Secure Password System against Imposter

Sung Bae Park¹ · Seung Bae Park¹· Moon Seol Kang³³

ABSTRACT

We present a new password system, called dual password system, with the user verification procedure. Dual password system is the first password system in the world preventing the exposure of secret information to imposter at the terminal. User of dual password system matches two alphabets at same location of first password and second password iteratively for inputting password. Therefore, the deriving method of first password and second password from the password is important in dual password system. Related to the deriving method of first password and second password from password, a new problem, called dual password derivation problem, is defined, and the evaluation factors for the solutions of the dual password derivation problem are presented.

1. Introduction

Password system is most well known and commonly used entity authentication system because it is easy to implement, low price and convenient to use. In spite of its advantages, the password system is used in the restricted circumstances because: 1) the secret information can be exposed to imposter at the terminal; 2) the password system is weak for the attacks including replay attack and off line dictionary attack [2, 6].

Biometrics is secure against imposter, unique and immutable. Security against imposter makes entity authentication systems based on biometric techniques [5, 8, 9] to be spread in a broad range of civilian applications, but the systems are expensive, and user reveals rejection symptom.

Challenge response protocols [7] and zero knowledge based protocols [1, 3, 4] are suggested to provide the secure mechanisms against the attacks, but they are inconvenient to use on the terminal. For a shortcoming of the protocols, most commercial entity authentication systems do not adopt the protocols, as an example, the internet banking system adopts the password system at the terminal and the public key infrastructure for the launched information on the channel. From the advantages of the password system and the shortcomings of the entity authentication systems based on biometric techniques, it is important to develop the technology that combines only the positive aspects of the password system and the biometric technique based entity authentication systems, but no technology has been presented in the world as yet.
In this paper, we present a new password system, called dual password system (DPS), with the user verification procedure. DPS is the first password system in the world that succeeds on the advantages of the traditional password system and prevents the exposure of the secret information to impostor at the terminal. That is, DPS is easy to implement, low price, convenient to use, and secure against impostor at the terminal.

User of dual password system inputs a password by matching of two alphabets at same location of first password and second password. Therefore, the deriving method of first password and second password from the password is important in dual password system. Related to the deriving method of first password and second password from password, a new problem, called dual password derivation problem, is defined, and the evaluation factors for the solutions of the dual password derivation problem are presented.

This paper is organized as follows. In Section 2, we describe dual password system with the user verification procedure. Section 3 includes the definition of dual password derivation problem with the estimation factors for the solutions of dual password derivation problem. In Section 4, we conclude this paper.

2. Dual Password System

Secret information of DPS is the concatenation of two secret information called first password and second password where the lengths of first password and second password are same, and the concatenation of first password and second password is called dual password.

Example 1 Let 213833 be the secret information of authorized user, then first password is 213, second password is 833, and dual password is 213833.

The input of dual password in DPS is done by the match of two alphabets at same position in first password and second password, and DPS supports the graphical user interface (GUI) such that user can match two alphabets. Authentication procedure of basic type of DPS is depicted in the follow.

Let S be a set of alphabets such that each element of S can be selected by user for consisting dual password, and \(x_1y_1 \cdots x_ny_n\) be dual password of authorized user for \(x_i, y_i \in S\) \((1 \leq i \leq n)\). DPS is the password system that verifies user by the following procedure:

1. DPS displays two boards called BB (base board) and MB (matching board) on GUI where BB contains all alphabets in S by the increasing order, and MB contains all alphabets in S by randomly selected order without replacement;
2. user matches an alphabet in BB and an alphabet in MB iteratively. Let the user match an alphabet in BB and an alphabet in MB \(l\) times, and \((v'_i, w'_i)\) be the \(l\)th matched pair of an alphabet \(v'_i\) on BB and an alphabet \(w'_i\) on MB by the user for \(1 \leq i \leq l\), then DPS matches the \(|S|\) pairs of two alphabets on BB and MB including \((v'_i, w'_i)\) in concurrent with the match of \((v'_i, w'_i)\);
3. let \((v'_i, w'_i)\{1 \leq i \leq l, 1 \leq t \leq |S|\} for each\} be a set of the \(|S|\) \(l\) matched pairs of two alphabets in 2 where \(v'_i\) is the \(i\)th alphabet on BB, \(w'_i\) is the \(i\)th alphabet on MB, then \{w'_i\{1 \leq i \leq l, 1 \leq t \leq |S|\} for each\} is send to the system;
4. DPS receives \{w'_i\{1 \leq i \leq l, 1 \leq t \leq |S|\} for each\} and fetches \(x_1y_1 \cdots x_ny_n\) from the memory;
5. DPS accepts the user if \(i = n\) and \(w'_u = y_u\) where \(u\) is a position of \(x_i\) on BB \(1 \leq i \leq l\).

DPS is a password system, but DPS is different from the traditional password system in the aspects of: (1) the password of DPS consists of first password and second password; (2) the input of dual password is done by the match of two alphabets at same location of first password and second password; (2) the input of dual password can be done without textual typing.

Example 2 Let \(S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}\), 6, 1, 3, 8, 9, 2, 7, 0, 4, 5 be randomly selected alphabets without replacement, and \(x_1y_1 = 63\) be dual password.

1. DPS displays BB and MB on GUI where BB contains all alphabets in S in the order of 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, and MB contains all alphabets in S in the order of 6, 1, 3, 8, 9, 2, 7, 0, 4, 5 (See (Figure 1));

(Figure 1) BB and MB before match 3 and 6

2. let user matches an alphabet in BB and an alphabet in MB once, and 6 in BB and 3 in MB be matched by the
user, then DPS matches 10 pairs of two alphabets on BB and MB including (6, 3) in concurrent with the match of (6, 3) (See Figure 2). In this example, we assume that two alphabets are matched if two alphabets are on the same column. At (Figure 2), 0 and 7 are matched because 0 is in the first column of BB, and 7 is also in the first column of MB:

![Figure 2] BB and MB after match of 3 and 6

1. \( (0, 7), (1, 0), (2, 4), (3, 5), (4, 6), (5, 1), (6, 3), (7, 8), (8, 9), (9, 2) \) are matched, and \( (7, 0, 4, 5, 6, 1, 3, 8, 9, 2) \) is send to the system;
2. DPS receives \( (7, 0, 4, 5, 6, 1, 3, 8, 9, 2) \), and fetches 63 from the memory;
3. the length of two password is 1, the number of match is 1, \( \omega_1^1 = \omega_1^1 = 3 \) because \( x_i = 6, \) and 6 is the 7th alphabet on BB. Therefore, DPS accepts the user.

The match of an alphabet in BB and an alphabet in MB can be done by using the input device. An Example 2, the user strokes the right arrow key to rotate MB, and DPS rotates MB once whenever the user stokes the right arrow key, and the match is completed when the user strokes another key such as the enter key.

Besides basic type of DPS, there can be various types of DPS. For this reason, we define DPS in the general form.

Definition 1 DPS is a password system that satisfies the following conditions:
1. DPS has to provide GUI such that user can match an alphabet in first password and an alphabet in second password;
2. a probability that unauthorized user be accepted by DPS on the assumption that he knows \( |S| \times m \) matched alphabets by authorized user on MB. We call this probability SSH (success using access history). Two cases of SSH must be considered: (a) \( (i \text{ mod } |P_2|) \)th alphabet of second password is contained in \( i \)th \( |S| \) alphabets for \( 1 \leq i \leq m \). We call this case SSH of Type 1; (b) \( i \)th \( |S| \) alphabets contain any alphabet in two password. We call this case SSH of Type 2;
3. a probability that unauthorized user be accepted by DPS on the assumption that he knows \( |S| \times P_2 \times n \) alphabets on MB gathered by himself when he failed the fabrication. We call this probability SFH (success using fail history);
4. a probability that is SFH on the assumption SSH;
5. number of alphabets to be remembered by authorized user;
6. number of alphabets to be send to the system.

In the above evaluation factors, 1, 2 and 3 are related to the security of DPS, and 4 and 5 are related to the performance of DPS. Evaluation factor 1 is referred to on-line dictionary attack in other literatures.

Example 3 Let \( S = \{ i | 0 \leq i \leq 9 \} \) be a set of alphabets, \( P = 6137, f(6137) = 61, g(6137) = 37 \), and let assume that (a) 6137 is selected in random; (b) the length of dual password
of any authorized user is 4;
(c) imposter has known 7, 0, 4, 5, 6, 1, 3, 8, 9, 2 for SSH of Type 1, and current MB contains 4, 0, 5, 6, 3, 1, 2, 8, 9, 7; (d) DPS refreshes the alphabets contained in MB whenever a match is completed. In this example, we consider OTS, SSH of Type 1, a number of alphabets to be remembered by authorized user and a number of alphabets send to DPS.

(1) OTS is 1/100;
(2) SSH of Type 1 is \( \frac{1}{6} \times \frac{1}{10} = \frac{1}{60} \);
(3) a number of alphabets to be remembered is 4;
(4) a number of alphabets send to DPS is 20.

4. Conclusions

Traditional password system is most wide spread entity authentication system because of its many advantages. In spite of the advantages of traditional password advantages, it has serious shortcomings that is the exposure of password at the terminal. Biometric based entity authentication systems are presented to overcome the shortcoming of traditional password system, but they have their own shortcomings including rejection symptom of user. For these reasons, it is important to develop the technology that combines only the positive aspects of the password system and the biometric technique based entity authentication system.

We have presented a new password system called DPS with the procedure verifying a user. DPS succeeds on the advantages of the traditional password system and avoids the exposure of the secret information to imposter at the terminal.

We have defined dual password derivation problem that is related to the security and performance of DPS, and we have presented the evaluation factors for the solutions of dual password derivation problem.

References