IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Study on Framework for Password-less Authentication

Sabin K Ravi[1], Sivadasan E T[2]

P G Scholar, Department of Computer Science and Engg, Vidya Academy of Science and Technology, Thrissur, India[1]

Associate Professor, Department of Computer Science and Engg, Vidya Academy of Science and Technology, Thrissur, India[2]

Abstract: This paper is to study the possibility of new and easy way for authentication which is cheaper and faster. In the time where there are many web based and cloud based applications and all uses password based authentication scheme and user require remembering many passwords. In this paper, a study on different possible authentication methods is done to find which require less user physical effort, which is more convenient, cheaper, faster and secure method so that it can take over the authentication process in future and make it easier for users.

Keywords: Authentication, Password Mobile Device, Human Computer Interaction, Security, Usability, Deployability.

I. INTRODUCTION

World Wide Web is being used by millions of people on everyday basis for various purposes which includes email, news, music downloads or browsing information about anything. Users frequently access web services in their day-to-day lives. Nowadays, it is destined to have a number of accounts for computers, Email accounts, websites, social networks, and many other services, all of which employs authentication method as passwords and thus having different passwords and security policies for each account .Memorizing all passwords is both difficult and troublesome, so people often end up in using simple passwords and hence compromising security. These practices are bound to help hackers, especially when we perform online transactions using computing devices. Hence, what we really require is a new and an innovative way to access web services that does not involve memorizing passwords with dozens of alphanumeric combinations, as well as does not add complexity for users.

In password-based authentication, the security is determined by the task of successfully guessing a user's password. Unfortunately, passwords tend to have low entropy and are easier to guess. To further enhance the security of password-based web services, a favorable solution is to make use of technology called two-factor or multi-factor authentication, wherein a user is required to provide more than one authentication factor, in general a user's password.

The other piece of authentication information is either generated by a physical token, for example, RSA Secur ID [1] or a mobile device encompassed with Google Authenticator application [2]. Although the two-factor authentication is able to enhance the security of web access, different service providers may require setting up their own two-factor authentication services. In addition, users have to undergo painful registration and login procedures.

II. AUTHENTICATION

User authentication generally occurs among most human computer interactions. In most scenarios, a user has to enter an id and provide the corresponding password to begin the use of a system. User authentication authorizes human-to-machine interactions among operating systems and applications and also allows both wired and wireless networks to enable access to network. In private and public computer networks, authentication is frequently done through the use of login ids (user names) and passwords. Knowledge about login credentials is supposed to guarantee that the user is authentic. Initially, each user registers to the system (or is registered by someone else, such as a systems administrator), with the help of assigned or self-declared password. Upon each subsequent use, the user must know and use the previously declared password. Nevertheless, password based authentication is not considered to provide adequate security for any system that contains sensitive data.

The domination of password based authentication is been there from the early days of authentication and still the only method being used widely. An authentication method should have certain characteristics like ease of using, should be faster and at the same time secure as well.

Different service provider use certain rules in defining passwords like password should have certain number of upper case, lowercase, number, special character. Example -yahoo mail, which makes authentication process troublesome and more pain full for users to remember. [3] to replace text based method the several proposal have been made, some of the scope of proposal include management software, federated login protocol, graphical password scheme, one time password, hardware tokens, phone aided schemes and biometric methods. The problem is that when certain method provide significant security then will be more costly to implement as well more difficult to use usability, deploy ability, security hence serves major factors in any method.

DOI 10.17148/IJARCCE.2016.52149

User benefits must be taken into consideration are the method must be memory wise effortless to remember, scalable for user so that can implement in large scale without burden to user, and which must avoid carrying certain object for the purpose but at the same time Quasi nothing to carry like mobile devices that everyone carries always can be used, physically effortless and easy to use, learn and also easy to recover from loss of token and credential like use backup methods.

Deployment benefits must be taken into consideration are accessible in the sense user who uses password based method must be allowed to use the method with same ease, negligible cost per user including both provider side and verifier side cost, server compatible so that no need to change existing setup to support current scheme ,browser compatible which makes sure no need to change the client side settings and can work on standard web browser and no extra additional software is required, also mature enough so that Anyone can implement or use the scheme for any purpose without having to pay royalties to anyone else.

Security benefits that should be considered are Resilient to Physical Observation: The attacker cannot impersonate a user after observing them one or more times to their account, Resilient to Targeted Impersonation: It is not possible for skilled investigator to impersonate a specific user by exploiting knowledge of personal details like birth date, names of relatives etc, Resilient-to-Throttled-Guessing: An attacker whose rate of guessing is constrained by the verifier and attacker cannot successfully guess the secrets, Resilient to Internal Observation: The attacker cannot impersonate a user by intercepting the user's input from the user's device, Resilient to Leaks from Other Verifiers: A verifier could not possibly leak anything which can help an attacker impersonate the user to the verifier, Resilient to Phishing: An attacker who simulates an authentic verifier cannot collect credentials that can be used later to impersonate the user to the valid verifier, Resilient to Theft: If the scheme uses a physical object for authentication, then the object cannot be utilized for authentication by another person who gains possession of that object, No Trusted Third Party: The scheme does not rely on a trusted third party who offers authentication mechanism, Requiring Explicit Consent: The authentication process cannot start without the explicit consent of the user.

[4]The common concept is that if users can be educated to select "perfect" passwords which are difficult task, offline brute-force attacks to recover such information will surpass the computational ability of modern machines. In reality, the current entropy is a perfectly random 8 character password. However, the most common password length, is less than that of a DES key.

Since DES was effectively broken by brute-force attacks in 1999 [5], this assumption is questionable. Nowadays, we are seeing a variety of password policies request 15 character passwords. In that case, the entropy is comparable to 3DES or AES. Also, a prevalence of password policies is provided for guiding users to select passwords that are effective. Our interpretation is that the community is demarcating the future viability of password system increases in password length and policies to ensure effective use of the password space, but human beings are capable of remembering approximately seven random items. Also an increase in password length does not necessarily mean a commensurate increase in entropy. The fundamentally limited amount of protection current passwords can provide is no longer sufficient to protect password-based authentication systems vulnerable to offline attacks from brute force attacks by the rapidly growing computing resources available. Because all passwords will be recoverable, the security of any system based on passwords will depend on the availability of cracking material, not how random passwords are. As such, protocols must be designed to not allow any type of offline attack, and the material that can be used to mount such an attack must be protected with the understanding that its confidentiality is equivalent to the security of the authentication mechanism as a whole.

III. EXISTING SYSTEM

There are several existing systems other than password based authentication being in use like [6] OAuth 2.0 is the up gradation of OAuth protocol which was originally created in late 2006. OAuth 2.0 focuses on client developer simplicity along with providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. [7]. the most ubiquitous method is the password based and has numerous problems, which includes susceptibility to unintentional exposure through phishing and cross-site password reuse. Two factor authentication schemes tend to have the potential to increase security but faces usability and deploy ability challenges. Phone Auth is a system intended to provide security assurances in comparison to or greater than that of conventional two factor authentication systems, in addition to offering the same authentication experience as traditional passwords. The work leverages the following key insights. First, a user's personal device (phone) can communicate directly with the user's computer (remote web server) with no interaction with the user. Second, it is possible to provide a layered approach to security, by which a web server can impose different policies depending on whether or not the user's personal device is present. [8]

Kerberos is a distributed authentication service that enables a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or just server) without sending data across the network. Sending data might allow an attacker or the verifier to subsequently impersonate the principal. Optionally, Kerberos provides integrity and confidentiality for data which is sent between the client and server. Kerberos was developed in the mid-eighties as part of MIT's Project Athena [9]. As the widespread usage of Kerberos spread to other environments, changes were required to support new policies and patterns of use. To

DOI 10.17148/IJARCCE.2016.52149

address these requirements, a new version was developed called the Version 5 of Kerberos (V5) which began in 1989 [10]. Though V4 still used by many sites, V5 is still considered to be standard Kerberos.

IV. RELATED WORK

[11] Google two step verification make use of two methods which are combined to provide more security in authentication process basically it makes use of primary method has user name and password and secondary method by means of either verification via SMS by sending a one-time password generated to the mobile device via SMS and user entering that as secondary verification.

[12] Traditional two-factor authentication protocols require a shared secret between the user and the service. For instance, OTP (one time password) protocols use a shared secret modulated by a counter (HOTP) or timer (TOTP). A demerit of these protocols is that the shared secret can be compromised if the server is compromised. We choose a design that is resilient to a compromise of the server side data's confidentiality at the same time Twitter doesn't persistently store secrets, and the private key material needed for approving login requests never leaves your phone.

Other attacks against two factor authentication have taken advantage of compromised SMS delivery channels. This solution overcomes that because the key necessary to approve requests never leaves your phone. Also, the updated login verification features additional information about the request to help user to determine if the login request you see is the one you're making.

[13] How Twitters two factor authentication works is When try to login to your Twitter account from another device, an alert will be sent to your phone asking you to authorize the login. On Android, the alert in the notifications area is tapped to open the Twitter app and go directly to the login requests page. After that, a request to authorize the login is given with a single tap there are no codes to enter. The request includes information such as time, location, and browser type, so user can be sure that the request is coming from user itself.

[14] RSA SecureID uses a hardware version of google authentication where the hardware token generates and displays new codes every 60 seconds which is used in authentication, RSA SecureID software version uses same algorithm as in hardware,[15] Push notifications makes authentication easy for users, and easy for administrators too.

Through one tap authentication using Duo's mobile application, users can quickly approve an authentication request through the press of a single button. Or, users can choose to answer a phone call, type in a onetime password, or even use hardware tokens. And also Authenticate from wherever user are, with support for multiple devices.

V. CONCLUSION

In this paper studied about authentication process and current methods used and what are the works related to a password-less authentication framework and how we can combine different methods to provide a better, easy, faster and secure mechanism for authentication and to replace traditional universal authentication systems based on passwords. In particular, even if the servers are compromised by attackers, the private keys of users are still safe and thus attackers cannot impersonate the users. These salient features make an attractive security solution for password-less web authentication. Several methods have been proposed which takes advantages of push message services for mobile devices and enables users to access multiple services by using pre-owned identities, such as email addresses, together with few taps on their mobile devices.

REFERENCES

[1] RSA Secur ID Hardware Authenticators, RSA Inc., available at http://www.emc.com/security/rsa-securid/rsa-securid-hardware-authenticators.html

[2] Google Authenticator Project – Two-Step Verification, Google Inc., available at http://code.google.com/p/google-authenticator/.

[3] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. IEEE Symposium on Security and Privacy - S&P 2012, pp. 553-567, IEEE Computer Society, 2012.

[4] L. S. Clair, L. Johansen, W. Enck, M. Pirretti, P. Traynor, P.McDaniel, and T. Jaeger. Password exhaustion: Predicting the end of password usefulness. Information Systems Security, pp.37-55, Springer Berlin Heidelberg, 2006.

[5] EFF DES cracker project. www.eff.org/Privacy/Crypto/Crypto misc/DESCracker/.

[6] OpenID Authentication 2.0 - Final, OpenID Community, 2007, available at http://openid.net/specs/openid-authentication-2 0.html.

[7] A. Czeskis, M. Dietz, T. Kohno, D. Wallach, and D. Balfanz. Strengthening user authentication through opportunistic cryptographic identity assertions. In Proceedings of the 2012 ACM conference on Computer and communications security, pp. 404-414, ACM, 2012.

[8] S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer. Kerberos: An authentication service for computer networks. In Project Athena Technical Plan, 1987.

[9] G. A. Champine, D. E. Geer, Jr., and W. N. Ruh. Project Athena as a distributed computer system. IEEE Computer, 23(9):40-51, September 1990.

[10] J. T. Kohl, B. C. Neuman, and T. Y. T'so. The evolution of the Kerberos authentication system. In Distributed Open Systems

[11] Google Authenticator Project – Two-Step Verification, Google Inc.,

[12] A. Smolen. Login verification on Twitter for iPhone and Android. Twitter, Inc., 2013, available at https://blog.twitter.com/2013/login-verification-on-twitter-for-iphone-and android.

[13] Thoughts on Twitter's new Two-Factor Authentication, Authy,2013, available at http://blog.authy.com/twitter.

[14] RSA SecurID Hardware Authenticators, RSA Inc.,available at http://www.emc.com/security/rsa-securid/rsa-securid-hardware-authenticators.htm.

[15] Duo Push: One-Tap Authentication, Duo Security, Inc., available at https://www.duosecurity.com/duo-push

DOI 10.17148/IJARCCE.2016.52149