Authentication by Encrypted Negative Password

Jobin Thomas Alummoottil
PG Scholar
Department of Master of Computer Application
Amal Jyothi College of Engineering
Kottayam, Kerala, India

Rony Tom
Assistant Professor
Department of Master of Computer Application
Amal Jyothi College of Engineering
Kottayam, Kerala, India

Abstract- This paper is about securing the passwords and making devices more secured from intruders. Most of systems today makes use of the technique in which the passwords are simply encrypted and aren't secured properly. This encrypted negative password system uses the technique in which inside the passwords are first hashed and then converted to negative password and eventually encrypted and stored within the database. But the processor and storage sources are getting increasingly more considerable, hashed passwords can't face up to precomputation assaults, which includes rainbow desk attack and lookup desk attack. This Encrypted Negative Password device still can resist the precomputation attacks. For that reason, by way of securing the pages with negative password machine, these types of vulnerabilities may be decreased.

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

I. INTRODUCTION

Due to the growth of the Internet, a plethora of online services have evolved, with password authentication being the most generally used authentication method due to its low cost and ease of implementation. As a result, password security has long piqued the interest of academia and industry. Despite significant advancements in password security research, passwords are still cracked as a result of users' sloppy behavior. For example, many users frequently choose weak passwords, and they frequently reuse the same passwords across several systems. They also frequently use familiar terminology to make passwords easier to remember. Passwords may also be compromised as a result of system issues. Flaws are continually being identified, and not all systems can be upgraded in time to withstand attacks, giving attackers the chance to enhance unauthorized access to vulnerable systems. In fact, because to a lack of maintenance, several older systems are more insecure. Finally, because passwords are frequently repeated, attackers may be able to log into high-security systems using passwords cracked from low-security systems.

II. BACKGROUND

According to Joseph Bonneau, Cormac Herley, password theory has fallen behind practice, with huge providers relying on back-end smarts to get by in the face of flawed technology. The research community has focused on the incorrect risks due to simplistic models of user and attacker behavior. Authentication is a classification problem suited to machine learning, with various signals available to largeWeb services in addition to the password. For the foreseeable future, passwords will serve as a helpful signal, with the purpose of decreasing harm at an acceptable cost rather than providing impenetrable protection.

R Bala Dinakar and Ch Gopal Krishna, This improvement is really convenient, but it also raises the risk of credentials being exposed to shoulder surfing assaults. Attackers can obtain users' credentials by watching them or using external recording equipment. To combat this, we introduced Pass Matrix, a revolutionary authentication method based on graphical passwords that can withstand shoulder surfing assaults. Pass Matrix provides no suggestion for attackers to find out or narrow down the password, even if they execute several camera-based assaults, with a one-time valid login pointer and circulative horizontal and vertical bars encompassing the whole scope of pass-images.

Mr. Rudresh Gurav, Ms. Leena Dabhade, Online authentication systems have begun to impose tougher password requirements in order to improve password security. To measure the association between passwords and personal information, we create a new statistic called Coverage. Personal-PCFG breaks passwords significantly quicker than PCFG and increases the likelihood of successful online assaults. We look at how users may choose basic distortion methods to reduce undesired association between personal information and passwords. Online authentication systems have begun to impose tougher password requirements in order to improve password security. This system has a way for regenerating passwords.

III. EXISTING SYSTEM

The present system makes use of the most basic mechanism of all the other methods. The simple password is simply encrypted before being saved in the database. This technique is extremely unsafe, and you may easily attack it and obtain the password. The hashing method, in which the raw password is hashed using hashing techniques such as the Secure Hash Algorithm or the Message Digest Algorithm, is the other primary technique still in use today. In comparison to the previous approach, it provides better security and also delivers the hashed value of the password rather than the real password. The plain password, on the other hand, may be derived from the hashed value obtained through the rainbow

10.5281/zenodo.5105435
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

table and lookup table attacks. As a result, we use the Encrypted Negative Password System to limit susceptibility and risk.

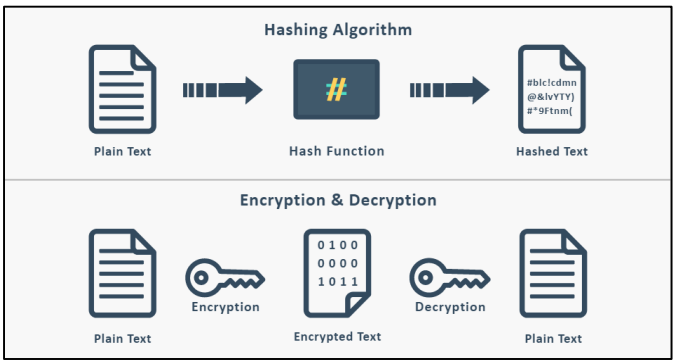
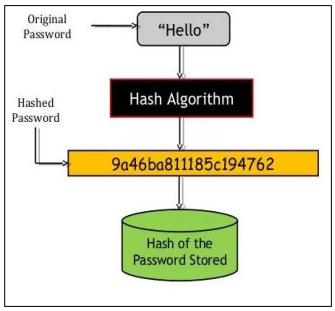


Fig. Normal Hashing Algorithm



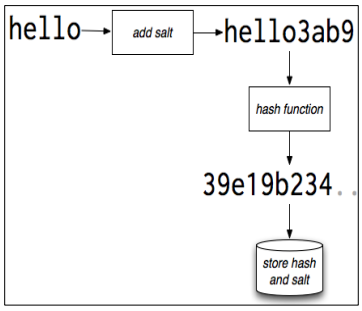


Fig. Normal Hash Password Fig. Salted Password

IV. PROPOSED SYSTEM

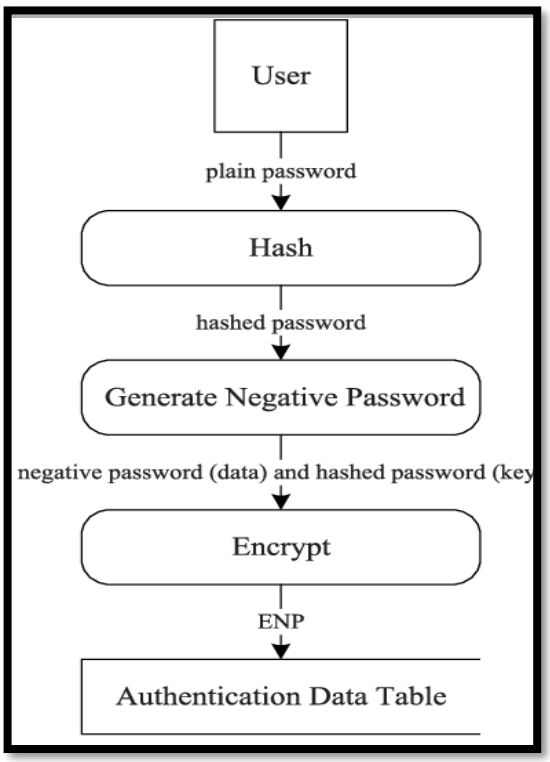
To secure passwords in an authentication data table, the system designer must first choose a cryptographic hash function and a symmetric-key algorithm, with the requirement that the size of the cryptographic hash function's hash value is equal to the key size of the symmetric-key method. Some cryptographic hash functions and symmetric-key methods are matched for convenience. In addition, other cryptographic hash functions and symmetric-key algorithms that aren't specified here might be employed in the ENP, demonstrating the framework's versatility.

In general, password protection solutions include:

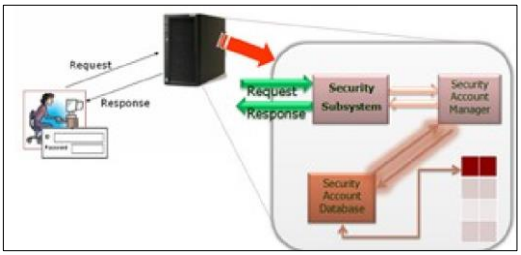
1) Hashed Password: A plain password is retrieved from the user and can be stored as such with just encryption, but this is not secure. To hash the password, we utilize the cryptographic hash function.

2) Salted Password: We employ the salted password strategy to prevent precomputation attacks, in which the plain password is concatenated with a random value (salt) and hashed.

V. DATA FLOW DIAGRAM

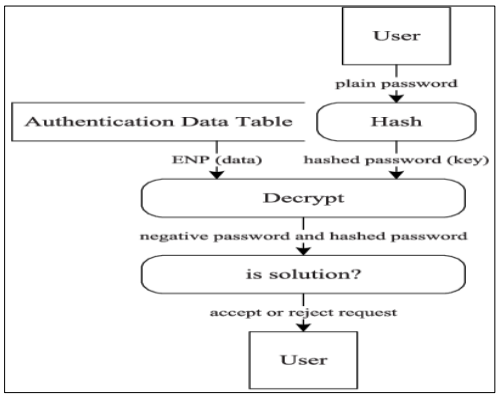


VI. ARCHITECTURE



The raw password is entered by the user and hashed using hashing techniques such as the Secure Hash Algorithm or the Message Digest Algorithm. The Negative Password is produced after the Hashing. The value of the negative password is then encrypted and saved in the authentication data database. We have a verification step in addition to the generating portion, where the password is confirmed or authenticated. This authentication is the most important component since the user provides a password to access the module, which must be validated.

10.5281/zenodo.5105435
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*



VII. DESCRIPTION OF MODULES

A. Data Owner

The data owner uploads their data to the Web server in this module. The data owner encrypts the data file for security reasons before storing it on the Web. The owner of the data file may be able to manipulate the encrypted data file. Meta data will be sent to Audit Web by the data owner. For audits and data integrity checks, raw or metadata information from the Web is available. The data owner will create an end user, and the data owner will be able to control the user's access permissions (read or write) as well as verify the password.

B. Verification and Auditing of Data

Using a digital signature and a web URL, the data owner may also audit the data integrity in the associated Web to see if the data is secure or not. If the material is no longer safe, he will delete it and re-upload it to the appropriate Web server.

C. Web Server

For an end user, the Web server is responsible for data storage and file authorization. Tags such as file name, secret key, digital sign, and owner name will be kept with the data file. The privileges will determine how the data file is sent. If the privilege is right, the data will be transferred to the appropriate user, and the file name, end username, and secret key will be checked. If all the conditions are met, the message will be sent to the appropriate user, or he will be identified as an attacker. The Web server can potentially behave as an attacker, modifying the data that will be audited by the audit Web and the data that will be audited by the audit Web. All Encrypted Negative Passwords, All Attackers, and All Password Attackers may be seen.

D. Data Consumer (End User)

The data consumer is the end user who makes a request for file contents and receives a response from the appropriate Web servers. If the file name, secret key, and access authorization are right, the end user will receive a file response from the Web; otherwise, he will be flagged as an attacker and his access to the relevant Web will be denied. If he wishes to access the file after banning it, he must first unblock it from the Internet and then verify the password.

E. Attacker

The attacker is the one who adds harmful material to the relevant Web file in order to integrate it. They might be from within or outside the Web. Internal attackers are those who come from within the Web and strike from within. External attackers are those who come from outside the Web and attack from there.

VIII. CONCLUSION

We devised the ENP password protection system and offered a password authentication system based on it in this study. The authentication data table elements in our framework are ENPs. Finally, we looked at the attack difficulty of hashed passwords, salted passwords, key stretching, and the ENP. As a result, this Encrypted Negative Password may be used to protect both passwords and websites. This approach also protects against rainbow table and lookup table attacks, as well as password security. The password is secure, and no one will ever be able to crack it. We are transforming the hash value into negative values and increasing it instead of just hashing it.

IX. REFERENCES

[1] Authentication by Encrypted Negative Password System , Wenjian Luo, Senior Member, IEEE, Yamin Hu, Hao Jiang and Junteng Wang.

[2] A Negative Authentication System, Dipankar Dasguptha, Rukhsana Azeem

[3] AUTHENTICATION SCHEME BY ENCRYPTED NEGATIVE PASSWORD, Faculty of California State Polytechnic University, Pomona, Laxmi Chidri

[4] Authentication by Encrypted Negative Password for an Intuitive Stock Management System K.Subramanian, V.Sreyas, M.Nikitha and Mrs.S.Aarthi(Assistant Professor) Department of Computer Science & Engineering MeenakshiSundararajan Engineering College, Chennai, Tamil Nadu, India

[5] Wenjian Luo, Senior Member, IEEE, Yamin Hu, Hao Jiang, and Junteng Wang, "Authentication by Encrypted Negative Password", IEEE Transactions on Information Forensics and Security, Volume: 14 , Issue: 1 , Jan. 2019.

[6] Authentication by Encrypted Negative Password, Poornima S1 ,Nivetha M2, Pradeep Kumar M3 Asst. Prof. Subathra S,Student Department of Computer Science and Engineering, Assistant Professor in Computer Science and Engineering, Velalar College of Engineering and Technology, Thindal, Erode-12.

10.5281/zenodo.5105435
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*