효율적이고 안전한 인증에 기초한 사람이 기억하기 쉬운 패스워드

김용훈*, 조범준**
*조선대학교 컴퓨터공학과
**조선대학교 컴퓨터공학과
e-mail:mulmi99@ketis.or.kr, bjcho@chosun.ac.kr

Human Memorable Password based Efficient and Secure Identification

Yong-Hun Kim*, Beom-Joon Cho**
*Dept. of Computer Science Engineering, Cho-Sun University
**Dept. of Computer Science Engineering, Cho-Sun University

요 약

본 논문은 이른바 패스워드 기반 인증(PBI)이라고 부르는 사람이 기억하기 쉬운 패스워드 처리 과정의 인증 프로토콜을 제안한다. PBI는 온라인 사전 방식의 공격과 패스워드 파일의 중간 결과물의 공격들에 대응하여 안전하다. PBI는 실행 결과에서도 역시 뛰어나다.

1. 서론

인증은 프로토콜에 수반된 신분 증명이 자신임을 확인하는 과정이다. 그리고 검증자가 실제로 참여한다. 인증은 검증자가 증명자의 흉내를 예방하면서 자신임을 선언하여 인증을 처리하는 것이다. 패스워드 시스템은 간단한 구현, 낮은 가격 그리고 유용성의 이점들 때문에 가장 널리 사용되는 인증 시스템이다. 그리고 패스워드 시스템은 시스템 외부에서 패스워드를 선언하거나, 시스템 내부에서 도청하거나 오프라인 사전 공격들을 포함하는 패스워드 추측에도 보호를 할 수 있다.

원 타임 패스워드(one time password)[9]와 salting 기법[10]과 같은 몇몇 암호 테크닉들은 패스워드 시스템의 안전을 높이기 위하여 제안되었다. 그러한 노력에도 불구하고 완전한 패스워드 인증 처리 기술은 아직까지는 없다.

이러한 패스워드 시스템의 약점을 극복하고자 몇 가지 challenge response 프로토콜[2,6,7]과 영 지식(zero knowledge) 인증 프로토콜[4,5,8]이 제시되었다. 그러나 사람이 기억하기 쉬운 패스워드를 처리하지는 못하고 있다. 그 중 몇몇 프로토콜은 신뢰할 만한 써드파티(third party)가 필요하고, 다른 프로토콜들 원 패스(one pass)로는 완전하지 못하다.

본 논문은 사람이 기억하기 쉬운 패스워드 기반의 인증(PBI)시스템이라 부르는 새로운 인증 프로토콜을 소개한다. 그리고 PBI를 소개하기 전에, PBI에 관련되는 두 가지 인증 테크닉들을 소개한다.

PBI의 안전성은 제곱근(square root) 문제에 달려있다. 다시 말하면, PBI의 안전성은 두 소수의 곱 n이라면 mod n의 제곱근과 인자 n이 계산적으로 같음을 보여주는 능력이다[11]. 보안에 대응하는 재전송(Replay)공격, 선전송(Pre-play)공격, 중간 침입자(Man-in-the-middle)공격, 도청(Eavesdropping), 오프라인 사전(Off-line dictionary) 공격, 패스워드 파일(Password file) 손상, 심지어 오프라인 사전 공격을 실행한 패스워드 파일 공격까지도 PBI는 안전하다.

PBI는 challenge response 인증 프로토콜들 그리고 영 지식 인증 프로토콜들과 비교하면, PBI는 사람이 기억하기 쉬운 패스워드를 처리하고, 수많은 PBI의 패스는 원 패스(one pass)로 처리된다. PBI는 2절에서 설명한다.

1.1 표기법

표기법은 다음과 같다:

P : 사용자 패스워드.

X_1,Y_1,X_2,Y_2 : $(X_1+X_2) \bmod N \equiv P$ 그리고 $(Y_1+Y_2) \bmod N \equiv P$와 같은 정수.

N : N=pq 여기서 p,q는 정수이고 N은 계산 불가능한 약수.

E_K : 대칭암호키K

D_K : 대칭복호키K

R : 랜덤한 정수

H : 일방향 해쉬 함수(one-way hash function)

1.2 인증의 안전

인증보호에 필요한 기본적인 공격 목록은 다음과 같다.

· 재 전송 : 합법적인 사용자가 과거에 통신했던 메시지를 공격자가 저장했다가 이후의 통신에 재전송하는 공격이다.

· 선 전송 : 공격자 현재 통신에서 기록된 메시지로부터 메시지를 결정하여 과거의 메시지를 보낸다.

· 도청 : 공격자가 온라인상의 통신 내용을 도청하여 세션키의 정보를 알아내거나, 통신에서 사용되는 유용한 정보를 알아내는 공격이다.

· 중간 침입자 공격 : 통신 선로상의 중간에 위치한 공격자가 서버와 사용자 사이에 전송되는 정보들을 불법으로 도청·변경하여 전송함으로써 합법적인 사용자들 간의 세션키를 구해내는 공격이다.

· 패스워드 추측 공격(Password guessing attacks) : 공격자가 비교적 작은 사전에 포함된 보통의 단어를 패스워드로 선택하여 액세스 해본다. 기본적으로 온라인 사전에 의한 방법과 오프라인 사전에 의한 공격의 두 가지 방법으로 공격한다. (1) 오프라인 사전 공격: 공격자는 과거의 통신 기록에서 사전을 이용하여 통신 내용에 포함된 패스워드를 찾아 공격에 이용한다. (2) 온라인 사전 공격: 공격자가 사용자로 가장하여 사전을 이용하여 반복해서 패스워드를 입력한다. 만일 실패하면 사전상의 또 다른 패스워드를 입력하며, 입력이 유효할 때까지 시도한다. 본 논문에서는 오프라인 사전 공격만을 다룬다.

· Password file compromise: 공격자가 패스워드 파일에 사용자인 것처럼 보안을 유지한 채 민감한 파일을 액세스한다.

2. 패스워드 기반 인증

제곱근 modulo N (SQROOT) 문제는 혼성의 완전체 R 그리고 2차함수의 나머지 O modulo H를 위하여 O modulo H의 제곱근을 찾는 것이다 . 인자 p와 q를 알고 있을 때, SQROOT 문제는 다항식의 곱으로 해결될 수 있다[1,3]. 만일 인자 pq를 알지 못한다면, n의 인수분해하는 문제는 다항식에서 SQROOT 문제로 된다[11]. 그리고 N의 인수분해 문제는 NP-complete이다[1,3].

오프라인 사전 공격에 대항하는 보안 인증 테크닉을 그림1에 소개한다.

Prover	Verifier
P	$Y_1^2 \bmod N$, Y_2
Pick X1	
$X_2 \equiv (P-X_1) \bmod N$	
$X_1^2 \bmod N$	
	A, $X_1^2 \bmod N$, X^2 →
	Get $\delta \equiv (X_2-Y_2) \bmod Y$
	Test $4^{-1}(\delta^2-Y_1^2-X_1^2)^2 \bmod N \doteq X_1^2Y_1^2 \bmod N$

그림1: 첫 번째 인증 테크닉

위의 그림에서 P는 사용자 레지스터, 식별자는 A, 검증자는 $(0 \le Y_1 \le N-1)$사이의 랜덤한 Y_1을 선택하고, $Y_2 \equiv (P-Y_1) \bmod N$인 Y_2를 결정하고, 패스워드 파일 A에 $Y_1^2 \bmod N$ 과 Y_2를 저장한다.

식별자 A의 사용자가 P를 입력할 때, 검증자는 $(0 \le Y_1 \le N-1)$사이의 X_1을 선택하고, $X_2 \equiv (P-X_1) \bmod N$인 X_2를 결정하고, 검증자에게 A, $X_1^2 \bmod N$과 X_2를 전송한다. $\delta=(X_2+Y_2) \bmod N$이라 놓으면, 검증자는 $(X_1+X_2) \bmod N \equiv (Y_1+Y_2) \bmod N$이므로 $(Y_1-X_1)^2 \bmod N \equiv \delta^2 \bmod N$임을 알 수 있다. 그러므로 검증자는 $X_1^2Y_1^2 \bmod N \equiv (4^{-1}(Y_1^2+X_1^2-\delta^2)^2) \bmod N$이 유지되거나 증명자로부터 받은 $X_1^2 \bmod N$과 X_2를 사용하지 않아도 결정할 수 있으며, $Y_1^2 \bmod N$과 Y_2를 패스워드 파일에 저장한다.

이는 X_1을 랜덤하게 선택할 수 있어 재전송 공격에 대응하여 안전하다. 또한 $X_1^2 \bmod N$의 후보가 2^N 정도의 큰 저장 공간때문에 오프라인 사전 공격에도 대응하는 보안책이다. 비록 패스워드 파일이 손상되었더라도 $X_1^2 \bmod N$을 계산하여 찾아내는 것이 불가능하므로 패스워드 파일 손상에 대응할 수 있다. 이 테크닉은 X_1을 랜덤하게 선택하고, $X_1^2 \bmod N$으로부터 X_1을 찾는 계산이 불가능하여 오프라인 사전 공격에도 패스워드 파일 손상에 대응할 수 있다.

A, $X_{11}^2 \bmod N$과 X_{21}과 A, $X_{12}^2 \bmod N$과 X_{22}의 두

메시지를 검증자에게 보내면 공격자는 메시지를 도청하고 $\varepsilon=X_{22}-X_{21}$일 때 $X_{11}^2 \bmod N \equiv (X_{12}+\varepsilon)^2 \bmod N$을 사용하여 X_{11}또는 X_{12}를 결정한다. 그러므로 도청, 선전송, 중간 침입자 공격에 유용한 기술이다.

두 번째 인증 테크닉은 그림2에 묘사되어 있는 것처럼 도청에 대응하여 안전하다.

Prover	Verifier
P	$(Y_1^2+2Y_1Y_2) \bmod N$, $Y_2^2 \bmod N$
Pick X_1	
$X_2 \equiv (P-X_1) \bmod N$	
$(X_1+X_2)^2 \bmod N$	
$K=(X_1^2+2X_1X_2) \bmod N$	
Pick R	
$A, X_1^2 \bmod N, E_K(R,H(R))$ →	
	$(X_1+X_2)^2 \bmod N \equiv (Y_1+Y_2)^2 \bmod N$
	Get K_1
	$D_K(E_K(R, H(R)))$
	Test $H(R_1) \stackrel{?}{=} H(R_2)$

그림2 : 두 번째 인증 테크닉

두 번째 인증 테크닉은 식별자가 A이고, 사용자 레지스터가 P일 때 검증자는 $(0 \le Y_1 \le N-1)$사이의 랜덤한 Y_1과 $Y_2 \equiv (P-Y_1) \bmod N$의 Y_2를 선택하고 A에서 $(Y_1^2+2Y_1Y_2) \bmod N$과 $Y_2^2 \bmod N$을 패스워드 파일에 저장한다.

식별자가 A이고 사용자가 P를 입력하면 검증자는 $(0 \le X_1 \le N-1)$사이의 랜덤한 X_1과 R_1을 $X_2 \equiv (P-X_1) \bmod N$인 X_2를 결정하여 검증자에게 A, $X_2^2 \bmod N$, $E_{K1}(R, H(R))$을 보낸다. 여기서 $K_1=(X_1^2+2X_1X_2) \bmod N$. 검증자는 $(X_1+X_2)^2 \bmod N \equiv (Y_1+Y_2)^2 \bmod N$을 사용하여 K_1을 결정한다. 검증자는 $D_K(E_K(R,H(R)))$을 수행하고 $H(R_1)=H(R_2)$일 때까지 테스트한다. 여기서 $(R_1,H(R_2))=D_K(E_K(R,H(R)))$. 검증자는 증명자가 $H(R_1)=H(R_2)$로 될 때 수락한다.

Property n=pq라 하고, 두 소수 p와 q가 계산 불가능 할 때 n을 선택한다. 그리고 문제는 주어진 t에서 $(x+t)^2 \bmod n$에서 x를 찾는 것이다. 2차함수 나머지 a modulo n과 n은 NP-complete이다.

위의 특성은 참이다. 왜냐하면 주어진 혼합형 정수(composite integer)n의 a modulo n의 square root와 2차함수 나머지 a modulo n은 $(x+t)^2 \bmod n$에서 x를 찾는 특별한 문제이다.

이 테크닉은 X_1이 랜덤한 값에서 선택하기 때문에 재송신 공격에 대응하여 안전하다. $X_2^2 \bmod N$에서 X_2는 적절한 시간이 되면 찾을 수 있고, 암호문으로 공격당하기 쉬운 대칭 암호 프로토콜은 시스템의 미약한 환경아래 $(X_1^2+2X_1X_2) \bmod N$에서 X_1의 특성 때문에 계산하기가 어렵다. 그러므로 이 테크닉은 선전송, 도청, 중간 침입자 공격에 대응하여 안전하다. 이 테크닉은 $E_K(R,H(R))$의 모든 후보가 너무 거대하여 저장하기가 어렵기 때문에 오프라인 사전 공격에 대항하는 보안 방법이 될 수 있다. 또한 이 테크닉은 패스워드가 평문 패스워드로 저장되지 않기 때문에 오프라인 사전 공격도 어렵다.

그러나 이 테크닉은 $P_2 \bmod N \equiv (Y_1^2+2Y_1Y_2+Y_2^2) \bmod N$이기 때문에 오프라인 사전 공격의 수행했을 때 패스워드 파일의 결과물은 공격당하기 쉽다.

PBI는 그림3에 설명하였다.

Prover	Verifier
P	$Y_1^2 \bmod N$, $Y_2^2 \bmod N$
Pick X_1	
$X_2 \equiv (P-X_1) \bmod N$	
$X_1^2 \bmod N$, $X_2^2 \bmod N$	
$A, X_1^2 \bmod N, X_2^2 \bmod N$ →	
	Test $X_1^2X_2^2Y_1^2Y_2^2 \bmod N \stackrel{?}{=} C \bmod N$

그림3 : PBI

PBI에서 $C=64^{-1}((Y_1^2+Y_2^2-X_1^2-X_2^2)-4X_1^2X_2^2 -4Y_1^2Y_2^2)^2$. 식별자가 A이고, 사용자 레지스터가 P일 때 검증자는 $(0 \le Y_1 \le N-1)$사이의 랜덤한 Y_1과 $Y_2 \equiv (P-Y_1) \bmod N$의 Y_2를 선택하고 A에서 $Y_1^2 \bmod N$과 $Y_2^2 \bmod N$을 패스워드 파일에 저장한다.

식별자가 A이고 사용자가 P를 입력하면 검증자는 $(0 \le X_1 \le N-1)$사이의 랜덤한 X_1과 $X_2 \equiv (P-X_1) \bmod N$인 X_2를 결정하여 검증자에게 A, $X_1^2 \bmod N$, $X_2^2 \bmod N$을 보낸다. 검증자는 $(X_1+X_2) \bmod N \equiv (Y_1+Y_2) \bmod N$의 관계로 $(X_1+X_2)^2 \bmod N \equiv (Y_1+Y_2)^2 \bmod N$을 알고 있으며 검증자는 $(X_1+X_2)^2 \bmod N \equiv (Y_1+Y_2)^2 \bmod N$으로부터 $2(X_1X_2-Y_1Y_2) \bmod N \equiv (Y_1^2+Y_2^2-X_1^2-X_2^2) \bmod N$을 계산할 수 있다. 그러므로 검증자는 $(X_1^2X_2^2Y_1^2Y_2^2) \bmod N \equiv (64^{-1}((Y_1^2 +Y_2^2-X_1^2-X_2^2)^2-4X_1^2X_2^2-4Y_1^2Y_2^2)^2) \bmod N$을 유지하든지 검증자로부터 $X_1^2 \bmod N$, $X_2^2 \bmod N$을 사용하든지 않든지 $Y_1^2 \bmod N$, $Y_2^2 \bmod N$을 패스워드 파일에 저장한다.

PBI는 X_1의 선택이 랜덤하기 때문에 재전송 공격에 대응하여 안전하다. $X_1^2 \bmod N$에서 X_1을 결정하

는 계산이 불가능하기 때문에 PBI는 선전송, 도청, 중간 침입자 공격에 대응하여 안전하다. 또한 $X_1^2 \bmod N$의 후보가 2^N정도의 큰 저장 공간 때문에 PBI는 오프라인 사전 공격에 대응하여 안전하다. 또한 PBI는 패스워드 파일이 평문으로 저장되지 않기 때문에 오프라인 사전 공격도 어렵다. 게다가 PBI의 패스워드 파일의 중간 결과물이 SQROOT문제에 의존하며, $Y_1^2 \bmod N$이 후보가 2^N정도의 큰 저장 공간 때문에 오프라인 사전 공격에 안전하다.

PBI이 결과는 표1과 같다. 표1에서 검증자에게 첫 째로 $((Y_1^2+Y_2^2-X_1^2)^2-4X_1^2X_2^2-4Y_1^2Y_2^2)^2 \bmod N$과 두 번째로 $64^{-1}((Y_1^2+Y_2^2-X_1^2-X_2^2)^2-4X_1^2X_2^2-4Y_1^2Y_2^2)^2 \bmod N$을 계산했다.

	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

표1 : PBI 결과

3. 결론

이제까지 사람이 기억하기 쉬운 PBI과정의 인증 프로토콜에 대해 알아보았다. PBI는 오프라인 사전 공격, 패스워드 파일 결과물과 같은 잘 알려진 공격에 대해서 안전하다는 것을 알았다. 또한 PBI는 뛰어난 실행 결과를 얻을 수 있다.

참고문헌

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

[2] M. J. Beller and Y Yacobi, "Limitations of the Kerberos authentication system", Computer Communication Review, Vol.20, pp. 119-132, 1990.

[3] H. Cohen, A Course in Computational Algebraic Number. Theory, Springer-Verlag, Berlin, 1993.

[4] U. Feige, A. Fiat and A. Shamir, "Zero knowledge proof of identity", Journal of Cryptology, Vol.1, pp.77-94, 1983.

[5] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems", Advances in Cryptology-CRYPTO'86, LNCS 263, pp. 186-194, 1987.

[6] K. Gaarder and E. Snekkenes, "Applying a formal analysis technique to the CCITT X. S09 strong two way authentication protocol", Journal of Cryptology, Vol. 3, pp. 81-98, 1991.

[7] L. Gong, "A security risk of depending on synchronized clocks", Operating System Review, Vol.26, pp.49-53, 1992.

[8] L. C. Guillou and J. -J. Quisquater, "A practical zero-knowledge protocol to security microprocessor minimizing both transmission and memory", Advances in Cryptology-EUROCRYPT '88, LNCS 330, pp. 123-128, 1988.

[9] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, Vol.24, pp.770-772, 1981.

[10] R. Morris and K. Thompson, "Password security: a case history", Communications of the ACM, Vol.22, pp.594-597, 1979.

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