Authentication by Encrypted Negative Password

Poornima S[1] ,Nivetha M[2], Pradeep Kumar M[3] Asst. Prof. Subathra S [4]
[1,2,3] Student Department of Computer Science and Engineering
[4] Assistant Professor in Computer Science and Engineering
Velalar College of Engineering and Technology, Thindal, Erode-12.

Abstract **Secure password storage is a vital aspect in systems based on password authentication, which is still the most widely used authentication technique, despite its some security flaws. In this paper, we propose a password authentication framework that is designed for secure password storage and could be easily integrated into existing authentication systems. In our framework, first, the received plain password from a client is hashed through a cryptographic hash function (e.g., SHA-256). Then, the hashed password is converted into a negative password. Finally, the negative password is encrypted into an Encrypted Negative Password (abbreviated as ENP) using a symmetric-key algorithm (e.g., AES), and multi-iteration encryption could be employed to further improve security. The cryptographic hash function and symmetric encryption make it difficult to crack passwords from ENPs. Moreover, there are lots of corresponding ENPs for a given plain password, which makes precomputation attacks (e.g., lookup table attack and rainbow table attack) infeasible. The algorithm complexity analyses and comparisons show that the ENP could resist lookup table attack and provide stronger password protection under dictionary attack. It is worth mentioning that the ENP does not introduce extra elements (e.g., salt); besides this, the ENP could still resist precomputation attacks. Most importantly, the ENP is the first password protection scheme that combines the cryptographic hash function, the negative password and the symmetric-key algorithm, without the need for additional information.**

Keywords - Plain password ,Cryptographic hash function, Encrypted negative password, Symmetric key algorithm.

1.INTRODUCTION

Owing to the development of the Internet, a vast number of online services have emerged, in which password authentication is the most widely used authentication technique, for it is available at a low cost and easy to deploy Hence, password security always attracts great interest from academia and industry . Despite great research achievements on password security, passwords are still cracked since users' careless behaviors . For instance, many users often select weak passwords they tend to reuse same passwords in different systems they usually set their passwords using familiar vocabulary for its convenience to remember . In addition, system problems may cause password compromises. It is very difficult to obtain passwords from high security systems. On the one hand, stealing authentication data tables (containing usernames and passwords) in high security systems is difficult. On the other hand, when carrying out an online guessing attack, there is usually a limit to the number of login attempts . However, passwords may be leaked from weak systems . Vulnerabilities are constantly being discovered, and not all systems could be timely patched to resist attacks, which gives adversaries an opportunity to illegally access weak systems . In fact, some old systems are more vulnerable due to their lack of maintenance. Finally, since passwords are often reused, adversaries may log into high security systems through cracked passwords from systems of low security

2.BACKGROUND

Joseph Bonneau, Cormac Herley, said that the theory on passwords has lagged behind practice, where large providers use back-end smarts to survive with imperfect technology. Simplistic models of user and attacker behaviors have led the research community to emphasize the wrong threats. Authentication is a classification problem amenable to machine learning, with many signals in addition to the password available to largeWeb services. Passwords will continue as a useful signal for the foreseeable future, where the goal is not impregnable security but reducing harm at acceptable cost.

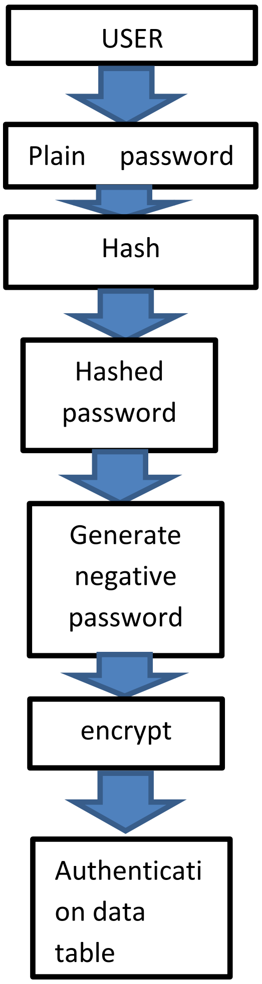
Ch Gopal Krishna and R Bala Dinakar, This development brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this tricky, we proposed a novel authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login pointer and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks.

Mr. Rudresh Gurav , Ms. Leena Dabhade, To increase password security, online authentication systems have started to enforce stricter password policies. We introduce a new metric called Coverage to quantify the correlation between passwords and personal information. Personal-PCFG cracks passwords much faster than PCFG and makes online attacks much more likely to succeed. We examine the use of simple distortion functions that are chosen by users to mitigate unwanted correlation between personal information and passwords. To increase password security, online authentication systems have started to enforce stricter password policies. Password re-generation method is available in this system.

3.PROPOSED METHOD

To protect passwords in an authentication data table, the system designer must first select a cryptographic hash function and a symmetric-key algorithm, where the condition that must be satisfied is that the size of the hash value of the selected cryptographic hash function is equal to the key size of the selected symmetric-key algorithm. For convenience, some matches of cryptographic hash functions and symmetric-key algorithms. In addition, cryptographic hash functions and symmetric-key algorithms that are not listed here could also be used in the ENP, which adequately indicates the flexibility of our framework. The proposed framework is based on the ENP; hence, for better understanding, the data flow diagram of the generation procedure of the ENP.

3.1 DATA FLOW DIAGRAM:



4.MODULES DESCRIPTION

4.1 Data Owner

In this module, the data owner uploads their data in the Web server. For the security purpose the data owner encrypts the data file and then store in the Web. The Data owner can have capable of manipulating the encrypted data file. The data owner will send Meta data to Audit Web. In audit Web raw or metadata information is available for auditing and data integrity checking purpose. Data owner will create an end user and the data owner can set the access permission (read or write) to user and also Verifies Password.

4.2 Data Auditing and Verification

The data owner can also audit the data integrity in the corresponding Web for verifying whether the data is safe or not using digital sign and web URL. If the data is not safe then he will delete the data and re upload the data to the corresponding Web server.

4.3 Web Server

The Web server is responsible for data storage and file authorization for an end user. The data file will be stored with their tags such as file name, secret key, digital sign, and owner name. The data file will be sending based on the privileges. If the privilege is correct then the data will be sent to the corresponding user and also will check the file name, end user name and secret key. If all are true then it will send to the corresponding user or he will be captured as attacker. The Web server can also act as attacker to modify the data which will be auditing by the audit Web and also View All Encrypted Negative Password, View All Attacker, View All Password Attackers.

4.4 Data Consumer(End User)

The data consumer is nothing but the end user who will request and gets file contents response from the corresponding Web servers. If the file name and secret key, access permission is correct then the end is getting the file response from the Web or else he will be considered as an attacker and also he will be blocked in corresponding Web. If he wants to access the file after blocking he wants to UN block from the Web and also verifies password.

Attacker is one who is integrating the Web file by adding malicious data to the corresponding Web. They may be within a Web or from outside the Web. If attacker is from inside the Web then those attackers are called as internal attackers. If the attacker is from outside the Web then those attackers are called as external attackers.

4.5 Data Consumer(End User)

The data consumer is nothing but the end user who will request and gets file contents response from the corresponding Web servers. If the file name and secret key, access permission is correct then the end is getting the file response from the Web or else he will be considered as an attacker and also he will be blocked in corresponding Web. If he wants to access the file after blocking he wants to UN block from the Web and also verifies password.

4.6 Attacker

Attacker is one who is integrating the Web file by adding malicious data to the corresponding Web. They may be within a Web or from outside the Web. If attacker is from inside the Web then those attackers are called as internal attackers. If the attacker is from outside the Web then those attackers are called as external attackers.

5.CONCLUSIONS

In this paper, we proposed a password protection scheme called ENP, and presented a password authentication framework based on the ENP. In our framework, the entries in the authentication data table are ENPs. In the end, we analyzed and compared the attack complexity of hashed password, salted password, key stretching and the ENP. The results show that the ENP could resist lookup table attack and provide stronger password protection under dictionary attack. It is worth mentioning that the ENP does not need extra elements (e.g., salt) while resisting lookup table attack.

5.1 FUTURE WORK

In the future, other NDB generation algorithms will be studied and introduced to the ENP to further improve password security.Furthermore, other techniques, such as multi–factor authentication and challenge–response authentication.

REFERENCES

[1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “Passwords and the evolution of imperfect authentication,” Communications of the ACM, vol. 58, no. 7, pp. 78–87, Jun. 2015.

[2] M. A. S. Gokhale and V. S. Waghmare, “The shoulder surfing resistant graphical password authentication technique,” Procedia Computer Science, vol. 79, pp. 490–498, 2016.

[3] J. Ma, W. Yang, M. Luo, and N. Li, “A study of probabilistic password models,” in Proceedings of 2014 IEEE Symposium on Security and Privacy, May 2014, pp. 689–704.

[4] A. Adams and M. A. Sasse, “Users are not the enemy,” Communications of the ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999

[5] E. H. Spafford, “Opus: Preventing weak password choices,” Computers & Security, vol. 11, no. 3, pp. 273–278, 1992.

[6] Y. Li, H. Wang, and K. Sun, “Personal information in passwords and its security implications,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2320–2333, Oct. 2017.

[7] D. Florencio and C. Herley, “A large-scale study of web password habits,” in Proceedings of the 16th International Conference on World Wide Web. ACM, 2007, pp. 657–666.

[8] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, “Designing password policies for strength and usability,” ACM Transactions on Information and System Security, vol. 18, no. 4, pp. 13:1–13:34, May 2016.

[9] D. Wang, D. He, H. Cheng, and P. Wang, “fuzzyPSM: A new password strength meter using fuzzy probabilistic context-free grammars,” in Proceedings of 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Jun. 2016, pp. 595–606.

[10] H. M. Sun, Y. H. Chen, and Y. H. Lin, “oPass: A user authentication protocol resistant to password stealing and password reuse attacks,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, Apr. 2012.

[11] M. Zviran and W. J. Haga, “Password security: An empirical study,” Journal of Management Information Systems, vol. 15, no. 4, pp. 161– 185, 1999.

[12] P. Andriotis, T. Tryfonas, and G. Oikonomou, “Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method,” in Proceedings of Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, 2014, pp. 115– 126.