

Performance Evaluation Of Shadow Attacks Under No Password Re-Use Method

Kommuri Madhavalatha & Rodda Sireesha

#1 M.Tech Scholar, Department of Computer Science and Technology,

Gitam Institute Of Technology, Gitam (Deemed To Be University), Visakhapatnam -530 032.

#2 Ph.D, Department of Computer Science and Engineering,

Gitam Institute Of Technology, Gitam (Deemed To Be University), Visakhapatnam -530 032.

ABSTRACT

In current day's security plays a vital role in each and every domain which is used by almost all MNC and IT companies. As security plays an important role there was a vast improvement of information technology to give utmost security for the data which is stored and accessed by the various users. As the information is increasing day by day the storage area also increases with a number of different websites. A lot of users access their valuable information from a different websites; the security level of password-protected accounts is no longer purely determined by individual ones. Although different users may register multiple accounts on the same site or across multiple sites, and these passwords from the same users are likely to be the same or similar. If any attacker tries to hack one account credentials of a particular user, the same credentials can be used to break his other accounts related to him, so that all the other accounts will also be revealed due to these credentials. This type of attack is named as shadow attack on password reuse. Here in our proposed application we try to

implement two types of shadow attacks based on the functionality they vary with one another. The attack which occur for an user having same password for his multiple accounts within the same site is known as intra site password reuse (ISPR) and if the same user or different user match with similar passwords either in different sites rather than same site is termed as cross site password reuse (CSPR) approach. We will show both the attacks in our current application provide an alternate solution for both approaches by avoiding passwords not to be used during the time of registration.

Key Words: Security, Attacks, Account Credentials, Hacker, Password Protected, ISPR, CSPR.

I. INTRODUCTION

Now a day's there were a lot of security primitives that are available in literature to provide highest level of security for the sensitive data which is stored on various local or remote servers, but they failed in achieving highest level of security in various applications. In the current days the main fundamental task of a security

admin is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. One of the challenges that occur in the current days is the design of secure authentication protocols as we know that there is a lot of root kits reside in PCs (Personal Computers) to observe user's behavior and to make PCs untrusted devices[1]. Also involving human beings in authentication protocols as a promising approach, but it is not easy because of their limited capability of computation and memorization. Therefore rely on users to enhance security of the application mainly degrades the usability. In this paper, we mainly demonstrate how careful visualization design can enhance not only the security but also the usability of authentication protocol. To that end, we

propose two main visual authentication protocols:

- I. One is a one-time-password protocol, and
- II. The other is a password-based authentication protocol.

After a deep analysis, we verify that our protocols are immune to many of the challenging authentication attacks applicable in the literature. Furthermore, using an extensive case study on a prototype of our protocols[2], we highlight the potential of our approach for real-world deployment: we were able to achieve a high level of usability while satisfying stringent security requirements.

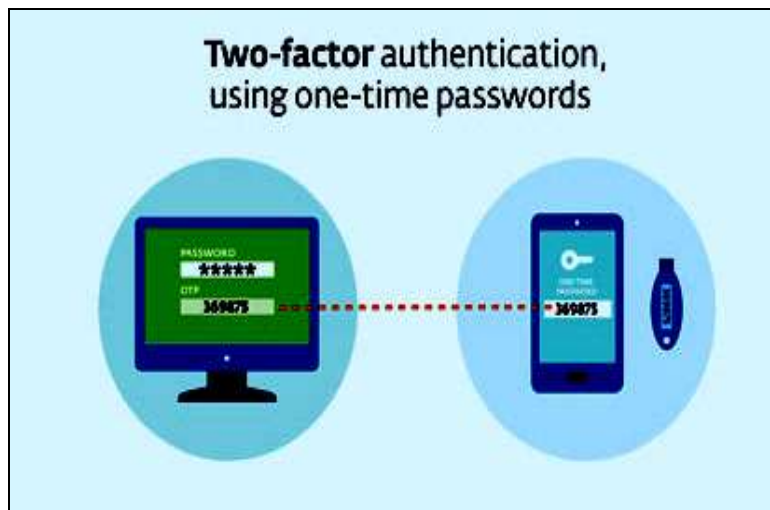


Figure 1. Represents the 2FA(Two Factor Authentication) using One-Time Passwords

From the above figure 1, we can get a clear idea that user while he need to get

login into in this site, he need to substitute the code which is displayed either in mobile

device or from any other sources like email id and so on[3]. If the code is correctly substituted in the box given below then the

page will be directed to the successful login, if not page will be directed to the error page.

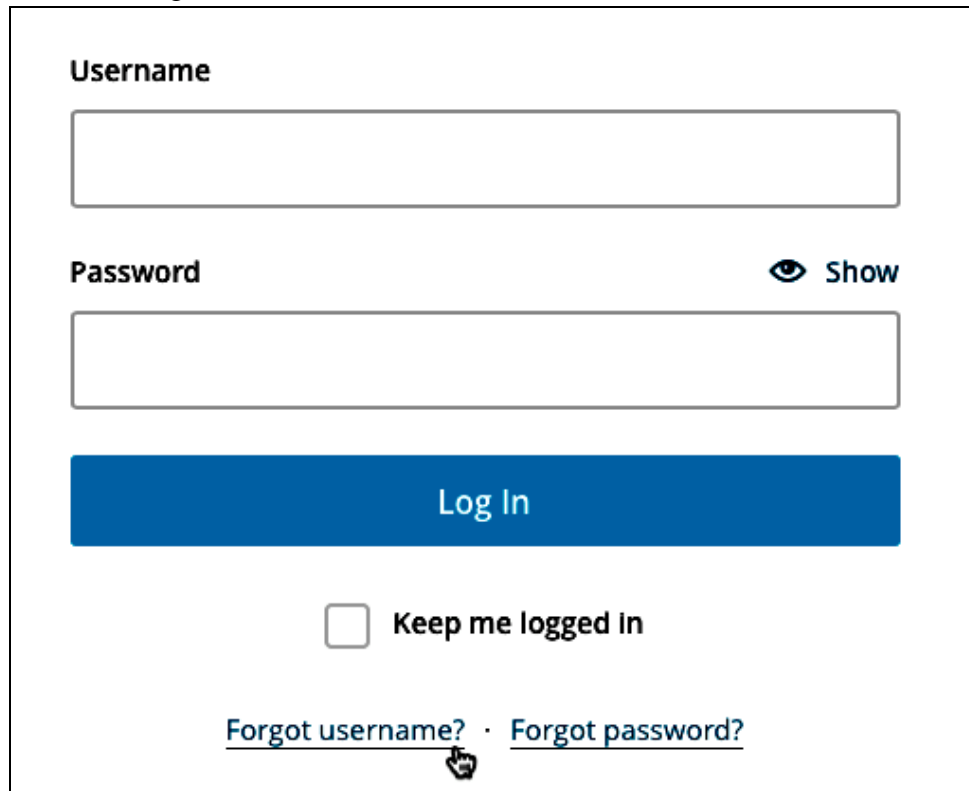
The login interface is enclosed in a black rectangular border. It contains a 'Username' label above a white text input field. Below that is a 'Password' label above another white text input field. To the right of the password field is an eye icon and the text 'Show'. A large blue button with the text 'Log In' is positioned below the password field. Underneath the button is a checkbox followed by the text 'Keep me logged in'. At the bottom of the form are two underlined links: 'Forgot username?' and 'Forgot password?'. A mouse cursor is shown pointing at the 'Forgot username?' link.

Figure 2. Represents the Login Interface with Username and Password for getting Login into the account. And the above window has the forget username and forget password option also

From the above figure 2, there is a window with two fields like username and password, where if any user or admin wants to enter into their account, he/she needs to substitute both the fields properly in the appropriate fields and then try to login into the account. If the username and password are wrong, the login attempt may be failed. If both credentials are correct, then only the user can be able to login or enter into the account. Also, we can see two more options like forgot username or forgot password, in

which if the user forgot any of the two options, he/she can be able to request those options. There is also another option like Keep me signed-In, in which if we choose this option, the password will be saved inside the cookies and the password is saved permanently in this system. This option has equal number of advantages as well as disadvantages in real-time usage. Coming to this password-based authentication system, most of the account users try to adopt this facility for authenticating their account. But mostly

this option is critical in the situations like more than one user account having save password or login credentials[4].This may lead to loose all the user accounts with similar login credentials.This motivated me to propose this current paper by concentrating more on Shadow attacks under password reuse[5].

II. BACKGROUND WORK

In this section we will mainly discuss about the background work that was carried out in order to prove the performance of our proposed analysis of shadow attacks based on password reuse. Now let us discuss about that in detail as follows:

MAIN MOTIVATION

In this section we will initially try to find out the reason behind designing this proposed model to avoid shadow attacks. The main reason behind this proposed model is password corpora ,which is the only reason why we motivated to design this proposed paper.In the year 2011,Dec 18th,there was a tremendous problem that occurred in china, where more than 70 million web accounts from four different famous websites were accidentally leaked to the public. This current incident is termed as “CSDN Password Leakage Incident”, because the first victim website was CSDN, one of the largest web communities for IT professionals in China. The CSDN leakage contains over six million accounts. Immediately following the CSDN leakage, a significant number of accounts of Tianya, duduniu, and 7k7k were leaked to the public in a similar manner.

TABLE 1
Basic Statistics of Leaked Passwords on Four Websites. Note that 7k7k has 8,825,710 accounts whose usernames are email addresses.

	Site Address	Amount	Valid Accounts	Data Type
CSDN	www.csdn.net	6,428,629	6,418,661	Username, Password, Email
Tianya	www.tianya.cn	30,179,474	26,337,242	Username, Password, Email
Duduniu	www.duduniu.cn	16,282,969	13,429,816	Username, Password, Email
7k7k	www.7k7k.com	19,138,270	5,047,665	Username (Email), Password
Total		72,029,342	51,233,384	

From the above table 1, we can clearly find out that there total 71 million number of accounts leaked from these four websites and the total number of distinct accounts after data preprocessing is 51,233,384. The leaked data from CSDN, Tianya, Duduniu include usernames, passwords, and email addresses, while the data from 7k7k contain usernames and passwords. The usernames of 8,825,710 accounts in 7k7k are email addresses.

In this section, we introduce background information of the four victim websites and their user base:

- CSDN [6] ranks first among all Chinese IT professional communities (one could consider it as a combination of MSDN.com and Slashdot.org). CSDN is a website announcing and reporting technology events as well as a technical forum. CSDN has more than 18 million registered individual users. The majority of

its user base is programmers and IT developers. It is currently ranked 473 in Alexa Top Global Sites (August 2015).

- Tianya [7] claims to be one of the largest Chinese online forums and blogs. Tianya has more than 65 million registered individuals and is known as one of the most influential Chinese forums. It is currently ranked 60 in Alexa Top Global Sites (August 2015).

- Duduniu [8] is a company site who mainly sells management platforms to Internet cafes (which provide Internet access to the public for a fee and are popular in China). Duduniu's services include billing tools and wholesales of vouchers for online games. The registered members of Duduniu are mainly owners or managers of Internet cafes.

- 7k7k [9] is a website collecting and sharing small flash games. Founded in 2003, 7k7k has become one of the top 50 popular Chinese websites as of September, 2009. The majority of its user base is young people[10]. It is currently ranked 4,021 in Alexa Top Global Sites (August 2015).

III. PROPOSED NOVEL SHADOW ATTACK EVALUATION BY NOT RE-USE OF SAME PASSWORDS

In this section we will find out the proposed novel shadow attack evaluation by not re-use of same passwords either of same user for same site or multiple accounts of that user in different sites.

PRELIMINARY KNOWLEDGE

In order to evaluate shadow attacks, we use the diverse password pairs in Dcdsp to perform the experiment, and diverse password pairs are distinct passwords of cross site accounts of the same users. In addition, we use the weaker passwords (compared by entropy [11]) in the diverse password pairs to guess the stronger ones. This shows the danger of the widely adopted users' behavior: using weaker passwords in low-valued accounts and stronger but similar ones in high-valued accounts.

The methods being tested include the following.

- 1) JtR default: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with JtR default rules.

- 2) JtR uni: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with added unigram prefix/suffix rules.

- 3) JtR bi: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with added unigram and bigram prefix/suffix rules.

- 4) JtR tri: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with added unigram, bigram and trigram rules

By analysis of above four factors we can able to achieve the following model in which shadow attacks can be eradicated by not using multiple accounts with same passwords.

IV. IMPLEMENTATION PHASE

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed novel IPath protocol. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My-SQL Server. The application is divided mainly into following 2 modules. They are as follows:

1. Data User Module
2. Admin Module

Now let us discuss about each and every module in detail as follows:

1. DATA USER MODULE

In the first module, every user need to register before he /she want to access the account. While registering into the site the user need to observe one important thing like no same password should be matched with his any of previous accounts of either the same site or different site with this current registration details. If there is any matching between current values with any of his or different users already registered accounts then the account can't be created. The system need to block the users not to get registered at this stage by telling the exact reason behind this failure. All these cases are monitored by the admin who gives authorization approval for the end users who try to register, login and access the information from the server.

2. ADMIN MODULE

In the module, the admin is one who will monitor and give all authorization access for the end users. Here the admin initially try to give login access for the newly registered user. The admin also has the facility for uploading the files or important documents into the server which is required for the end users. Also the admin can see the log information of both intra site password reuse attackers (ISPR) and cross site password reuse attackers(CSPR) information separately with invidual date and time.

Here the admin can see a graph analysis report for the total number of intra site attackers that are available in the application and total number of cross site attackers who are available inside the application. By having a detailed analysis the admin can figure out who is doing which sort of mistake in the current application. Here if any existed user try to login with a unique password during login and who wish to change the password which he remembers more in his change password option will be identified immediately by admin and he can't do such a operation.

V. CONCLUSION

In this paper, we for the first time have proposed a identification approach to detect the shadow attacks based on password reuse and try to optimize this shadow attacks by not using the same passwords for two or more accounts of same site or different sites. To the best of our knowledge, this is the first empirical study on web password reuses by analyzing a large number of sample data. Although the web password reuses are known to

researchers and Internet users, it is yet to perform a large-scale empirical study. We obtained 2,671,443 distinct users each of whom has at least two accounts from the

same site, and 2,306,055 distinct users each of whom had at least two accounts from different websites. We also obtained 350,849 distinct users who has at least two accounts on the same site and across sites simultaneously. We empirically studied the phenomenon of web password reuses (both ISPR and CSPR) utilizing the large password corpora and finally our experimental results clearly tell that our proposed approach is best in providing security against shadow attacks under no password reuse method.

VI. REFERENCES

- [1]. Luis von Ahn, Manuel Blum, Nicholas Hopper, and John Langford. CAPTCHA: Using Hard AI Problems for Security. In Proceedings of Eurocrypt, Vol. 2656 (2003), pp. 294-311.
- [2]. Bergmair, Richard (January 7, 2006). "Natural Language Steganography and an "AI-complete" Security Primitive". CiteSeerX: 10.1.1.105.129. (unpublished?)
- [3] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.
- [4] Z. Li, W. Han, and W. Xu, "A large-scale empirical analysis of chinese web passwords," in 23rd Usenix Security Symposium. San Diego: USENIX, 2014.
- [5] D. Wang, H. Cheng, Q. Gu, and P. Wang, "Understanding passwords of chinese users: characteristics, security and implications," <https://www.researchgate.net/>, July 2014.
- [6] CSDN, <http://www.csdn.net/company/about.html>.
- [7] Tianya, <http://help.tianya.cn/about/history/2011/06/02/166666.shtml>.
- [8] Duduniu, "http://baike.baidu.com/view/1557125.htm."
- [9] 7k7k, <http://www.7k7k.com/html/about.htm>.
- [10] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in 2012 IEEE Symposium on Security and Privacy (SP), 2012, pp. 538-552.
- [11] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, "Nist special publication 800-63-1 electronic authentication guideline," 2006.

VII.ABOUT THE AUTHORS



KOMMURI MADHAVILATHA is currently pursuing her 2 Years M.Tech (CST) in Department of Computer Science and Engineering at Gitam Institute of Technology, GITAM (DEEMED TO BE UNIVERSITY), Visakhapatnam, AP, India. Her area of interest includes Data Mining and Data Analysis.



RODDA SIREESHA is currently working as Associate Professor in Department of Computer Science and Engineering at Gitam Institute of Technology, GITAM (DEEMED TO BE UNIVERSITY), Visakhapatnam, AP, India. She has many years of teaching experience in engineering colleges. Her area of interest includes Data Mining and Data Warehousing.