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

Abstract

This paper is about securing the passwords and making the system more secured from intruders. Most of the stock management systems uses the method where in the passwords are just encrypted and are not secured properly. This encrypted negative password system uses the technique where in the passwords are first hashed and then converted to negative password and finally encrypted and stored in the database.However the 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. This Encrypted Negative Password system still can resist the precomputation attacks. Thus by securing the pages with negative password system, all these vulnerabilities can be reduced.

Keywords - *Authentication, negative table, lookup table attack*

I. INTRODUCTION

The stock management systems generally consist of all the stocks which are managed by the stores and quality department of the company. These stocks may be raw materials or finished products and these are valuable information which is needed to be secured properly. Most of these data's need to be secured as they should not be available to the other department. These information should be unknown and must not be disclosed to others and thus instead of using just plain passwords we can use the encrypted negative password system.

II. EXISTING SYSTEM

The existing system actually uses the simplest mechanism of all the other techniques. 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 for the Stock Management system.

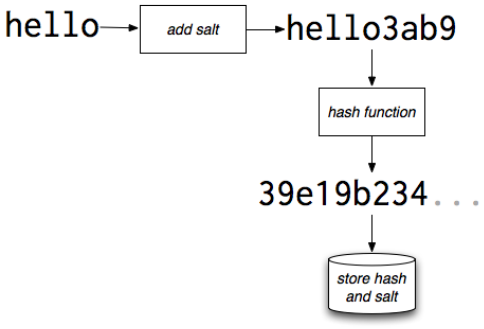


Fig.1 Salted Password

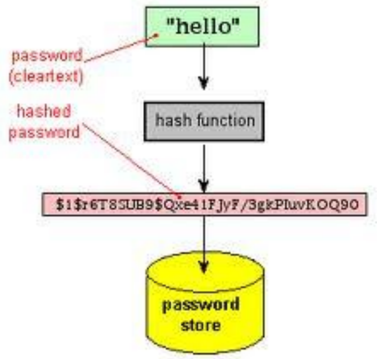


Fig.2 Normal Hash Password

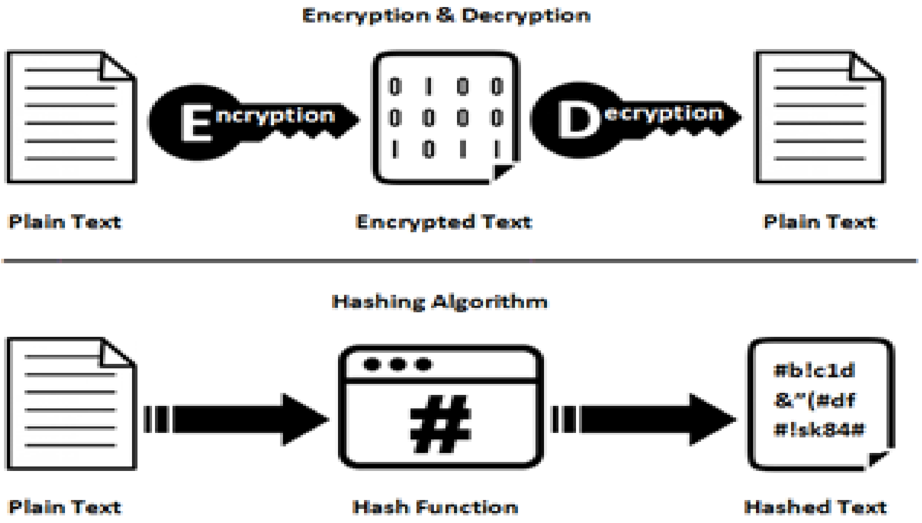


Fig.3Normal Hashing Algorithm

III. PROPOSED SYSTEM

A. Motivation

The Stock Management systems use the method where in the plain passwords are just encrypted and stored. They must be secured as there might be access to the password table for all the departments so it is easy for them to access and misuse the work. So hence by protecting them by this encrypted negative password system we can provide more security. Thus by hashing also we can protect by it also has some loop holes thus we are using the encrypted negative password system to protect the system in each way.

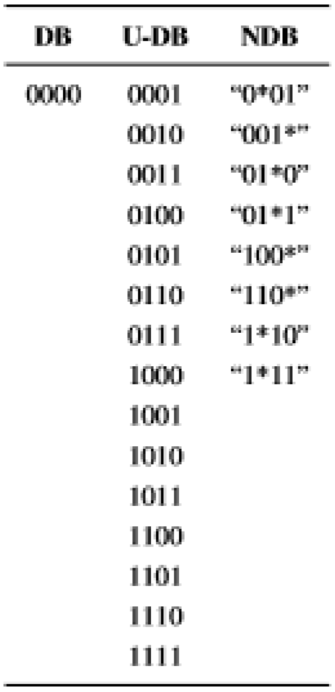
Generally the password protection schemes where:

1) Hashed Password: The Plain Password is obtained from the user and can be stored as the same with just encryption but it's not safe. So we use the cryptographic hash function to the hash the password.

2) Salted Password: To reduce precomputation attacks we use the salted password technique were in the plain password is concatenated with a random value(salt) and is hashed.

B. Actual working

This system gets the plain password from the user and stores in the database as the negative of the plain password. The working is that the plain password is obtained from the user and first hashed using the Secure Hash Algorithm or the Message Digest Algorithm. Then after hashing the hashed value is converted into negative value and then it's encrypted and stored. Thus during verification also the password is not revealed and is secured.



DB	U-DB	NDB
0000	0001	“0*01”
	0010	“001*”
	0011	“01*0”
	0100	“01*1”
	0101	“100*”
	0110	“110*”
	0111	“1*10”
	1000	“1*11”
	1001	
	1010	
	1011	
	1100	
	1101	
	1110	
	1111	

Fig.4 Negative Database

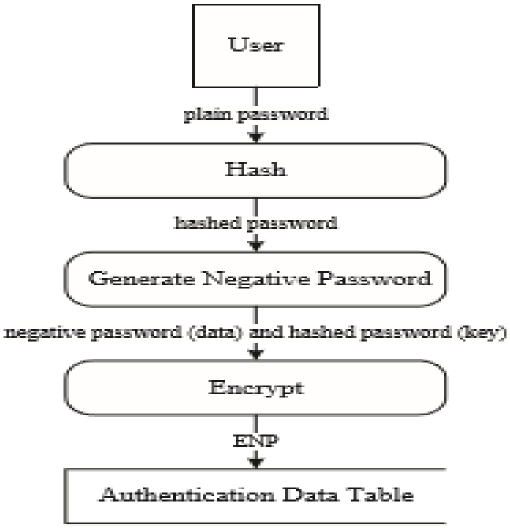

User
plain password
Hash
hashed password
Generate Negative Password
negative password (data) and hashed password (key)
Encrypt
ENP
Authentication Data Table

Fig.5 Generation of Encrypted Negative Password

C. Architecture

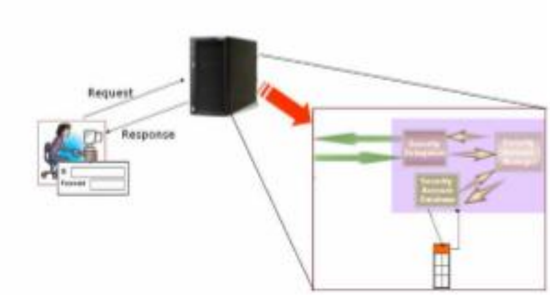


Fig.3 Architecture of Authentication of Encrypted Negative Password

The user enters the plain password and its hashed using the hashing algorithms like the Secure Hash Algorithm or the Message Digest Algorithm. After Hashing the Negative Password is generated. After the negative password is created the value is then encrypted and stored in the authentication data table.

Along with the generation part we also have the verification part were in the password is verified or authenticated. This authentication is the main part as the user enters the password for entering into the module and thus has to be verified.

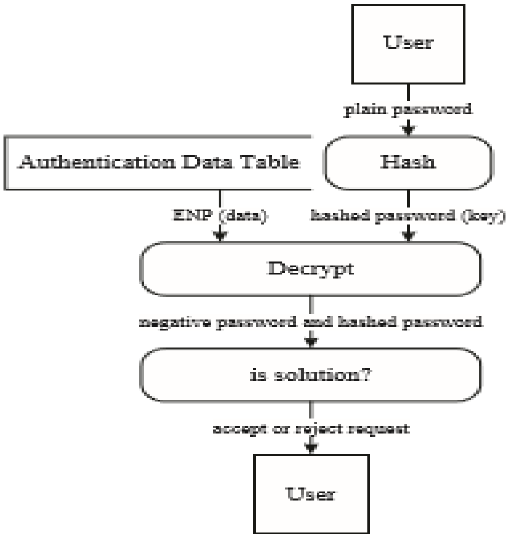


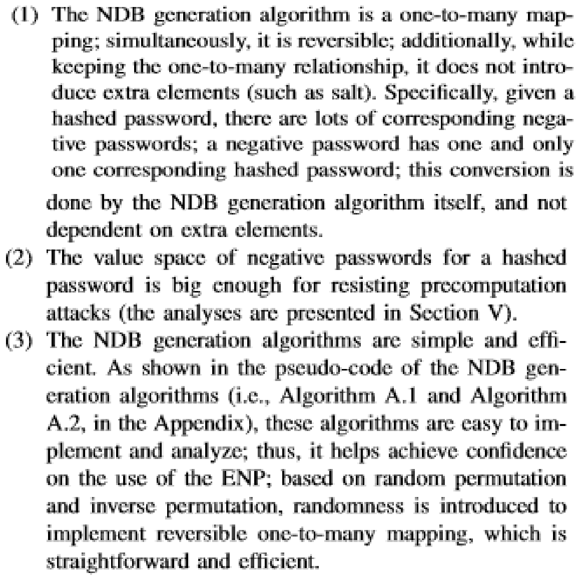
Fig.6 Authentication of Encrypted Negative Password

D. Algorithms

The creation of the negative password is that the plain password is converted into the ASCII value and then converted into binary values of 0's and 1's. Then we split the values as two bit pairs and there are 4 forms:

00->0
01->1
10->*
11->*

For eg: "00101101" its denoted as "0**1".



(1) The NDB generation algorithm is a one-to-many mapping; simultaneously, it is reversible; additionally, while keeping the one-to-many relationship, it does not introduce extra elements (such as salt). Specifically, given a hashed password, there are lots of corresponding negative passwords; a negative password has one and only one corresponding hashed password; this conversion is done by the NDB generation algorithm itself, and not dependent on extra elements.

(2) The value space of negative passwords for a hashed password is big enough for resisting precomputation attacks (the analyses are presented in Section V).

(3) The NDB generation algorithms are simple and efficient. As shown in the pseudo-code of the NDB generation algorithms (i.e., Algorithm A.1 and Algorithm A.2, in the Appendix), these algorithms are easy to implement and analyze; thus, it helps achieve confidence on the use of the ENP; based on random permutation and inverse permutation, randomness is introduced to implement reversible one-to-many mapping, which is straightforward and efficient.

IV. CONCLUSION

Thus this 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.

The Stock Management system has the record of all the goods which are required and produced and thus each department has its own work and must not be interlinked and have access so thus we are securing it using the encrypted negative password system. The main departments for this stock management wherein we have the Material Requisition Note, Goods Requisition Note, Finished Product and the Suppliers where in each module had its own set of procedures to work on to process the whole part.

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] J.Bonneu, C.Herley, P.C.Van Oorschot and F.Stanjano, "Passwords and the evolution of imperfect authentication", Communications of the ACM, vol. 58, pp.78-87, Jun-2015.

[4] M.A.S.Gokhale and V.S.Waghmare, "The shoulder surfing resistant graphical password authentication techniques", Procedia Computer Science, vol. 79, pp.490-498, 2016.

[5] Development of inventory management system, Yang Fan Zhongnan, IEEE International Conference on Information Management and Engineering, 16-18 April 2018