. Syverson (1994), "A Taxonomy of Replay Attacks [Cryptographic Protocols]", *Proceedings of Computer Security Foundations Workshop VII*, CSFW, 7(s), Pp. 187–191.

[15] Fahad Ikram, Muhammad Sharif & Mudassar Raza (2008), "Protecting Users against Phishing Attacks", *7th CIIT Workshop on Research in Computing*.

[16] FIDO. FIDO Alliance Universal 2nd Factor (U2F), November 2015. https://fidoalliance.org/specs/fido-u2f-v1.0-rd-20140209.zip.

[17] M.M. Baig & W. Mahmood (2007), "A Robust Technique of Anti Key-Logging using Key-Logging Mechanism", *Digital EcoSystems and Technologies Conference, Inaugural IEEE-IES*, Pp. 314–318.

[18] http://www.dailymail.co.uk/

[19] The quest to replace passwords: a framework for comparative evaluation of web authentication schemes

[20] Dinei Florencio & Cormac Herley (2008), "One-Time Password Access to any Server without Changing the Server", *Proceedings of ISC '08*, Taipei

[21] https://developers.facebook.com/docs/facebook-login

[22] http://oauth.net/

[23] support.google.com

[24] H. Alsaiari, M. Papadaki, P.S. Dowland & S.M. Furnell (2014), "Alternative Graphical Authentication for Online Banking Environments", *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance*, HAISA.

[25] Markus Byström & Michael Palmgren (2011), "Cognitive Authentication Schemes".

[26] N. Hopper & M. Blum (2001), "Secure Human Identification Protocol", *ASIACRYPT*.

Shameer Mohammed has earned his Master of Computer Applications (MCA) degree from University of Madras, Chennai. He is currently working as a Lecturer at Sur College of Applied Sciences, Ministry of Higher Education, Sultanate of Oman. He has profound Software Development experience and worked with renowned IT MNC's in India and GCC countries. His technical skills are Java EE technologies. His research interest areas are gamification, SOA, software engineering, reliability, software testing, and web technologies. He has published one research paper, attended three conferences. He has presented the paper titled "The need for effective information security awareness practices in Oman higher educational institutions" at Symposium of communication, Information Technology, Applied Biotechnology "Current Trends and Future Scope ", Sur – CAS, Oman, 12-13th MAY, 2015.

Dr. L. Ramkumar at present working as a Lecturer, Information Technology in Sur College of Applied Sciences, Oman. He is having 18 years of experience in teaching, consulting and software development. He has conducted training for leading corporate companies in India and abroad in the field of Database, Data warehousing, Cloud Computing and Mobile Technology. He has presented articles in various journals around the Globe. He has did his research in the field of Applications of Computers Science in the Management of AAVIN Dairy Cooperatives. He is a regular author of Technical articles in Indian Regional technical magazine "Tamil Computers".

V.R. Rajasekar has earned his Master of Engineering (ME) degree from Sathyabama University, Chennai, India. He holds CCNA and CEH certification. He is currently working as faculty in College of Applied Sciences, Ministry of Higher Education, Sultanate of Oman.His areas of interest are Data Communication and network security. For the past ten years, he has published serveral papers in reputed journals and conferences, in the area of computer security.