IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10764

AUTHENTICATION BY ENCRYPTED NEGATIVE PASSWORD

A.PRABHAKARAN[1],N.KARTHIKEYAN[1], K.AMSAVALLI[2]

Student, B.E Computer Science Engineering, Anand Institute of Higher Technology, Chennai, India[1]

Assistant Professor, CSE, Anand Institute of Higher Technology, Chennai, India[2]

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 the 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 serialized code is converted into a negative password. Finally, the negative password is encrypted into an Encrypted Negative Password (abbreviated as ENP) using a Hashing algorithm (e.g., SHA 152), 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 pre computation 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.

Keywords:

ENP	Encrypted Negative Password
NDB	Negative Database
ENPI	Encrypted Negative Password Implementation
NVD	National Vulnerability Database
SHA	Secure Shell Algorithm

I. INTRODUCTION

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 behaviours. The 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. In this case 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. After obtaining authentication data tables from weak systems, adversaries can carry out offline attacks. Passwords in the authentication data table are usually in the form of hashed passwords. However, because processor resources and storage resources are becoming more and more abundant, hashed passwords cannot resist pre computation attacks, such as rainbow table attack and lookup table attack. 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. After obtaining authentication data tables from weak systems, adversaries can carry out offline attacks. Passwords in the authentication data table are usually in the form of hashed passwords.

OBJECTIVE

The objective of this project are

DOI 10.17148/IJARCCE.2021.10764

- Implement a computationally light weight efficient password protection scheme called Encrypted Negative Password (abbreviated as ENP).
- To design and implement the service layers to expose this password protection layer to various other layers in the server side architecture.
- To implement the solution in such a way that it should be easier to integrate this with existing systems.
- To prove that the proposed scheme provides a strong security against various kinds of attacks.
- To provide an efficient user interface access to the clients to access the portal.
- To deploy the project over the cloud so that it can be accessed from various geographical location from any device.

SCOPE

By securing the password the online sites can provide security and protected from the cracking password. Passwords in the authentication data table presented in the form of hashed passwords. Processor resources and storage resources are becoming more and more abundant, so that the hashed passwords cannot resist pre computation attacks, such as rainbow table attack and lookup table attack.

II. ANALYSIS

SYSTEM ANALYSIS

System analysis is a problem solving technique that decomposes a system into its component pieces for the purpose of studying how well those components parts work and interact to accomplish their purpose. The proposed system uses the SHA-512 algorithm. These algorithms can be performed in Java Ecplise because it has a library like luna/neon that will be useful to this project.

PROBLEM DEFINITION

Systems make it easy for a user to discover a valid User name, displaying a message when a logon failure occurs. Such messages may say Invalid Username, telling the hacker that he or she should keep guessing Usernames. When a valid Username is found, a malicious hacker may then be shown another revealing message, such as, "Invalid password." Ideally, a system's logon failure message should be generic, such as, "Invalid Username or password," regardless of the reason for failure. Otherwise, the hacker could enumerate a valid User Name and start guessing passwords, looking for a weak one, which brings us to the next point. Weak passwords are a significant authentication system security weakness. If at all possible, enforce password rules for every system on the network, especially for systems at the network border. Password and account rules should at least require a mix of letters and numbers, and should specify a minimum password length, password history, account lockout and password expiration. If possible, set password rules that do not allow a password to be the same as the Username or the user's first or last name, as these are easy to guess. The goal is to force users to choose strong passwords.

EXISTING SYSTEM

In Existing systems based on password authentication, which is still the most widely used authentication technique, despite its some security flaws. The major flaws is in application we store password and that is not registered in the database in encrypted form. The plain password is just encrypted and stored in the database. This mechanism is highly insecure and you can also find that it is easy to attack and get the password. The other main mechanism which is used till date is the hashing mechanism where in the plain password is hashed using hashing algorithms such as the Secure Hash Algorithm or the Message Digest Algorithm. Comparing to the previous mechanism it provides more security and also it doesn’t provide the actual password but the hashed value of the password. But the plain password can be from the hashed value from the rainbow table attack and lookup table attack. Thus to reduce the vulnerability and risk we are using the Encrypted Negative Password System.

PROPOSED SYSTEM

In Proposed System, Confidential Password access will be secured by encrypting the password and storing into database using symmetric key encryption technique. Before comparing the values password must be decrypted using the key and then only we can compare using login values. The main framework to protect passwords in the authentication data table, the system designer should first select a cryptographic hash function and a symmetric-key algorithm, where the condition satisfied is that the size of the hash value of selected cryptographic hash function is equal to key size of the selected

Vol. 10, Issue 7, July 2021

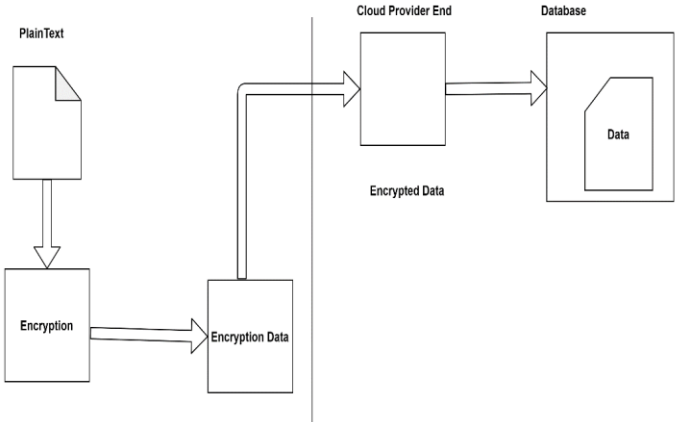
DOI 10.17148/IJARCCE.2021.10764

symmetric-key algorithm. In addition, cryptographic hash functions and symmetric-key algorithms could also be used in the ENP, which adequately indicates the flexibility of our framework.

III. SYSTEM DESIGN

Overall System Design

The received plain password from a client is hashed through a cryptographic hash function. Then, the Serialized code is converted into a negative password. Finally, the negative password is encrypted into an Encrypted Negative Password using a Hashing Algorithm and multi-iteration encryption could be employed to further improve security.



IV. MODULES

1. Data Owner Registration
2. Data User Registration
3. Data Owner Login
4. Data User Login

1. DATA OWNER REGISTRATION

Initially Data Owner must have to register their detail and after login. Then data Owner can upload files into cloud server with encrypted keywords and hashing algorithms. He she can view the files that are uploaded in cloud. Data Owner can approved oreject file request sent by data users.

1.1 Login/Registration:

In order to be a part of domain, user needs to register on the portal. In order to register on the portal, user need to provide some personal information which will be stored at back-end. At the time of login the credentials Username and password will be used to authenticate the user.

1.2 View Files (Search):

It is the core module for the Data user. In this module user can search specific files (desired). User can search specific file by providing a tag (can be part of content or name of the file) in the searching bar, if the file exists for the particular tag value, the file title will be shown on the dashboard. In the case of wrong tag insertion for search, the returned output will be null.

1.3 Download Files:

This module depends on the Search module. After searching files if some files list returned, User gets option for downloading the files. User can select specific file and download it by providing the respected private key (which is mailed him/her by the data owner)

2. DATA USER REGISTRATION

Initially Data Users must have to register their detail and then login into cloud. Data Users can search all the files upload by data owners. He she can send request to the files and then request will send to the data owners. If data owner approve the request then he/she will receive the decryption key in registered

2.1 Login Module:

Data Owner need to login on the portal in order to upload the data on the cloud.

2.2 Data Upload:

This module is dedicated for the process of uploading the content on the cloud server. Data owner have to select any data file (text) from the local machine in order to upload it on cloud server.

2.3 View Files(Search):

If the data owner wants to search any specific file, this module provides the option. The output of search operation will provide the list of the files; the module will also have the option for deletion of specific file.

2.4 File Share:

This module provides the option for file sharing. The module is somehow depends on the View file module. After searching files, the data owner can select specific file(s) and select specific user(s) with whom he want to share with.

3. DATA USER LOGIN

The user module allows users to register, log in, and log out. Users benefit from being able to sign on because this associates content they create with their account and allows various permissions to be set for their roles. the user module supports user roles, which can be set up with fine-grained permissions allowing each role to do only what the administrator permits. Each user is assigned one or more roles. By default there are three roles: anonymous (a user who has not logged in) and authenticated (a user who is registered), and administrator (a signed in user who will be assigned site administrator permissions).

4. DATA OWNER LOGIN

A Data Owner is a senior business stakeholder who is accountable for the quality of one or more data sets. Data owners are either individuals or teams who make decisions such as who has the right to access and edit data and how it's used.

V. RESULTS AND DISCUSSION

The system finally protects 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 adequately indicates the flexibility of our framework.

KEY BENEFITS OF THE PROPOSED SYSTEM

- Make it difficult to crack password from ENPs.
- User either send or receive the file will be done on safe manner.
- Confidential Password access will be secured by encrypting the password and storing into database using symmetric key encryption technique.
- Before comparing the values password must be decrypted using the key and then only we can compare using login values.
- To make effective use of Data Hashing & Negative Password Technique.Resistance to attack lookup table.

VI.CONCLUSION

Encrypted Negative Password can be used for securing the Passwords and also the webpages. This system also prevents the rainbow table attack and also the look up table and secures the passwords. The password used is safe and no one can ever try to break the password. Instead of just hashing we are converting the hash value into negative values and encrypting. Thus during verification also thus we check whether it's the solution or not but do not get to know the actual password.

REFERENCES

1. E. H. Spafford, "Opus: Preventing weak password choices," Computers & Security, vol. 11, no. 3, pp. 273–278, 1992.
2. A. Adams and M. A. Sasse, "Users are not the enemy," Communications of the ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.
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. 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.
5. 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.
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.