타인의 관찰에 의한 패스워드 노출로부터 안전한 패스워드 시스템

박 승 배[†] · 박 성 배[††] · 강 문 설[†††]

요 약

인가된 사용자가 패스워드를 입력하는 과정이 타인에게 관찰되어도 패스워드가 노출되지 않는 세계 최초의 패스워드 시스템인 듀얼 패스워드 시스템을 제안하고, 듀얼 패스워드 시스템이 사용자를 인증하는 과정을 제시한다. 듀얼 패스워드 시스템의 패스워드 입력은 first password와 second password의 동일한 위치에 있는 두 기호를 매칭하는 과정을 반복하여 이루어진다. 따라서, 패스워드로부터 first password와 second password를 유도하는 방법은 듀얼 패스워드 시스템에서 중요한 의미를 갖는다. 패스워드로부터 first password와 second password를 유도하는 방법과 관련하여 dual password derivation 문제를 정의하며, dual password derivation 문제의 해에 대한 평가 척도들을 제시한다.

Secure Password System against Imposter

Sung Bae Park[†] · Seung Bae Park[††] · Moon Seol Kang[†††]

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.

키워드 : 패스워드 시스템(Password System), 듀얼 패스워드(Dual Password), Dual 패스워드 시스템(Dual Password System), First Password, Second Password, Dual Password Derivation 문제(Dual Password Derivation Problem)

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.

† 종신회원 : 초당대학교 컴퓨터과학과 교수
†† 정 회 원 : 순천제일대학 인터넷정보학부 교수
††† 종신회원 : 광주대학교 컴퓨터전자통신공학부 교수
논문접수 : 2002년 11월 6일, 심사완료 : 2003년 2월 10일

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 imposter at the terminal. That is, DPS is easy to implement, low price, convenient to use, and secure against imposter 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 213853 be the secret information of authorized user, then first password is 213, second password is 853, and dual password is 213853.

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 $x_1x_2\cdots x_n y_1 y_2\cdots y_n$ be dual password of authorized user for $x_i, y_i \in S$ $(1 \le i \le n)$. 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^j, w^j) be the jth matched pair of an alphabet v^j on BB and an alphabet v^j on MB by the user for $1 \le j \le l$, then DPS matches the $|S|$ pairs of two alphabets on BB and MB including (v^j, w^j) in concurrent with the match of (v^j, w^j) ;

③ let $\{(v_t^j, w_t^j) \mid 1 \le j \le l,\ 1 \le t \le |S| \text{ for each } j\}$ be a set of the $l \times |S|$ matched pairs of two alphabets in ② where v_t^j is the tth alphabet on BB, v_t^j is the tth alphabet on MB, then $\{w_t^j \mid 1 \le j \le l,\ 1 \le t \le |S| \text{ for each } j\}$ is send to the system ;

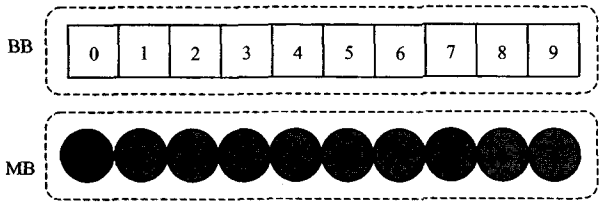
④ DPS receives $\{w_t^j \mid 1 \le j \le l,\ 1 \le t \le |S| \text{ for each } j\}$ and fetches $x_1x_2\cdots x_n y_1 y_2\cdots y_n$ from the memory ;

⑤ DPS accepts the user if $l = n$, and $w_{x_i}^j = y_j$ where u is a position of x_j on BB $1 \le j \le l$.

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.

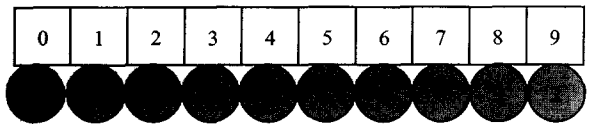
① DPS displays BB and MB on GUI where BB contains all alphabets in S in the order of 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, and MB contains all alphabets in S in the order of 6, 1, 3, 8, 9, 2, 7, 0, 4, 5 (See (Figure 1)) ;



(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

③ {(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 ;

④ DPS receives {7, 0, 4, 5, 6, 1, 3, 8, 9, 2}, and fetches 63 from the memory ;

⑤ the length of two password is 1, the number of match is 1, $w_{x_i}^1 = w_7^1 = 3$ 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 other 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 anthorized user on MB. We call this probability SSH (success using auccess history). Two cases of SSH must be considered : (a) (i mod $|P_2|$)th alphabet of second password is contained in ith $|S|$ alphabets for $1 \le i \le m$. We call this case SSH of Type 1 ; (b) ith $|S|$ alphabets contain any alphabet in two password. We call this case SSH of Type 2 ;

Theorem Let $S = s_1 s_2 \cdots s_m$ be a set of alphabets, $x_1 x_2 \cdots x_n y_1 y_2 \cdots y_n$ be dual password such that x_i, y_i are randomly selected with replacement ($1 \le i \le n$), then the probability to make fraudulent use of dual password is $1/m^n$ on the assumption that imposter does not know any information of the dual password.

3. Dual Password Derivation Problem

In this subsection, we define a new problem called *dual password derivation problem* that is related to the deriving method first password and second password from password, and also we present the evaluation factors for the solutions of dual password derivation problem.

Definition 2 Let S be a set of alphabets, P be a given string, f be a function deriving first password P_1 by using P, and g be another function deriving second password P_2 by using P, then dual password derivation problem is finding f and g such that the following probabilities or amounts are minimized :

① a probability that unauthorized user be accepted by DPS in a trial on the assumption that he knows nothing for the dual password. We call this probability OTS (one time success) ;

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 success history). Two cases of SSH must be considered : (a) (i mod $|S_2|$)th alphabet of second password is contained in ith $|S|$ alphabets for $1 \le i \le m$. We call this case SSH of Type 1 ; (b) ith $|S|$ 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 $S = \{i \mid 0 \le i \le 9\}$ 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 shortcoming 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

[1] M. Blum, A. De santis, S. Micali, and G. Persiano, "Noninteractive zero-knowledge," SIAM Journal on Computing, Vol.20, No.6, pp.1084-1118, 1991.

[2] D. C. Feldmeier and P. R. Karn, "UNIX password security-ten years later," Advances in Cryptology-CRYPTO '89, LNCS 435, pp.44-63, 1990.

[3] U. Feige, A. Fiat and A. Shamir, "Zero knowledge proofs of identity," Journal of Cryptology, pp.77-94, 1988.

[4] S. Goldwasser, S. Micali and C. Rachoff, "The knowledge complexity of interactive proof systems," SIAM Journal on Computing, pp.186-208, 1989.

[5] A. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," IEEE Trans. Pattern Ana. Machine Intell., Vol.19, No.4, pp.302-313, 1997.

[6] D. V. Klein, "Foiling the cracker : a survey of, and improvements to, password security," Proceedings of the 2nd USENIX UNIX Security Workshop, pp.5-14, 1990.

[7] K. -Y. Lam and T. Beth, "Timely authentication in distributed systems," Second European Symposium on Research in Computer Security, LNCS 648, pp.293-303, 1992.

[8] Z. M. Kovcs-Vajna, "A fingerprint verification system based on triangular matching and dynamic time warping," IEEE Trans, Pattern Ana. Machine Intell., Vol.22, No.11, pp. 1266-1276, 2000.

[9] A. J. Willis and L. Myers, "A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips," Pattern Recognition 34, pp.255-270, 2001.

박 승 배

e-mail : sbpark@chodang.ac.kr

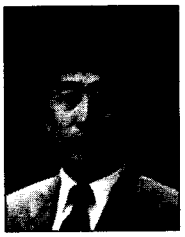
1989년 전남대학교 계산통계학과(이학사)

1992년 전남대학교 대학원 전산통계학과 (이학석사)

1996년 전남대학교 대학원 전산통계학과 (이학박사)

1996년~현재 초당대학교 컴퓨터과학과 조교수

관심분야 : 암호 알고리즘, 암호 프로토콜, 보안



박 성 배

e-mail : psbsos@suncheon.ac.kr

1985년 전남대학교 계산통계학과(이학사)

1987년 전남대학교 대학원 전산통계학과 (이학석사)

1998년 전남대학교 대학원 전산통계학과 (이학박사)

1988년~현재 순천제일대학 인터넷정보학부 교수

관심분야 : 분산시스템, 분산멀티미디어, 이동컴퓨팅

강 문 설

e-mail : mskang@hosim.kwangju.ac.kr

1986년 전남대학교 전산통계학과(이학사)

1989년 전남대학교 대학원 전산통계학과 (이학석사)

1994년 전남대학교 대학원 전산통계학과 (이학박사)

1989년~1994년 전남대학교 전산학과 조교 및 시간강사

1997년~2002년 한국정보처리학회 논문지 편집위원회(부위원장)

1994년~현재 광주대학교 공과대학 컴퓨터전자통신공학부 부교수

1996년~현재 한국정보처리학회 소프트웨어공학연구회 운영위원회(편집위원)

관심분야 : 소프트웨어공학, 컴포넌트기반 소프트웨어 개발, 객체지향시스템, 정보보호관리