International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Securing Passwords using Encrypted Negative Password

Mary Lidhiya

Student, Dept. of Computer Applications, Christ Knowledge City college, Kerala, India

---

Abstract - *Hacking and password cracking are becoming vulnerable day by day with the advancements in technology. Password storage and encryption have to be made more secured to escape from these fraudulent activities. In this project, we preferred a password encryption method which will add more security in password storage and can be implemented easily in every password authentication platform. This is a strong encryption method where it is very difficult to breech the security by cracking passwords thus gaining un-authorized access to personal information. Here, the first thing that we do is to hash the plain password entered by the user by using a cryptographic hash function. And secondly, we convert the hashed password into a negative password. And finally the negative password is again encrypted into an encrypted negative password by using a symmetric key algorithm. This multi iteration encryption method helps in preventing attacks such as lookup table attacks and rainbow table attacks. And the algorithm makes it really harder for hackers and attackers to breech through, and provides a strong password protection against security threats.*

***Key Words*: ENP, Negative Database, Security, Decryption, Hash Function.**

1. INTRODUCTION

Along with the development of the Internet, a huge 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, while carrying out an online guessing attack, there is usually a limit to the number of login attempts. However, weak systems results in leaking passwords. Vulnerabilities are constantly being discovered, and not all systems could be able to resist attacks, which affect the system and 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.

In this paper, a password protection scheme called Encrypted Negative Password is proposed, which is based on the Negative Database. Here, the first thing that we do is to hash the plain password entered by the user by using a cryptographic hash function. And secondly, we convert the hashed password into a negative password. And finally the negative password is again encrypted into an encrypted negative password by using a symmetric key algorithm. This multi iteration encryption method helps in preventing attacks such as lookup table attacks and rainbow table attacks. And the algorithm makes it really harder for hackers and attackers to breech through, and provides strong password protection against security threats.

This scheme can be implemented in the places where high security is needed. So that in this paper we implement the security using ENP technique in police administrative areas where the police officers in each station can upload and view the case files under their control. They can safely store and access their files using this ENP technique without worrying about hacking their confidential data.

2. PROPOSED FRAMEWORK

The proposed framework includes two phases: The Registration phase and Authentication phase .When adopting our frame work to protect passwords in an authentication data table, the system designer must first select 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.

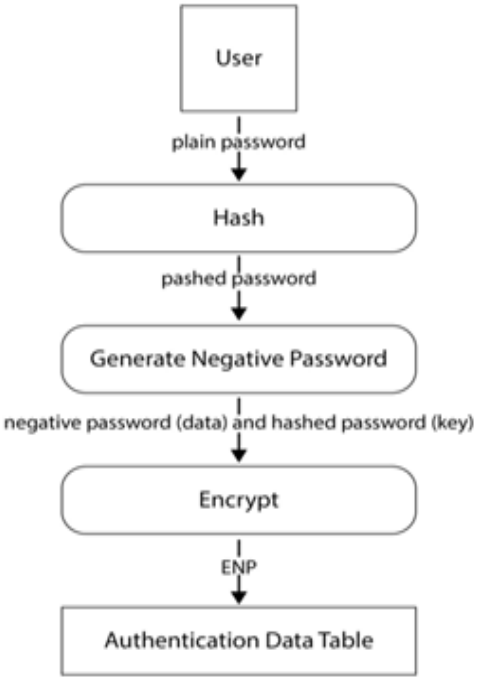


Fig -1: Data flow diagram of the generation procedure of the ENP

In registration phase on the client side, a user enters username and password. Then, the username and plain password are transmitted to the server through a secure channel. The received password is hashed using the selected cryptographic hash function. The hashed password is then transformed into a negative password using an Negative database generation algorithm. The negative password is encrypted to an ENP using the selected symmetric-key algorithm, where the key is the hash value of the plain password. Here, as an additional option, multi-iteration encryption could be used to further enhance passwords. The username and the resulting ENP are stored in the authentication data table and "Registration success" is returned, which means that the server has accepted the registration request.

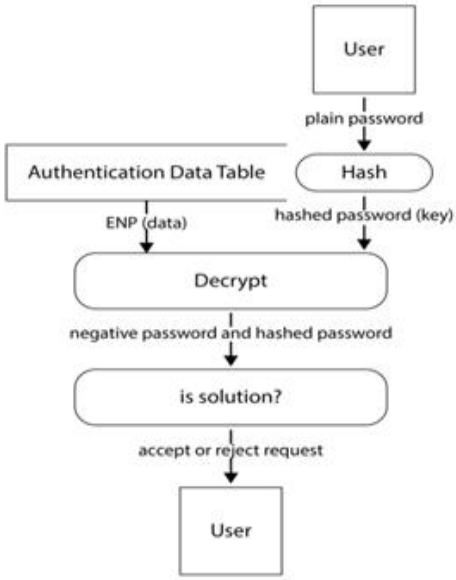
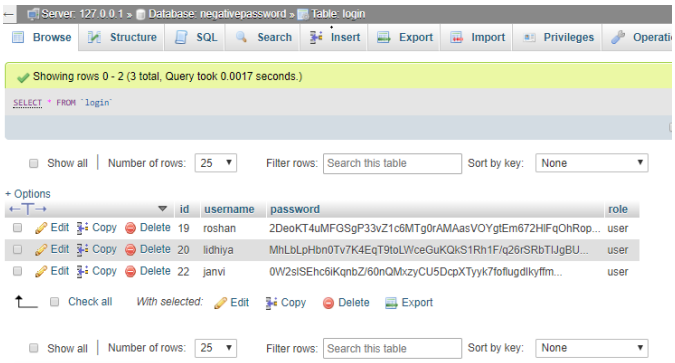


Fig -1: Data flow diagram of the verification procedure of the ENP

In authentication phase, on the client side, a user enters his/her username and password. Then, the username and plain password are transmitted to the server through a secure channel. The ENP is decrypted using the selected symmetric-key algorithm, where the key is the hash value of the plain password; thus, the negative password is obtained. If the hash value of the received password is not the solution of the negative password, then "Incorrect username or password!" is returned.



3. CONCLUSIONS

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 while resisting lookup table attack.

ACKNOWLEDGEMENT

I would like to thank my teachers, friends and family who helped me to accomplish this paper.

REFERENCES

[1] "One-time password authentication scheme based on the negative database" DongdongZhaoa,b, Wenjian Luoa,2015.

[2] ."Negative Iris Recognition" Dongdong Zhao, WenjianLuo, Senior Member, IEEE, Ran Liu, and Lihua Yue,2016.