Authentication System Using Cryptographic Secure Password Storage

Prof. S.A.Sagar, Osheen Bhat, Megha Raina, Shital Patil

Abstract: Secure password storage is a vital aspect in systems based on password authentication. There are some security flaws in authentication technique. Due to this password can be still easily cracked. Therefore, we are going to develop a system that will provide a way of storing password by using cryptographic functions. System will adopt a framework to prevent password in data table. 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. The system consists of two phases: the registration phase and authentication phase. In registration phase, user enters username and password. The received password will be converted to hash value by using Elliptic curve cryptography (ECC) algorithm. This hash value will be then converted into negative password using negative password generation algorithm. The negative password will be then converted into Encrypted Negative Password by using selected symmetric-key algorithm i.e. Attribute Based Encryption (ABE). While encryption key will be hash value of plain password. This ENP will be then store to authentication data table. 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.

Keywords: Authentication, dictionary attack, lookup table attack, negative database, secure password storage.

Introduction:
Nowadays computer as well as information security is the most significant challenge. Authorized users should access the system or information. Authorization can’t occur without authentication. For this authentication various techniques are available. Among them the most popular and easy is the password technique. Password ensures that computer or information can be accessed by those who have been granted right to view or access them. 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. 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. In this paper, a password protection scheme called Encrypted Negative Password (ENP) is proposed, which is based on the Negative Database (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 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 symmetric encryption is introduced to further improve the strength of ENPs. Compared with the salted password scheme and key Stretching, the ENP guarantees the diversity of passwords by itself without introducing extra elements (e.g., salt).

To summarize, the main contributions of this paper are as follows:
(1) We propose a password protection scheme called ENP, and we propose two implementations of the ENP: ENPI and ENPII, including their generation algorithms and verification algorithms. Furthermore, a password authentication framework based on the ENP is presented.
(2) We analyze and compare the attack complexity of hashed password, salted password, key stretching and the ENP. The results show that the ENP could resist lookup table attack without the need for extra elements and provide stronger password protection under dictionary attack.

Related work

A. Typical Password Protection Schemes

1) Hashed Password:
The simplest scheme to store passwords is to directly store plain passwords. However, this scheme presents a problem that once adversaries obtain the authentication data table, all passwords are immediately compromised. To safely store passwords, a common scheme is to hash passwords using a cryptographic hash function because it is infeasible to directly recover plain passwords from
hashed passwords. The cryptographic hash function quickly maps data of arbitrary size to a fixed-size sequence of bits. In the authentication system using the hashed password scheme, only hashed passwords are stored. However, hashed passwords cannot resist lookup table attack. Furthermore, rainbow table attack is more practical for its space-time tradeoff.

Processor resources and storage resources are becoming richer, which makes the precomputed tables used in the above two attacks sufficiently large, so that adversaries could obtain a higher success rate of cracking hashed passwords.

2) Salted Password:

To resist precomputation attacks, the most common scheme is salted password. In this scheme, the concatenation of a plain password and a random data (called salt) is hashed through a cryptographic hash function. The salt is usually generated at random, which ensures that the hash values of the same plain passwords are almost always different. The greater the size of the salt is, the higher the password security is. However, under dictionary attack, salted passwords are still weak. Note that compared with salted password, the ENP proposed in this paper guarantees the diversity of passwords without the need for extra elements (e.g., salt).

3) Key Stretching:

To resist dictionary attack, key stretching, which converts weak passwords to enhanced passwords, was proposed. Key stretching could increase the time cost required to every password attempt, so that the power of defending against dictionary attack is increased. In the ENP proposed in this paper, like key stretching, multi-iteration encryption is used to further improve password security under dictionary attack, and compared with key stretching, the ENP does not introduce extra elements (e.g., Salt).

B. Negative Database:

Some concepts of NDB are given below. Every entry in an ‘*’. The symbol ‘0’ only match the bit 0, and the symbol ‘1’ only match the bit 1; The symbol ‘*’ can match either the bit 0 or 1. Every entry in an NDB consists of two kinds of positions: specified positions and unspecified positions. Positions where the symbols are ‘0’ or ‘1’ are called specified positions, while positions where the symbols are ‘*’ are called unspecified positions. Accordingly, both ‘0’ and ‘1’ are specified symbols, and the ‘*’ is the unspecified symbol. A sequence of bits is covered by one entry in an NDB; that is to say, the bits of the sequence are matched by the symbols of the entry at the specified positions. If a sequence of bits is covered by one entry in an NDB, we say that the sequence is covered by the NDB. If an NDB covers every entry in the (U-DB), we say that the NDB is complete; otherwise, it is incomplete. The NDB converted from a DB with only one entry is called the single NDB; otherwise, it is called the multiple NDB.

Motivation:

We are developing this system for providing more security to sensitive data. We analyze and compare the attack complexity of our scheme with that of typical password storage schemes (i.e., Hashed password, Salted password) under lookup table attack and dictionary attack. To provide a way for prevention of data tables to keep user’s sensitive information safe from various attacks. We are going to use combination of various techniques to convert plain text information into encrypted information.

We are developing this system for providing more security to sensitive data. We analyze and compare the attack complexity of our scheme with that of typical password storage schemes (i.e., Hashed password, Salted password) under lookup table attack and dictionary attack. To provide a way for prevention of data tables to keep user’s sensitive information safe from various attacks. We are going to use combination of various techniques to convert plain text information into encrypted information.

System Architecture:

Figure shows the flow of our System. The system consists of two phases: The registration phase and authentication phase. In registration phase, user enters username and password in plain text. The received password will be converted to hash value by using ECC algorithm. This hash value will be then converted into negative password using negative password generation algorithm. The negative password will be then converted into Encrypted Negative Password (ENP) by using selected symmetric-key algorithm i.e.
Attribute Based Encryption (ABE). While encryption key will be hash value of plain password. This ENP will be stored to authentication data table. If the user password is match with Authentication System then Registration will be Successful.

Conclusion:

In this paper, we propose a password authentication framework that is designed for secure password storage and could easily integrated into existing authentication systems. We are going to propose password protection scheme called Encrypt Negative Password (i.e., ENP) and records in authentication data table are Encrypted Negative Passwords. 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 (e.g., salt) while resisting lookup table attack. In the future, other NDB generation algorithms will be studied and introduced to the ENP to further improve password security.

References: