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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

A solution to shadow attacks based on password reuses

T.V.S.Srivatsava[1], P.Sudheer Kumar[2]

UG Student, Department of Computer Science & Engineering, VVIT, Guntur[1]

Assistant Professor, Department of Computer Science & Engineering, VVIT, Guntur[2]

Abstract: The expansion of internet connectivity has increased development of many websites. There are several means of authentication mechanisms for every user to use those web applications. Of them password based authentication is widely used. User may show interest in working with other different applications but it becomes inconvenient for a user to remember several different passwords. So he/she uses same password in one domain to another domain. This leads to one of the cyber security threat called as shadow attacks.

Keywords: Authentication, Shadow Attacks, Cyber Security.

I. INTRODUCTION

There are varieties of gadgets and mechanisms were invented which enhances security of verification and validation. However most commonly used authentication is password based [1]. This is because password based authentication is cheaper than other mechanisms such as scanners and biometric which are most costly than password based authentication. So a user feels ease to use same passwords for multiple websites or same password for multiple accounts in a single domain [2]. So it becomes easier for a hacker to break through all accounts and retrieve sensitive information [3]. This is called as shadow attack. These attacks happen when a hacker uses many approaches to crack passwords such as brute force approach. This is referred as trial and error method. By using this hacker can use all possible combinations to crack the passwords. Secondly, there are dictionary attacks which can help a hacker to crack passwords. If a hacker manages to crack a single password, he could crack all accounts easily because there are many cases in which one account is interlinked to several domains. So there are many accounts prone to shadow attacks. We classify these attacks in to two categories. They are Intra-site password reuses and cross site password reuses.

Intra-site password reuses: If a user prefer using the same password of one account in one domain it is referred as intra-site password reuse.
Example: User of Gmail uses same password in multiple accounts.
Cross-site password reuses: If a user prefer using a password of one domain to another domain is referred as cross-site password reuse.

Recently in china there was a large disaster occur due to the password reuses [4]. The famous website which was storing the numerous number of people data was publicly leaked. Thus the secure password is now available in public. The intruders, hackers, spoofers are pretty much used the leaked password. Thus many people suffer a lot due to this disaster. Also most of the people who are from different occupation such as Administrator, Business Man, common people government worker maintain their data in database of that particular site to use it in anywhere at any time. But the problem arises due to repeated passwords. The repeated use of one password in other site eased the work of hackers to break in their accounts. Most of the citizens of china reused their passwords in many sites[9]. Although Chinese users do prefer a different set of character set (e.g., digits) than English-speaking users (e.g., who prefer letters), they both create passwords at the similar strength [10].Citizens of China use to store their data in different site or the same site caused a problem when the data base leaked. The password is publicly taken by the hackers. Then they apply the password in various scenarios such as bank account, user details, passbook etc. The misuse of the revealed data is violently affecting most of the citizens in china. There are several works considered through Lavenshtein algorithm. Here we introduce a method for protecting web passwords from shadow attacks using the concept of rainbow table methodology and password cracking algorithm.

II. RELATED WORK

Robert Morris and Ken Thompson proposed and elaborate the idea about Password Security with deep history

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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

evaluation. Here they implemented the UNIX based systematic approach for securing the OS. Here the password is used to maintain a simple data using the Encryption format. The mechanism they used to try to proposed is of simple and ethnic way at which the data can be simply poster and the user needs to select the key for encrypting the file using the required key. Thus the encryption is done while storing in the database. Thus once the user selects the password and they enter into the database. In the data base storage inbuilt key provided by the sites was maintained. When the password entered it automatically encrypt the password and the encrypted data stored in the data base. Which it leads to time consuming. When there is additional pattern issue the password may get corrupted. Evaluation of two decades of proposals to replace text passwords for general-purpose user authentication on the web using a broad set of twenty-five usability, deploy ability and security benefits that an ideal scheme might provide. The scope of proposals we survey is also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. Our comprehensive approach leads to key insights about the difficulty of replacing passwords. Not only does no known scheme come close to providing all desire benefits: none even retains the full set of benefits that legacy passwords already provide. In particular, there is a wide range from schemes offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to use. We conclude that many academic proposals have failed to gain traction because researchers rarely consider a sufficiently wide range of real-world constraints. Beyond our analysis of current schemes, our framework provides an evaluation methodology and benchmark for future web authentication proposals.

The problem of shadow attack based on password reuse technology overcome by Weili Han, ChenSun, ChenguangShen, Chang Lei, eanShen presents combining multiple factors during authentication, a service can provide better assurance of security. However, the users are likely to feel inconvenient, or even discard the service. This paper, therefore, addresses this issue and introduces a novel method, referred to as the Quantified risk and Benefit adaptive Authentication Factors combination (QSBAF). QSBAF balances the requirements for both security and usability in the authentication of an information system and improves the system's ability to respond quickly to emerging risky events. In QSBAF, the authentication factors can be dynamically combined on the basis of quantified risk, benefit measurements, and combination policies. Furthermore, QSBAF provides an adaptive mechanism, which is driven by history data to justify the measurements of risk and benefit. In this paper, we use the online banking system as a typical scenario to demonstrate the usage of QSBAF.

We also implement a prototype of QSBAF to evaluate the performance of its feasibility in real application scenarios. In this paper we are going to introduce one of our methods to prevent this shadow attacks based on password reuses by using our password cracking algorithm and rainbow table methodology. We develop the first cross-site password-guessing algorithm, which is able to guess 30% of transformed passwords within 100 attempts compared to just 14% for a standard password-guessing algorithm without cross-site password knowledge.

III. EXISTING METHODOLOGY

In previous mechanism the data that stored in the normal database is not valuable it can be processed and maintain in a simple scheme of which it should be used. The main use of the database is used to protect the data. If any one of the malfunction done in that website is not accurate. A person can register several accounts on websites. If their registered email addresses are the same, we believe these accounts belong to the same user. That a person may use multiple emails addresses to register multiple accounts, and addition information could be obtained to link these email addresses. For example let us consider Gmail. It allows users to create multiple accounts with same password. For example user's corresponding friends may be aware of the linkage or it can be identified by the same email name but different email domain. So the passwords can be easily leaked.

A. Problem identification methodology:
The shadow attack prevention is maintained in this module here the data that is used to process for the simple and efficient dual core process maintained using honey pot pattern the honey pot pattern is used to maintain used for simple process. This should be avoided with the mesh related format.

The Shadow Honey pot architecture is a systems approach to handling network-based attacks, combining filtering, anomaly detection systems and honeypots in a way that exploits the best features of these mechanisms, while shielding their limitations. Our architecture is not limited to server applications, but can be used for client-side applications such as web browsers, P2P clients, etc.

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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

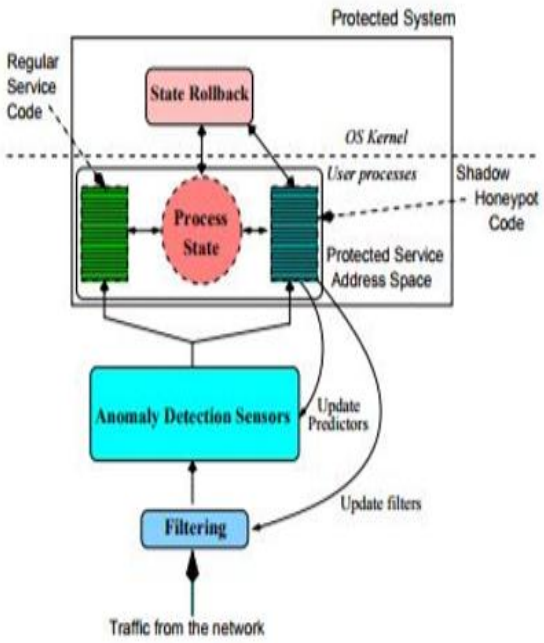


Fig 1: Architecture of Honey pot method for shadow attacks prevention**.**

IV THE PROPOSED METHODOLOGY

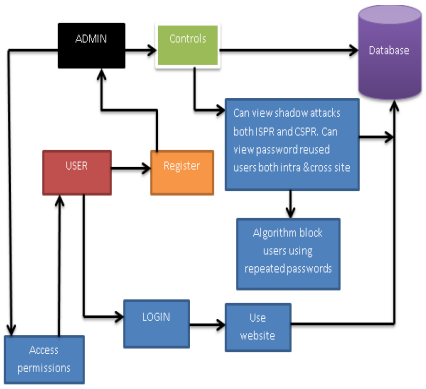


Fig 2: The pictorial representation.

These are the following modules in our project:

A. Admin:

Admins responsibility is to make sure to give access permissions to the users. Secondly, admin can view users who have repeated passwords so that action could be taken to them. He can view graphs of intra and cross sites users with repeated passwords.

B. User:

User can use website and can perform various actions like changing their data or data posting. And basing on user action the application responds. If a user reuse their passwords the application prevents user from using so as to eradicate these shadow attacks.

C. User classification:

The next process is the user classification mechanism. The user classification mechanism is designed with the two data set process one is ISPR and another one is CSPR .The ISPR is derived as the Intra site password reuse and the CSPR designed for the cross site password reuse. They can be viewed by admin using our rainbow table mechanism.

D. Dataset Design:

Dataset design is the next design of module. The modelled purposes are used to avoid the data set leakage in the system. Here the data set is designed with the clustering and also the hierarchical process. The clustering is the

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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

grouping mechanisms were the data are designed with the simple and effective process. The hierarchical model is used to link between the resource and the system .The process usability is used to link between the resource and performancemaintenance of the system is used to design. The usage of data set is used to avoid the resource leakage of the user and guarantees the security mechanism.

V. PASSWORD REUSE RATES

Rates of different user group result confirms our hypotheses that users in academic organizations are better educated with web security than common users and tend to use different passwords for accounts in different websites. Another reason may be that users incline to reuse passwords when registering with low-valued or easily replaceable email accounts. Academic emails, however, are difficult to be replaced. To measure the password strength, we adopt the same metrics used by Bonneau [7]. On the contrary, it is interesting to find out that users with international email addresses are most likely to reuse their passwords cross site. Surprisingly, VIP users, those who would pay annual fees for their email addresses, also have a high rate of cross-site password reuses, which is second to I18n users. In China due to these password reuses shadow attacks have occurred. And many users passwords were leaked. These leaked passwords are from four main-stream websites with millions of users in China: CSDN [5], Tianya [6], Duduniu [7], 7k7k [8].

Rates of CSPR between Two Sites.

	Tianya	Duduniu	7k7k
CSDN	33.29% (745,451)	27.10% (203,791)	35.69% (239,974)
Tianya	-	30.74% (497,772)	0.00% (416,514)
Duduniu	-	-	38.96% (468,010)

Fig 3: The rates of cross-site password reuse between two sites

V Algorithm and process used for cracking

E. Password cracking Algorithm:

Algorithm 1 Shadow Attacks

Input: Input password α and target password β
Intermediate result: Candidate password α'
Output: Re Used or Not Re Used
Check (α', β): if $\alpha' = \beta$ **return** Cracked
if α contains any sequential pattern **then**
  Sequential Transformation$(\alpha) \rightarrow \alpha'$
  Check (α', β)
end if
if len(α)>6 **then**
  $\alpha' \leftarrow$ Deletion(α)
  Check (α', β)
end if
if len(α)<10 **then**
  $\alpha' \leftarrow$ Insertion(α)
  Check (α', β)
end if
Capitalization$(\alpha) \rightarrow \alpha'$
Check (α', β)
Reverse$(\alpha) \rightarrow \alpha'$
Check (α', β)
Leet$(\alpha) \rightarrow \alpha'$
Check (α', β)
Substring Movement$(\alpha) \rightarrow \alpha'$
Check (α', β)
Subword transformation$(\alpha) \rightarrow \alpha'$
Check (α', β)
return Not Cracked

Fig 4: Password cracking algorithm.

The above algorithm is useful for cracking the relevant passwords in any website. We take an input password as alpha and target password as beta. The intermediate result is candidate password. Ultimately we derive whether the user is reusing their passwords or not. In this algorithm we first check the length of password and thereby we apply substitution and various sequence of transformations for given passwords. These random changes in current string derive the matched password. If the current password matches the older one it is said to be cracked password and thereby we can determine this current password causes shadow attack.

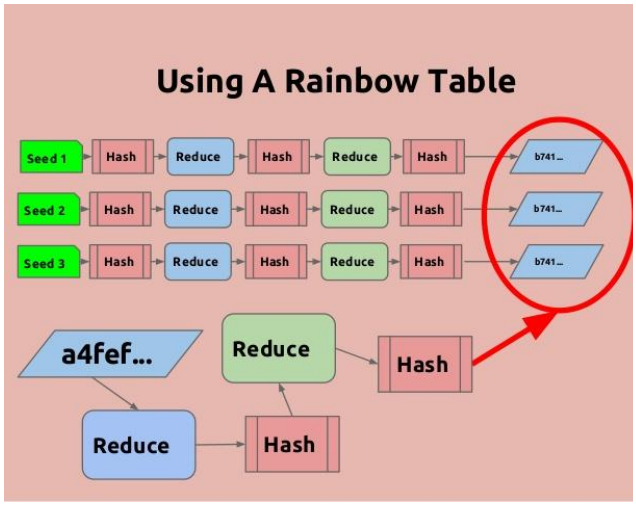
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

F. Rainbow Table:

Rainbow table is a pre computed table for reversing cryptographic hash functions. Basically it is used for cracking passwords. We use this rainbow table mechanism and password cracking algorithm for cracking passwords so as to prevent the shadow attacks. These rainbow tables can be used for cracking plain text passwords easily.



G. Fig 5: Rainbow Table.

III. VI EXPERIMENTAL RESULTS

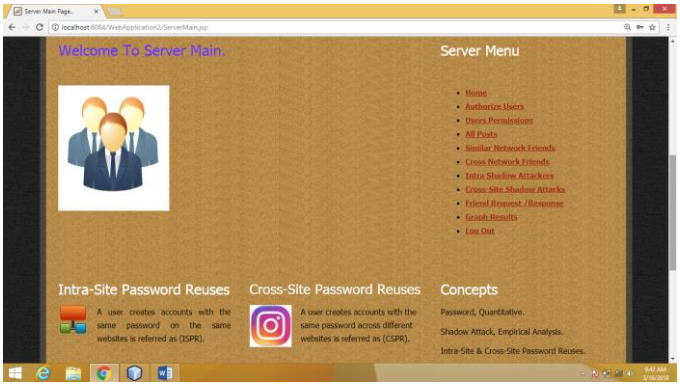


Fig 6**:** Admin module.

Admin can authorize users, give access permissions and can view both intra and cross sit shadow attacks. There are results graph through which admin can understand how many intra and cross site attackers are there. ISPR and CSPR of a user can be identified by the admin. Thereby shadow attacks can be prevented.

Fig 7: Intra site shadow attackers.

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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

Intra site password attackers are found in this tabular format. Thereby the users who are performing shadow attacks can be identified. Here on observation we can identify any user log details. It defines he is using the same password of other user in this site thereby he I an intra-shadow attacker or an ISPR (Intra-site password re user).

Fig 8: Cross site shadow attackers.

Cross site password attackers are found in this tabular format. Thereby the users who are performing shadow attacks can be identified. Here on observation we can identify a user log details. It defines he is using the same password in multiple sites thereby he is an cross-site shadow attacker or CSPR (Cross site password re user).

Fig 9: User module.

In users module user can register for any domain and can use the website. Depending on his passwords the application functionality is determined. By this application a user can understand how shadow attacks are caused. Here we take four sites like Facebook, twitter, LinkedIn, Pintrest. We include these dummy sites and define how shadow attacks are caused and how they are prevented.

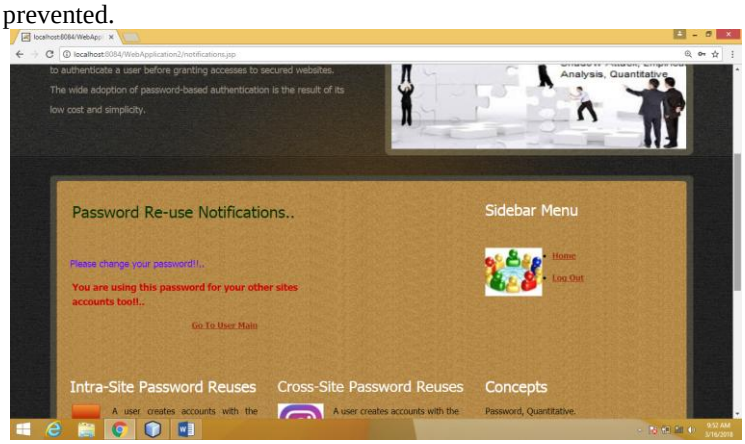


Fig 10: Blocking password reuses.

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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

If a user reuses his password in another account the user is blocked and hence the shadow attacks can be prevented by this methodology. Because password reuse is the main factor for shadow attacks. So by reducing reused passwords we can improvise the strength of user account.

Fig 11: Intra-Cross site password reuse graph.

Through this graph admin can understand the ratio of users who are reusing their passwords. Through this graph we can understand that few number of users are reusing their password in intra-site, And others in cross-site. This analysis can help administrator to control password reuses and thereby prevent the shadow attacks.

VII CONCLUSION

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 have 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. Although the password reuses are known to researchers for years, a large-scale in-depth empirical analysis of password reuses is still absent so far. Das et al. [2] leverage 6,077 distinct accounts. The quantitative answers shed lights on the serious threat of web password reuses, i.e., password shadow attacks, where an adversary may attack an account of a user using the same or similar passwords of his/her other less sensitive accounts. As a future direction, we would study CSPR from both adversaries and defenders points of view, leveraging the logs or activities that are available in the public domain. By using our algorithm methodology we can prevent shadow attacks. In addition, we will evaluate how the password policies affect CSPR after understanding the policies of many websites.

REFERENCES

[1] R. Morris and K. Thompson, "Password security: A case history," Communications of the ACM, vol. 22(11), pp. 594–597, 1979.
[2] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in NDSS'2014, 2014.
[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW'07 Proceedings of the 16th international conference on World Wide Web, 2007, pp. 657–666.
[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] CSDN, "http://www.csdn.net/company/about.html."
[6] Tianya, "http://help.tianya.cn/about/history/2011/06/02/ 166666.html."
[7] Duduniu, "http://baike.baidu.com/view/1557125.html."
[8] 7k7k, http://www.7k7k.com/html/about.html.
[9] D. Wang, H. Cheng, Q. Gu, and P. Wang, "Understanding passwords of chineseusers:characteristics, security and implications," https://www.researchgate.net/, July 2014.
[10] 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.