안전하고 효율적인 신원확인을 위한 암호기반 시스템

박종민* · 박병전**

The Password base System for the safe and Efficient Identification

Jong-Min Park* · Byung-Jun Park**

요 약

사용자 고유번호와 패스워드 기반의 사용자 인증 매커니즘을 수행하는 네트워크 시스템 환경에서는 스니퍼 프로그램 등을 이용하여 불법 도청함으로써 쉽게 사용자의 패스워드를 알아낼 수 있다. 이러한 불법적인 도청에 의한 패스워드 노출 문제를 해결하는 방법으로 일회용 패스워드, Challenge-Response 인증 방식이 유용하게 사용되며, 클라이언트/서버 환경에서는 별도 동기가 필요 없는 시간을 이용한 일회용 패스워드 방식이 특히 유용하게 사용될 수 있다. 본 논문에서는 안전성은 Square root problem에 기초를 두고 있고, 프리플레이 공격, 오프라인 사전적 공격 그리고 서버 등을 포함하여 지금까지 잘 알려진 공격(해킹)들에 대해서 안전성을 높이기 위한 암호기반 시스템을 제안한다. 암호기반 시스템 확인은 패스워드를 생성하는데 특별한 키를 생성할 필요가 없다는 것이다. 암호기반 시스템은 검증자를 확인하는데 걸리는 시간이 적게 소요되면서 특출하다.

ABSTRACT

Almost all network systems provide an authentication mechanism based on user ID and password. In such system, it iseasy to obtain the user password using a sniffer program with illegal eavesdropping. The one-time password and challenge-response method are useful authentication schemes that protect the user passwords against eavesdropping. In client/server environments, the one-time password scheme using time is especially useful because it solves the synchronization problem.

In this paper, we propose a new identification scheme One Pass Identification. The security of Password base System is based on the square root problem, and Password base System is secure against the well known attacks including pre-play attack, off-line dictionary attack and server comprise. A number of pass of Password base System is one, and Password base System processes the password and does not need the key. We think that Password base System is excellent for the consuming time to verify the prover.

키워드

Identification, password base, Challenge-Response, square root problem

Ⅰ. Introduction

Identification is a process whereby a verifier is assured that the identity of a prover is as declared, thereby preventing impersonation [1, 2].

The password system is widely used identification scheme because of its advantages including easy implementation, low price and usability. The attacks which

* 조선이공대학 U-사이버보안과

** 조선대학교 (교신저자: 박병전)

접수일자 2008. 07. 30

must be guarded in the password system include: password disclosure at the outside of the system and line eavesdropping within the system, both of which allow subsequent replay [3] and password guessing including off-line dictionary attacks [4, 5].

Several cryptographic techniques have been presented for enhancing the security of the password system, but no cryptographic technique has been presented secure against the practical attacks including replay attack or pre-play attack [6] and off-line dictionary attack after server compromise [7] as yet. Examples include one time password [8] and salting technique. Pre-play attack is possible to fall the one time password system in secure, and off-linedictionary attack can be applied to the password system using the salting technique [5, 9].

In this paper, we present a new cryptographic identification scheme Password base System. The security of Password base System depends on the fact that if n is theproduct of two primes, then the ability to calculate square root mod n is computationally equivalent to the ability to factor n. Password base System is secure against the well attacks such as replay attack, pre-play attack, man-in-the-middle attack, eavesdropping, off-line dictionary attack, server compromise and off-line dictionary attack after server comprise.

Comparing Password base System with challenge response identification protocols and Zero Knowledge based identification protocols, Password base System processes the password and does not use the key, and a number of Password base System is one. Comparing Password base System only with Zero Knowledge based identification scheme, Password base System also satisfies that the prover provides not directly reusable by the verifier.

Comparing Password base System with non-interactive Zero Knowledge identification idea, Password base System does not use interactive proof, but the probability, the attacker impersonates the prove successfully, is not equal to that of non-interactive Zero Knowledge identification scheme.

II Preliminaries

A. Notation

Our notation is shown in the following :

P : A password of a user.

X_1, Y_1, X_2, Y_2 : Integers such that$(X_1 + X_2) \bmod N \equiv P$ and $(Y_1 + Y_2) \bmod N \equiv P$

N: N = pq where p and q are primes such that N is computationally infeasible to factor.

E_K : Symmetric encryption with key K.

D_K : Symmetric decryption with key K.

R: Random integer.

H: One way hash function.

B. Based on zero-knowledge proof

Zero knowledge protocols are designed to address that allowing a prove to demonstrate knowledge of a secret while revealing no information whatsoever of use to the verifier in conveying this demonstration of knowledge to others.

A proves knowledge of s to B in t executions of a 3-pass protocol[10,11]

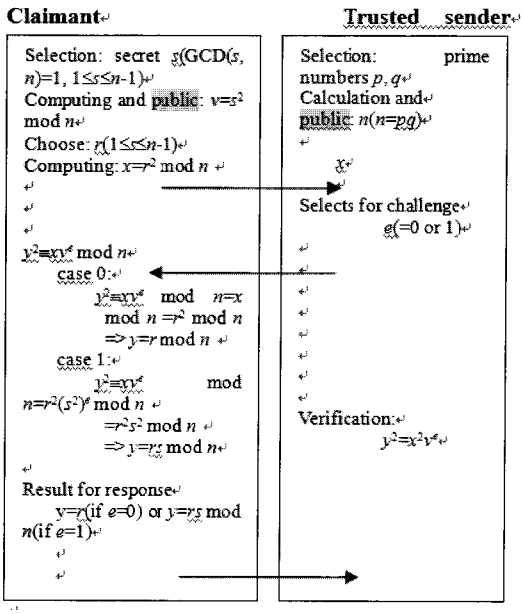

그림 1 영지식 프로토콜

Fig. 1 Zero Knowledge Protocol

C. NP-complete

The square root modulo n (SQROOT) problem is to find a square root of a module n for the given composite integer n and quadratic residue a modulo n. If the factors p and q are known, then SQROOT problem can be solved in polynomial time. If the factors p and q are unknown, then the factoring problem of n is reduced to SQROOT problem[12,13]in polynomial time [14], and the factoring problem of n is NP-complete [15].

Ⅲ. Password Base System

We first introduce an identification technique in Fig. 2which well describes how identification scheme is to be designed so that secure against off line dictionary attack.

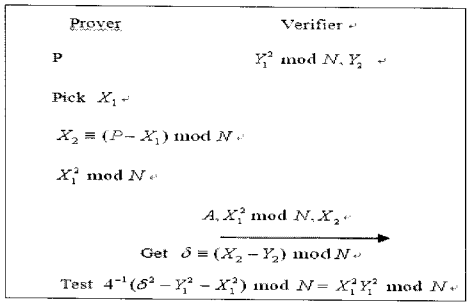

그림 2 첫 번째 신분확인 기술

Fig. 2 The first identification technique In the identification technique described at above, when a user registers P with his identity A, the verifier file.

chooses Y_1 in random ($0 \le Y_1 \le N-1$) and determines Y_2 such that Y_2 such that $Y_2 \equiv (P-Y_1) \bmod N$, and then stores $Y_1^2 \bmod N$ and Y_2 at A of the password file.

When the user inputs P with his identity A, the verifier chooses X_1 in random ($0 \le X_1 \le N-1$) and determines X_2 such that $X_2 \equiv (P-X_1) \bmod N$, and then sends A, $X_1^2 \bmod N$ and X_2 to the verifier. Let $\delta = (X_2 - Y_2) \bmod N$, the verifier knows $(Y_1 - X_1)^2 \bmod N \equiv \delta^2 \bmod N$ because of $(X_1 + X_2) \bmod N \equiv (Y_1 + Y_2) \bmod N$. Therefore, the verifier can determine whether $X_1^2 Y_1^2 \bmod N \equiv (4^{-1}(Y_1^2 + X_1^2 - \delta^2)^2) \bmod N$ is hold or not by using $X_1^2 \bmod N$ and X_2 received from the prover, and $Y_1^2 \bmod N$ and Y_2 stored at the password

The technique is secure against replay attack, because X1 is chosen in random. The technique is also secure against off-line dictionary attack, because it is too huge to store 2^N candidates for $X_1^2 \bmod N$. The technique is also secure against just password file compromise, because it is computationally infeasible to find X1 from $X_1^2 \bmod N$ even if the password file compromise, because it is computationally infeasible to find X1 from $X_1^2 \bmod N$ even if the password file is compromised. The technique is also secure against password file compromise with having performed off line dictionary attack, because it is computationally infeasible to find X1 from $X_1^2 \bmod N$, and X1 is chosen in random.

Let A, $X_{11}^2 \bmod N$ and X_{21} and A, $X_{12}^2 \bmod N$ and X_{22} be two messages sent to the verifier, then the attacker eavesdropped the messages in past communications can determine X_{11}^2 or X_{12} by using

$$X_{11}^2 \bmod N \equiv (X_{12} + \varepsilon)^2 \bmod N \text{ where } \varepsilon = X_{22} - X_{21}.$$

Therefore, the technique is vulnerable to eavesdropping, pre-play attack and man-in-the-middle attack.

The second identification technique in Fig. 3 describes how identification scheme is to be designed so that secure against eavesdropping.

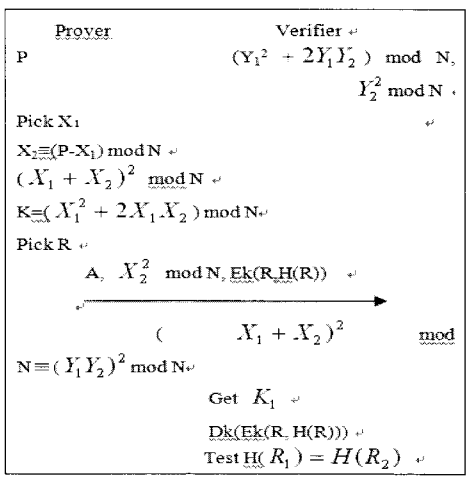

그림 3 두 번째 신원인식 기술

Fig. 3 The second identification technique

In the second identification technique, when a user registers P with his identity A, the verifier chooses Y_1 in random ($0 \le Y_1 \le N-1$) and determines Y_2 such that $Y_2 \equiv (P-Y_1) \bmod N$, and then stores $(Y_1^2+2Y_1Y_2) \bmod N$ and $Y_2^2 \bmod N$ at A of the password file.

When the user inputs P with his identity A, the verifier chooses X_1 and R_1 in random ($0 \le X_1 \le N-1$) and determines X_2 such that $X_2 \equiv (P-X_1) \bmod N$, and then sends A, $X_2^2 \bmod N$, $Ek_1(R, H(R))$ to the verifier where $k_1=(X_1^2+2X_1X_2) \bmod N$. the verifier can determine K_1 by using the fact that $(X_1+X_2)^2 \bmod N \equiv (Y_1+Y_2)^2 \bmod N$. The verifier performs $Dk(Ek(R, H(R)))$ and then tests whether $H(R_1)=H(R_2)$ is hold or not where $(R_1, H(R_2))=Dk(Ek(R, H(R)))$. The verifier accepts the prover only when $H(R_1)=H(R_2)$ is hold.

We can see that above property is true, because the problem finding a square root of a modulo n for the given composite integer n and quadratic residue a modulo n is a special case of the problem finding x in $(x+t)^2 \bmod n$ for a given t, quadratic residue a modulo n and n.

The technique is secure against replay attack, because X_1 is chosen in random. From the property, it is computationally infeasible to find X_1 in $(X_1^2+2X_1X_2) \bmod N$ under weak environments for the protocol that X_2 in $X_{22} \bmod N$ can be found in reasonable time heuristically, and the symmetric cryptosystem is vulnerable to cipher text only attack. Therefore, the technique is secure against pre-play, eavesdropping and man-in-the-middle.

The technique is secure against off-line dictionary attack, because it is too huge to store all candidates for $E_k(R,H(R))$.

The technique is secure against password file compromise without having performed off-line dictionary attack, because the password was not stored at the password file in clear text.

The technique is vulnerable to password file compromise with having performed off-line dictionary attack because of $P^2 \bmod$

$$N \equiv (Y_1^2+2Y_1Y_2-Y_2^2)$$

mod N. The Password base System described in Fig. 4.

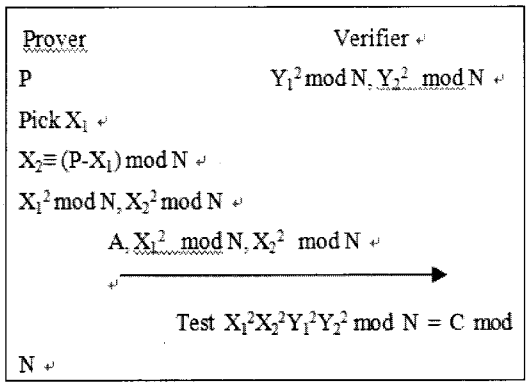

그림 4 안전한 패스워드 기반 시스템
Fig. 4 password base System Secure

In the password base system secure, $C=64^{-1}(Y_1^2+Y_2^2-X_1^2-X_2^2)^2-4X_1^2X_2^2-4Y_1^2Y_2^2)^2$. When a user registers P with his identity A, the verifier chooses Y_1 in random ($0 \le Y_1 \le N-1$) and determines Y_2 such that $Y_2 \equiv (P-Y_1) \bmod N$, and then stores $Y_1^2 \bmod N$ and $Y_2^2 \bmod N$ at A of the password file.

When the user inputs P with his identity A, the verifier chooses X_1 in random ($0 \le X_1 \le N-1$) and determines X_2 such that $X_2 \equiv (P-X_1) \bmod N$, and then sends A, $X_1^2 \bmod N$ and $X_2^2 \bmod N$ to the verifier. The verifier knows $(X_1+X_2)^2 \bmod N \equiv (Y_1+Y_2)^2 \bmod N$ because of $(X_1+X_2) \bmod N \equiv (Y_1+Y_2) \bmod N$, and therefore the verifier can calculate $2(X_1X_2-Y_1Y_2) \bmod N \equiv (Y_1^2+Y_2^2-X_1^2-X_2^2) \bmod N$, leaded from $(X_1+X_2)^2 \bmod N$. Therefore, the verifier can determine whether $(X_1^2X_2^2Y_1^2Y_2^2) \bmod N \equiv (64^{-1}((Y_1^2+Y_2^2-X_1^2-X_2^2)^2-4X_1^2X_2^2-4Y_1^2Y_2^2)^2) \bmod N$ is hold or not by using $X_1^2 \bmod N$, $X_2^2 \bmod N$ and received from the prover, and $Y_1^2 \bmod N$, $Y_2^2 \bmod N$ stored at the password file.

The Password base System is secure against replay attack, because X1 is chosen in random. It is computationally infeasible to determine X_1 in $X_1^2 \bmod N$. Therefore, the Password base System is secure against pre-play, eavesdropping, man-in-the-middle. The Password base System is secure against off-line dictionary attack, because it is too huge to store 2^N candidates for $X_1^2 \bmod N$.

The Password base System is secure against password file compromise without having performed off-line dictionary attack, because the password was not stored at the password file in clear text, and furthermore the Password base System is also secure password compromise with having performed off line dictionary attack, because the security against password file compromise of the Password base System depends on SQROOT problem, and it is too huge to store 2^N candidates for Y_1^2 mod N.

The performance of Password base System is in Table 1. In Table 1, we have assumed that the verifier first calculates $((Y_1^2+Y_2^2 - X_1^2 - X_2^2)^2) - 4X_1^2X_2^2 - 4Y_1^2Y_2^2)^2$ mod N and then calculates $64\text{-}1(Y_1^2+Y_2^2 - X_1^2 - X_2^2)^2 - 4X_1^2X_2^2 - 4Y_1^2Y_2^2)^2$ mod N.

표 1 안전한 패스워드 기반 시스템의 성능
Table 1 The performance of password base system secure

	Prover	Verifier (Off line)	Verifier (On line)
Pass	1	0	0
Random number generation	1	1	0
Modular square multiplication	2	2	1
Modular multiplication	0	0	2

Ⅳ. CONCLUSIONS

We have presented a new identification scheme called password base system. The password base system is secure against the well known attacks such as replay attack, pre-play attack, man-in-the-middle attack, eavesdropping, off-line dictionary attack, password file compromise, and furthermore secure against the password file compromise with having performed off-line dictionary attack. It is the stability that is based on Square Root Problem, and we would like to suggest password base system, enhancing the stability, for all of the well-known attacks by now including Off-line dictionary attack, password file compromise, Server and so on.

A number of pass of password base system is one, password base system processes the password and does not use the key. We think that password base system is excellent in the consuming time to verify the prover.

The password base system is also excellent in the aspect of the performance.

REFERENCES

[1] A. Hill, A. D. Brett, and C. J. Taylor, *"Automatic landmark identification* using a new method of non-rigid correspondence" in Proceedings of IPMI '97 Conference, vol. 1230, pp. 483~488,1997.

[2] E. Moulines, P. Duhamel, J.F. Cardoso, and S. Mayrargue, *Subspace methods for the blind identification* of multichannel fir filters, IEEE Transactions on Signal Processing, SP-43, pp. 516~525, 1995.

[3] Bao, F., R. Deng and W. Mao. *Efficient and practical fair exchange protocols with off-line* TTP. 1998 IEEE Symposium on Security and Privacy. Oakland, IEEE Compute Society. pp 77~85. 1998.

[4] A. W. Senior and A. J. Robinson. *An off*-line cursive handwriting recognition system. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3) pp309~321, 1998.

[5] Jong-Min Park, Yong-Hun Kim, Beom-Joon Cho, "Password System Enhancing the Security against", The Korean Institute of Maritime Information & Communication Science, Vol. 8, No. 8, pp.2004.

[6] Andreoni, J. and H. Varian, *"Pre*-play Contracting in the Prisoners' Dilemma", mimeo, University of Wisconsin, 1999.

[7] Bensaid, B. and R.J. Gary-Bobo, *"An Exact Formula for the Lion's Share: A Model of Pre*-Play Negotiation," Games and Economic Behavior, 14, pp 44~89, 1996.

[8] Neil Haller. The s/key(tm) *one*-time password system. In Proceedings of the 1994 Symposium on Network and Distributed System Security, pp 151~157, 1994.

[9] Neil Haller. The s/key(tm) one-time password system. *Symposium on Network and Distributed System Security,* pp 151~157, February 1994.

[10] B. Schneier, Applied cryptography, John Wiley & Sons, 1996.

[11] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like cryptosystems", Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 2-21

[12] P. MacKenzie, "The PAK suites: Protocols for Password-Authenticated Key Exchange", 2002.

[13] Jong-Min Park, "Efficient and Secure Authenticated Key Exchange", The Korean Institute of Maritime Information & Communication Science, Vol. 3, No. 3, pp.2005.

[14] H. Woll, "Reductions among number theoretic problems, Information and Computation, Vol. 72, pp. 167-179, 1987.

[15] E. Bach, Algorithmic Number Theory, Volumn 1: Efficient Algorithms, MIT Press, Cambridge Massachusetts, 1996.

저자소개

박 종 민(Jong-Min Park)

1988년 조선대학교 전자계산 전공 (공학석사)
2005년 조선대학교 컴퓨터공학전공 (공학박사)
2008년 ~ 현재 조선이공대학 U-사이버보안과
※관심분야 : 바이오인식, 패턴인식, 인공지능, 정보보호 및 보안

박병전(Byung-Jun Park)

1993년 서울대학교 통계학 전공 (이학석사)
1998년 조선대학교 통계학 전공 (이학박사)
2005년 ~ 현재 조선대학교
※관심분야 : 바이오인식, 패턴인식, 통계학, 정보보호 및 보안