International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

J1970 AUTHENTICATION BY ENCRYPTED NEGATIVE PASSWORD

[1]Gundeti Uday, [2]Sahu Sahu Shivaram, [3]Veena Kumari Pullemla, [4]Mohammed Fauzaan

[1,2,3] Assistant Professors,Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

[4]student,Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

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 except the plain password.

I.INTRODUCTION

O WING 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 an attack, 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 precomputation attacks, such as rainbow table attack and lookup table attack. Note that there is a trend of generalization of adversaries, because anyone could obtain access to information on vulnerabilities from vulnerability databases, such as the Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVD), and the Common Vulnerabilities and Exposures (CVE) , and then make use of these information to crack systems. Moreover, they could download and use attack tools without the need for very professional security knowledge. Some powerful attack tools, such as hashcat [20], RainbowCrack and John the Ripper , provide a variety of functions, such as multiple hash algorithms, multiple attack models, multiple operating systems, and multiple platforms, which raises a higher demand for secure password storage. In these situations, attacks are usually carried out as follows. First, adversaries precompute a lookup table, where the keys are the hash values of elements in a password list containing frequently-used passwords, and the records are the corresponding plain passwords in the password list. Next, they obtain an authentication data table from low security systems. Then, they search for the plain passwords in the lookup table by matching hashed passwords in the authentication data table and the keys in the lookup table. Finally, the adversaries log into higher security systems through cracked usernames and passwords, so that they could steal more sensitive information of users and obtain some other benefits. A considerable number of attacks are carried out in this way, so that adversaries could obtain passwords at a low cost, which is advantageous to their goals. One of the main reasons for the success of the above lookup table attack is that the corresponding hashed password is determined for a given plain password. Therefore, the lookup table could be quickly constructed, and the size of the lookup table could be sufficiently large, which results in a high success rate of cracking hashed passwords. Typical password protection schemes include hashed pass-word, salted password and key stretching. Among these schemes, hashed password would be gradually eliminated for its vulnerability for precomputation attacks. Although salted password could resist precomputation

attacks, it introduces an extra element (i.e., salt) and could not resist dictionary attack. In addition, salt tends to be implemented by mistake (such as salt reuse and short salt). Key stretching schemes, such as bcrypt, scrypt and Argon2 (the winner of Password Hashing Competition), are used to defend against dictionary attack. Although key stretching schemes provide stronger password protection than salted password under dictionary attack, they impose an extra burden on programmers for configuring more parameters. In addition, they also use salt to resist precomputation attacks. Besides these schemes, some other password protection schemes were proposed. In , a scheme based on MD5 was proposed. It is a variant of salted password, where the salt is two random strings. Although it could resist lookup table attack and make dictionary attack difficult, it introduces many parameters, which makes it complicated and inconvenient to use. In , dynamic salt generation and placement are used to improve password security. Essentially, this scheme is also a variant of salted password, where the salt is a random string that is dependent on the original password. Consequently, it could resist lookup table attack, however it could not defend against dictionary attack and also introduces an extra element (i.e., salt). In, improved dynamic Key-Hashed Message Authentication Code function (abbreviated as d-HMAC) was proposed for password storage. It is also a variant of salted password, where the salt is the user's public key, and it introduces a secret key, which makes it inconvenient to use. In summary, although some new password protection schemes were proposed, they are similar to typical password protection schemes essentially. Therefore, in Section VI, without loss of generality, we only compare the typical password schemes with our scheme. In this paper, a password protection scheme called Encrypted Negative Password (abbreviated as ENP) is proposed, which is based on the Negative Database (abbreviated as NDB), cryptographic hash function and symmetric encryption, and a password authentication framework based on the ENP is presented. The NDB is a new security technique that is inspired by biological immune systems and has a wide range of applications. Symmetric encryption is usually deemed inappropriate for password protection. Because the secret key is usually shared by all encrypted passwords and stored together with the authentication data table, once the authentication data table is stolen, the shared key may be stolen at the same time . Thus, these passwords are immediately compromised. However, in the ENP, the secret key is the hash value of the password of each user, so it is almost always different and does not need to be specially generated and stored. Consequently, the ENP enables symmetric encryption to be used for password protection. As an implementation of key stretching , multi-iteration encryption is introduced to further improve the strength of ENPs.

II.LITERATURE SURVEY

In the cloud storage to protect outsource data by adding fault tolerance reparation becomes critical. Due to lower repair bandwidth while providing fault tolerance of regenerating codes have gained popularity. By using existing methods for regenerating-codeddata

it only provide private auditing and it requires data owners to always stay online and for repairing also there is data owner is require which is sometimes impractical. By manipulating the classic Merkle Hash Treeconstructionfor block tag authentication, it improves the existing proof ofstorage models and as well as achieve efficient data dynamics,multiple auditing tasks explore the technique of bilinearaggregate signature to extend the result into a multi-user setting with the help of TPA which can perform multipleauditing tasks simultaneously. The proposed schemes are highly efficient and provably secure as per Extensive security and performance analysis

2.1Cipher text-Policy Attribute-Based Encryption

AUTHORS: Taeho Jung1, Xiang-Yang Li12, Zhiguo Wan34, Meng Wan5

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous AttributeBased Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

2.2Multi-authority attribute based encryption with honest-but-curious central authority

AUTHORS: Vladimir Boˇzovi´c1 , Daniel Socek2? , Rainer Steinwandt1 , and Vikt´oria I. Vill´anyi

An attribute based encryption scheme capable of handling multiple authorities was recently proposed by Chase. The scheme is built upon a single-authority attribute based encryption scheme presented earlier by Sahai and Waters. Chase's construction uses a trusted central authority that is inherently capable of decrypting arbitrary ciphertexts created within the system. We present a multi-authority attribute based encryption scheme in which only the set of recipients defined by the encrypting party can decrypt a corresponding ciphertext. The central authority is viewed as "honest-but-curious": on the one hand it honestly follows the protocol, and on the other hand it is curious to decrypt arbitrary ciphertexts thus violating the intent of the encrypting party. The proposed scheme, which like its predecessors relies on the Bilinear DiffieHellman assumption, has a complexity comparable to that of Chase's scheme. We prove that our scheme is secure in the selective ID model and can tolerate an honest-but-curious central

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

authority. Building on the proposal for multi-authority based attribute based encryption from [4], we constructed a scheme where the central authority is no longer capable of decrypting arbitrary ciphertexts created within the system. In addition to showing security in the selective ID model, we showed that the proposed system can tolerate an honest-but-curious central authority. Since both Chase's scheme and the proposed scheme rely on the same hardness assumption, and have a comparable complexity, the new scheme seems a viable alternative to Chase's construction. However, since only the proposed method is capable of handling a curious yet honest central authority, the proposed scheme is recommended in applications where security against such a central authority is required.

III.SYSTEM ARCHITECTURE:

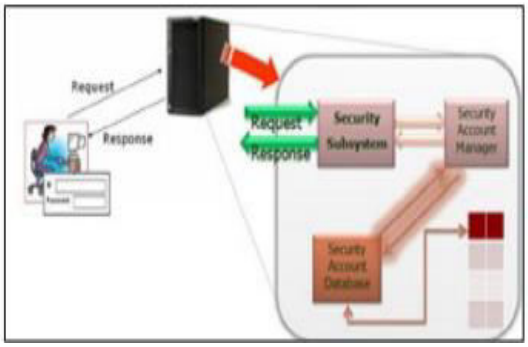

Figure 3.1 System Architecture

IV.OUTPUT

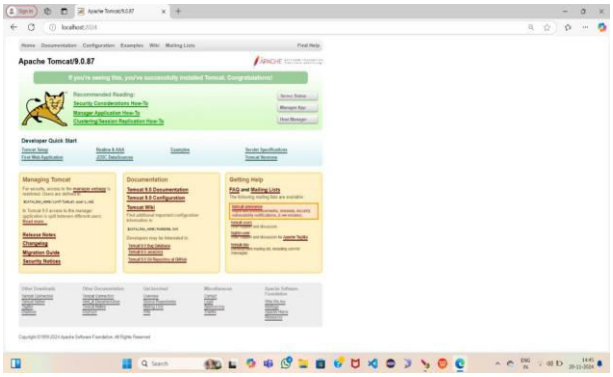

Figure 4.1

Figure 4.2

Figure 4.3

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

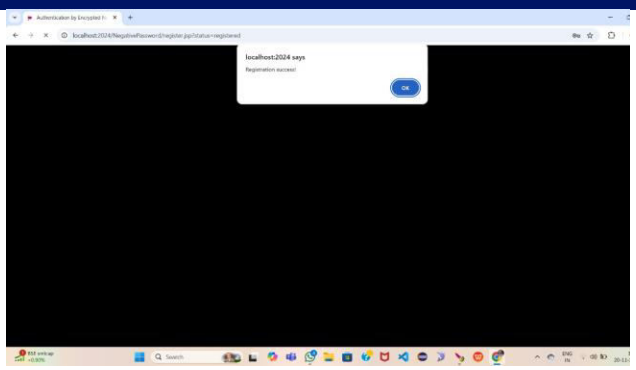

Figure 4.4

Figure 4.5

Figure 4.6

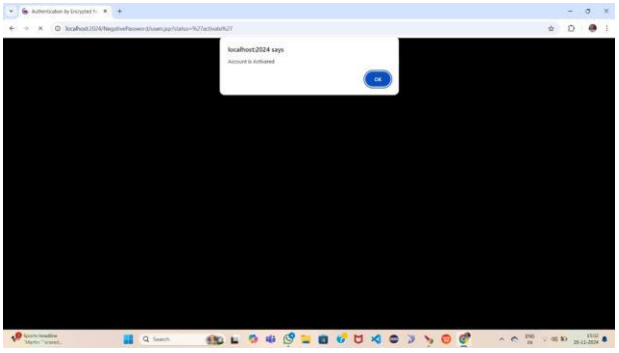

Figure 4.7

Figure 4.8

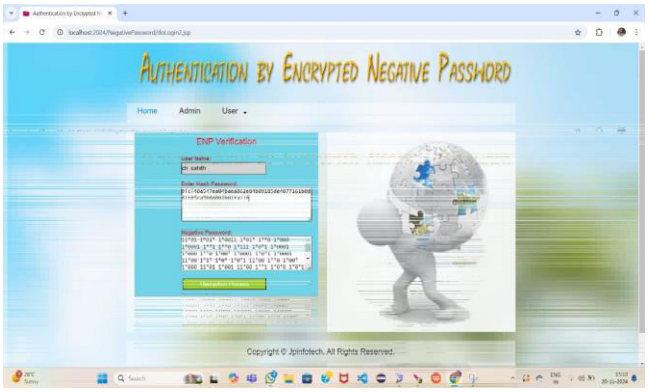

Figure 4.9

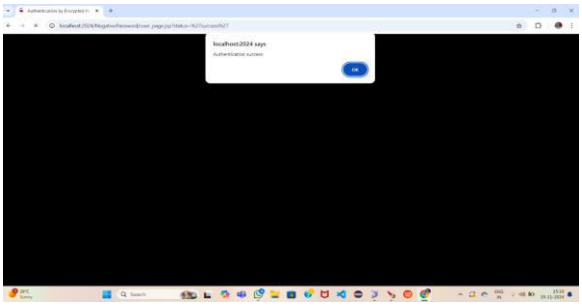

Figure 4.10

V.CONCLUSION

In this paper, we proposed a password encryption system named ENP in this thesis, and proposed an ENP-based password authentication mechanism. The entries in the authentication data table are ENPs inside our system. In the end, the attack difficulty of the hashed password, salted password, key

stretching, and the ENP was evaluated and contrasted.

The findings indicate that under dictionary attack, the ENP should avoid the lookup table attack and provide better password protection. It should be remembered that, while resisting the lookup table attack, the ENP does not require additional elements (e.g., salt).

In the future, to further boost password protection, other NDB generation algorithms will be researched and applied to the ENP. In addition, other methods would be incorporated into our password security system, such as multi-factor authentication and challenge-response authentication.

VI.FUTURE ENHANCEMENT

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, will be introduced into our password authentication framework

VII.REFERENCE

[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 Dasgupta, 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, Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India. 1

[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.