IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Secure Authentication Scheme against password Guessing Attacks

C.A. Thriveni[1*], K. Madhavi[2]

[1] Department of Computer science, JNTUACEA, JNTU, Ananthapuramu, India
[2] Department of Computer science, JNTUACEA, JNTU, Ananthapuramu, India

**Corresponding Author: thriveniveni5203@gmail.com, Tel.: 9550641869*

Available online at: www.ijcseonline.org

Accepted: 05/Jun/2018, Published: 30/Jun/2018

***Abstract*—** With the rapid growth of websites, the registered users accounts across the websites increased from aggressive manner. The user may contain multiple accounts in a single website or across the different websites. So, for the different accounts the user may use the same password or the similar password which is already used, but with the prefix or postfix. As the result, guessing a single password may leak the remaining passwords which lead to the major concern of the security and user may forget the passwords of different sites. Hence a secure authentication scheme against password guessing attacks is necessary for logging in to the account with the single password reused for all the accounts in a secure manner with Single Sign on (SSO). In SSO, the tool allows a user to register and sign in with one set of credentials and gain access to the multiple applications and services. SSO increases security by using the difficult passwords which restrict guessing attacks, and also provides a better user experience for customers, employees by reducing the number of required accounts, passwords and provides simple access to all the applications and services they need.

***Keywords*—** Security, Authentication, Password guessing attacks, Brute force attacks, Dictionary attacks.

I. INTRODUCTION

Secure authentication is a term which satisfies or meets the certain attributes of a single piece of data claimed by an entity. Authentication is the process of confirming the identity. It involves in verifying the validity of at least one form of identification. Password guessing is the type of attacks which has parts like a brute force attack and dictionary attacks. The Brute force attack is a type of password guessing attack with the process of trying every possible word until a right password is found or identified, whereas dictionary attacks is the process of using common dictionary words to identify the user's password.

Generally authenticating with password is the majorly used technique to access different sites [1]. Basically, the user may hold many numbers of accounts in or across the webpages. Each account is allowed to set the different password for the accounts. This makes user forget his passwords. It doesn't matter the user chooses the ease login choice or the typical one. There is a high chance of forgetting or leakage of authenticating password [2]. Even there is some process of guessing tools to crack the login of users. The password remembering is a challenge and wastes the time for regaining or recovering the password. Usually corporate spend few hundreds of dollars in regaining its employee passwords. According to Forrester Research study, password resets can cost an enterprise an average of 179 dollars for an employee per year. Multiply that by the number of users and the information technology (IT) costs to get high, fast. Fewer passwords mean fewer to reset, less time and less costs for user administration.

Protocols using browser based Single Sign On provides convenience and security for user and service provider alike. By providing SSO protocols, users are relieved of the burden of having to remember multiple set of ID'S and password for different web services they wish to use. Similarly the service provider is relieved of the burden of a variety of logins related tasks such as clients contacting them for stolen password, recovery of forgotten passwords, revocation of possibly compromised passwords etc. As such, by substituting multiple identities corresponding to multiple service providers connected via a central identity provider with a single identity, SSO protocols are promising a more secure Internet experience, especially given that clients typically use easy to remember weak passwords and usually use the same passwords to access different applications [3]. Due to the proliferation of social networking, cloud computing and the Internet of things, SSO schemes are now becoming more popular. Social networking giants such as Facebook, Google, Twitter and several others are providing SSO services to the public. An SSO authentication scheme relies on three main components: the users wishing to be granted access to certain services, the service provider SP (known also as the relying party) and the Identity Provider (IDP) who delegates identity assertions to the service providers [4].

Section-II contains the related work of previous published papers with description and drawbacks. Section-III deals with a secure authentication scheme against predicting passwords by providing security. Section-IV deals with the necessary discussion and results of proposed system. Section-V concludes the whole paper.

II. RELATED WORK

Here authors D. Akhawe, and D. Song planned to introduce web based password manager instead of local password manager. Author found that an attacker can learn user's credentials for arbitrary websites and also the vulnerabilities diverse, ranging from logic, and authorization mistakes to misunderstanding about the web security model [5]. Authors Weili Han and Minyue Ni have done empirical analysis on password reuses by analyzing a large data. Most of the people reuse their password across multiple services by using N-gram, prefix and suffix. Hence the leakage of password is analyzed with the security concern [6]. Author Lee anticipated that a network of computer logging, SSO is a novel mechanism. This allows a certified user to login to various accesses to the help of only one registration. But the threats have been induced in terms of programs. Thus, two different leakages from the secure password raised. One is the malicious approach to heirs the certified user. Another is an exterior attack in terms of forgery. Author Yan minglai raised a new SSO and said that, provided greatly organized arguments with security. But, the demonstration leaves it as a credential privacy failure [7].

W. Yang planned for a password models which assign a feasible value of every string. That type of models is useful in research to analyse the user's perspective of choosing passwords. Graphs of guessing number which is produced from such models are massively used method of research. Here author M. Luo proposed the feasibility threshold analysis, which is having the at most advantages over graph numbers. Even they are speeders and data is provided beyond what is feasible in graphs of guessing the number [8]. X. Wang focused on attacks and reports the first "field study" on the web SSO system, he discovered some serious logic flaws like open ID, sears, farm vile etc. Every flaw allows an attacker to sign in as the victim user which reveals the gravity and pervasiveness of security critical logic flaws within the web SSO system [9]. Author N. Li has also seen the related statistical language modelling is benefited. For probabilistic password theories, a large number of evaluations are done. This also in the model of author Markov utilizes the various normalization methods. Methods of Markov when works efficiently, then its significance in terms of performance is comparatively good for the feasibility context free grammar model in reference of author Weir et.al [10]

Jones and G. Rymer supports that password based authentication is the most popular form of authentication. Password authentication is having a number of issues like users using large number and high complexity required of passwords, users frequently reused, and choose weak passwords. Author thought and address to solve these problems is to centralize password management by using a password manager SSO, which increases the user's security [11]. Author Halilarslans with reference from Single password authentication by author T.Acar and said that users got to need authentication with several times totally different group of username and password that access various service suppliers and applications in their daily task and on social life. During this case, the user should get to learn several pair of usernames and password. This one is then to enforce the user exploitation ordinary passwords or to stay note of passwords anywhere. It's a retardant as a secret of personal user information on social life that to get additional crucial issues on business applications. To urge eliminate this drawback, one sign on (SSO) is usually recommended. SSO describes a group of usernames and password mainly multiply passwords to access for various service suppliers and applications. During this study, we tend to argue the prevalent and therefore the current issue of SSO protocols in literature is one in all the SSO protocols, is employed to look at a model [12].

III. Secure Authentication Scheme against Password Guessing attacks

Single Sign On leaving the frustrated approaches like signing on to different sessions individually and take advantages of not keeping the many passwords in mind and gives the great convenience. With the arrival of Single Sign On the typicality came into the finger steps with just access to single click. SSO also incorporates security high by reducing frequent attack targets of user credentials downed in one. And that downed one set is highly protected from advanced encryption system (AES).

The encrypted information on AES is supported with 256 bit operation. Instead of passing user's passwords or storing credentials on user's devices, this mechanizes with tokens to authenticate. To allow SSO, the corporation known as identity provider should make central server so that all software as a service like various applications can link with their unique identities. Later the encrypted information will satisfy the user's identity. The server will locate the identities and issue tokens to the service providers.

Algorithm:

```
Step 1:  Start
Step 2:  User installs PM  // PM → Password manager
Step 3:  With PM, user access to SAAS
                              //SAAS → software as a service
Step 4:  SAAS app generates keys and encrypts user id
         and password
Step 5:  Encrypted format is stored in password cloud
         server, and keys in key server
Step 6:  User access and requests for specific cloud based
         application
Step 7:  SAAS fetches encrypted information from stored
severs
Step 8:  Username and password is decrypted and sent to
         requested SAAS app
Step 9:  After confirmation, finally transfer to web
browser
Step 10: End.
```

The system model consists of four entities: Admin, User, Identity provider, Service provider.

a) Admin: In the system the admin acts as owner. The admin provides the service web applications for the users. Admin plays the jobs of accepting or authorizing the user to access web services that are permitted by admin. The owner can also de-authorize the user when not in use or for various reasons.

b) User: For accessing the web services, the user first needs to register. The user can register and can log on from any of the web services without re-entering the user id and secret password. User can easily login for the first time and can shuffle from the current web application for another web application for greater experience and improved security.

c) **Identity provider:** Identity Provider must implement a centralized authentication server that all apps can use to confirm a user's identity. This server can validate user identities and issue access tokens, the encrypted bits of data that confirm the identity and privileges of a user. User to access the services, the one need to register for their personal credentials is directed to a service provider for verification, which are stored on central server. Central server then provides an identity to user to logon. The central server then generates an access token and waits for the service provider reply.

d) **Service provider:** A Service provider plays a mediator's job between users and centralizes server. When the user requests access to an application for the trusted group, instead of requesting a password, the service provider requests the identity provider authenticates the user's identity. When the central server generates an access token, then the job of a service provider is to identify the type of token it is, type of login it is and grants the access token to user for secure login without ever showing the sign-on screen for the user.

IV. Results and Discussion

With the aid of a Secure authentication against password guessing attacks, the number of users that are victims of guessing attacks are gradually degraded because of there is pros with not remembering password for different accounts and even though the password is cracked, the access tokens are sent as one time password for different users. In this, the user can access various services with a uni-sign on. So the password is only one which can be easily remembered.

The comparison of before and after secure authentication against guessing attacks is shown in graphs individually. The simulation and analysis of guessing and leaked passwords of users having two or more accounts with password reused are shown in figure1

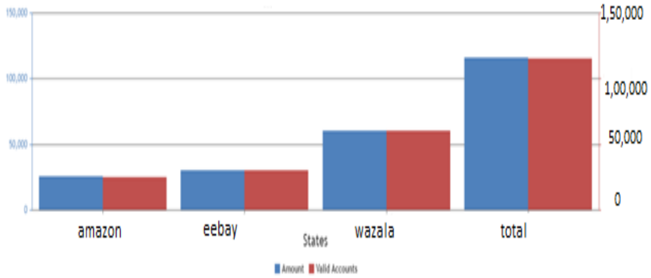

Figure 1: **Statistics of leaked passwords**

Figure 1 shows the statistical graph by comparing three sites, namely amazon, eBay and wazala. And the total number of accounts in combining all accounts are also indicated. And table 1 produces with site names, total amount of accounts and valid accounts in the total amount of accounts.

Table 1: Valid accounts

Account name	**Amount**	**Valid accounts**
Amazon	50,784	25,000
EBay	60,242	29,999
Wazala	1,20,626	59,999
Total	2,31,652	1,14,998

Table 2: Users for analysis of CSPR

Number of accounts	Number of users	Percentage
1	84,346	73.345
2	99,859	8.835
3	110	0.095
4	15,544	13.516
6	110	0.095
8	31	0.026

Table 2 produces the number of accounts holding by a user in or across the websites. And the related percentage is given. Whereas table 3 gives the accounts having among two sites and its percentage is provided.

Table 3: Percentage rate of CSPR

	Amazon	EBay	1Wazala
Amazon	-	50,244 16%	40,786 19%
EBay	40,786 19%	-	1,00,628 16%
Wazala	40,786 19%	40,244 33%	-

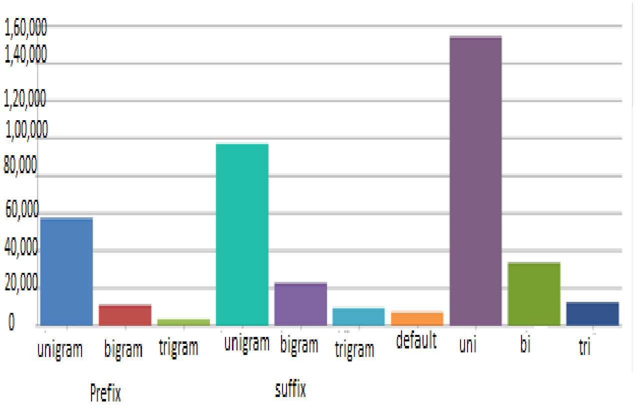

Figure 2: Used N-gram prefix/suffix

The overall accounts in the three websites, the user using password with prefix, suffix unigrams, bigrams, trigrams, default, and individual unigram, bigram and trigram is shown in figure 2.

Hence the leakage of passwords is analyzed and with the security concern of password, the secure authentication schemes against password guessing attacks, i.e., single sign on is used and explained as follows.

By using one sign on with advanced encryption system, the inducers have a very less chance of predicating password. For cracking with advanced tool also the one may need several years. Thus the corporation can maintain the data and logger security.

After using one sign on authentication the user also uses prefix, suffix of unigram, bigram, and trigram. But the comparatively the using of N-gram has reduced which is shown in the figure 3.

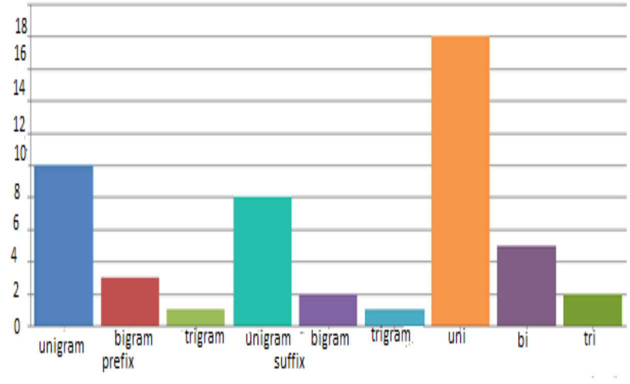

Figure 3: **Mostly used N-gram prefix/suffix**

V. Conclusion

With the growth of rapid number of sites, the user is registering into those sites for accessing necessary services. As user is accessing the various accounts from different sites, the user might create same password for the sites with the minor changes of using suffix or prefix. The attacker can guess at least one password and try dictionary attacks for decrypting remaining passwords. So, with a secure authentication against predicting attacks, the user registers only once and browses different sites securely. A secure authentication removes the concern of security with encryption information but also for logging. The security is enhanced in protecting single password rather than 'n' passwords. The tokens are exchanged for accessing provided services for authenticating the registered user. Advanced encryption systems in one sign on have a very less chance of predicting password. Results of SSO produces, reducing user's time and IT cost. The user shall keep a unique password which cannot be disclosed.

REFERENCES

[1] D. Florencio and C. Herley, "A large-scale study of web password habits, "in *Proceedings of the 16th international conference on World Wide Web- WWW '07*, 2007, p. 657.

[2] J. Yan A. Blackwell R. Anderson A. Grant "Password memorability and security: Empirical results" IEEE Security Privacy vol. 2 no. 5 pp. 25-31 Sep. /Oct. 2004.

[3] Kostas Theoharoulis Ioannis Papaefstathiou "Implementing Rainbow Tables in high end FPGAs for superfast password Cracking" International Conference on field programmable Logic and applications (FPL) ISBN: 978-l-4244- 7842-2 Aug. 2010.

[4] T. Arai H. Yamaguchi T. Sekiguchi and Y. Takemi "Fundamental technology to support cloud computing" IT platform 2010

[5] Z. Li, W. He, D. Akhawe, and D. Song. The emperor's new password manager: Security analysis of web-based password managers. In USENIX Security, 2014.

[6] Weili Han, Zhigong Li and Minyue Ni "Shadow Attacks based on Password Reuses: A Quantitative Empirical Analysis"

[7] Chang, C.C and Lee, C.Y. (2012) a secure single sign-on mechanism for distributed computer networks. IEEE Trans. Ind. Electron., 59, 629–637

[8] Csdncleartext passwords 2011.

[9] R. Wang, S. Chen, and X. Wang. Signing me onto your accounts through Facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services. In Security and Privacy (SP), 2012 IEEE Symposium on, pages 365–379, 2012.

[10]N.LiandMarkovesecurity.org/TC/SP2014/papers/AStudyofProbabilisticPasswordModels

[11] D. Llewellyn-Jones and G. Rymer. Cracking pwdhash: A brute force attack on client-side password hashing. In The 11th International Conference on Passwords (Passwords 2016). Springer, 2017.

[12] T. Acar M. Belenkiy A. Küpçü "Single password authentication" Computer. Networks vol. 57 no. 13 pp. 2597-2614 Sep. 2013.

Authors Profile

C A Thriveni received B.Tech in Computer Science and Engineering from BIT institute of technology, Hindupur, Andhra Pradesh in 2015. Currently, she is pursuing M.Tech in Software Engineering from JNTUA College of Engineering, Ananthapuramu, Andhra Pradesh, India. Her areas of interests include Network Security and Cloud Computing.

Dr. K. Madhavi is Associate Professor in Computer Science and Engineering, JNTUA, Ananthapuramu, Andhra Pradesh, India. She received Ph.D. from JNTUA University. Her areas of interests include Wireless Networks, Image Processing, and Cloud Computing.