One Pass Identification processing Password-based

Byung-Jun Park and Jong-Min Park

Abstract— Almost all network systems provide an authentication mechanism based on user ID and password. In such system, it is easy 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 present a new identification scheme OPI(One Pass Identification). The security of OPI is based on the square root problem, and OPI is secure against the well known attacks including pre-play attack, off-line dictionary attack and server comprise. A number of pass of OPI is one, and OPI processes the password and does not need the key. We think that OPI is excellent for the consuming time to verify the prover.

Index Terms— identification, pre-play attack, off-line dictionary attack, server comprise, square root modular a 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 most widely used identification scheme because of its advantages including easy implementation, low price and usability. The attacks which 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 [5] and password guessing including off-line dictionary attacks [6, 12].

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 [3] and off-line dictionary attack after server compromise [4] as yet. Examples include one time password [7] and salting technique. Pre-play attack is possible to fall the one time password system insecure, and off-line dictionary attack can be applied to the password system using the salting technique [8, 12].

In this paper, we present a new cryptographic identification scheme OPI (One Pass Identification). The security of OPI depends on the fact that if n is the product of two primes, then the ability to calculate square root mod n is computationally equivalent to the ability to factor n. OPI is secure against the well know 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 OPI with challenge response identification protocols and ZK(Zero Knowledge) based identification protocols, OPI processes the password and does not use the key, and a number of pass of OPI is one. Comparing OPI only with ZK based identification scheme, OPI also satisfies that the prover provides not directly reusable by the verifier.

Comparing OPI with non-interactive ZK identification idea, OPI does not use interactive proof, but the probability, the attacker impersonates the prover successfully, is not equal to that of non-interactive ZK identification scheme.

II. PRELIMINARIES

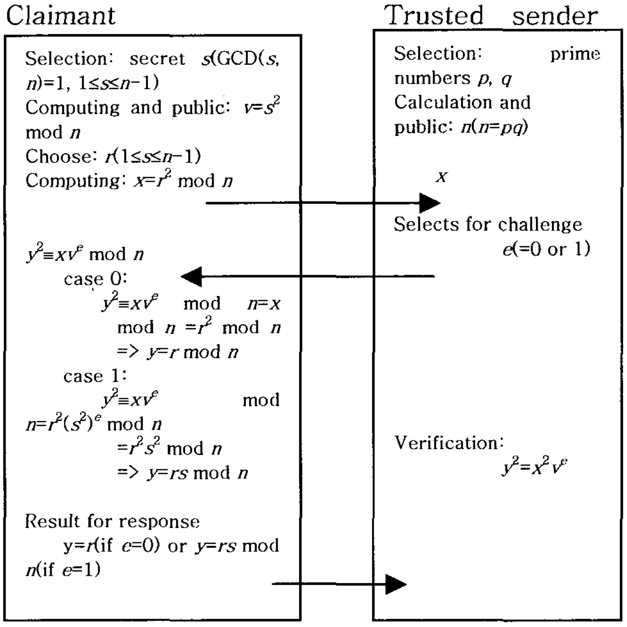
Claimant
Trusted sender
Selection: secret s(GCD(s, n)=1, 1≤s≤n−1)
Computing and public: $v=s^2$ mod n
Choose: r(1≤s≤n−1)
Computing: $x=r^2$ mod n
Selection: prime numbers p, q
Calculation and public: n($n=pq$)
x
Selects for challenge e(=0 or 1)
$y^2 \equiv xv^e$ mod n
case 0:
$y^2 \equiv xv^e$ mod $n=x$ mod n $=r^2$ mod n
=> $y=r$ mod n
case 1:
$y^2 \equiv xv^e$ mod $n=r^2(s^2)^e$ mod n
$=r^2s^2$ mod n
=> $y=rs$ mod n
Verification: $y^2=x^2v^e$
Result for response
y=r(if e=0) or $y=rs$ mod n(if e=1)

Fig. 1 ZK(Fiat-Shamir identification Protocol).

Manuscript received October 30, 2006.

Byung-jun Park is with BK21 Project Corp.

Jong-Min Park is with field school of computer, Dongshin University

Zero knowledge protocols are designed to address that allowing a prover 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

III. ONE PASS IDENTIFICATION

The aim of this paper is to design the identification scheme such that (1) processes the secret information inputted by the prover, (2) minimizes a number of passes and (3) does not need this key while preserving (4) secure against the well known attacks and (5) excellent performance in the aspect of the time consumed in verification of the prover. OPI described in the following is activated when a prover inputs his password pwd:

Protocol: OPI

1)System parameter

A trusted center publishes the common modulus n = pq for all users, after selecting two secret primes p and q such that n is computationally infeasible to factor.

2)Selection of the prover's parameters

The prover selects a random integer $x_{1i}(1 \le x_{1i} \le n-1)$ and obtains timestamp t_i where i denotes $_i$th access to a system resource. The prover determines x_{2i} such that $x_{2i} \equiv (pwd-x_{1i}) \bmod n$.

*3)*Parameters stored at the verifier's password file:

$y_1^2 \bmod n$ and y_2 are stored where y_1 $(1 \le y_1 \le n-1)$ is selected in random and $y_2 \equiv (pwd- y_1) \bmod n$.

4)Protocol message

The prover sends t_I, x_{2i} and $(x_{1i} + t_i)^2 \bmod n$ to the verifier.

5)Protocol action

The verifier accepts prover's identity, if the following Equ. 1 is hold.

$C^2 \bmod n =(4(y1^2 \bmod n)(x_{1i} +t_i)^2 \bmod n) \bmod n$ where $C=((x_{1i}+t_i)2+y1^2-(x2^2_i+y2^2_i+ t_i^2)+(2x_{2i}y_2 +2x_{2i}+t_i-2y_2t_i))$ (Equ. 1)

We first have to show that whether OPI permits the prover to access system resource and whether the attacker can impersonate the prover, the one is showed in Theorem 1 while the Will show that OPI is secure against the well known attacks excepting on line dictionary attack also in the following.

In replay attack[13], the attacker records messages which were sent in past communications and re-sends them at a later time. Let assume that the prover sends only x_{2i} and $x_1{}_i^2 \bmod n$, then the prover sends time variant parameters to the verifier, because x_{1i} is selected in random. But the verifier permits the attacker to access a system resource, when the attacker re-sends x_{2j} and $x_1{}_j^2 \bmod n$ as if x_{2i} and $x_1{}_i^2$ for $2 \le i$ and $j<i$. Time stamp t_i prevents re-use of t_j because of $t_j \neq t_i$ for $2 \le i$ and $j<i$. For this reason, OPI is secure against replay attack.

For pre-play attack, the attacker records message which were sent in past communications and determines current messages from the recorded message. Let assume that prover sends t_j, x_{2j} and $x_1^2{}_j \bmod n$, then the verifier permits the attacker to access a system resource, when the attacker sends t_j, x_{2j} and $x_1^2{}_j \bmod n$, then the verifier permits the attacker to access s system resource, when the attacker sends t_j, x_{2j} and $x_1^2{}_j \bmod n$ for $2 \le i$ and $j<i$, because the attacker can determine t_i.

We have to consider the security of OPI against pre-play attack for the two cases: whether the attacker can determine (a) $(x_{1i}+t_i)^2 \bmod n$; (b) $(x_{1j}+t_i)^2 \bmod n$ from t_j, x_{2j} and $(x_{1j}+t_i)^2 \bmod n$ for $2 \le i$ and $j<i$.

For the case of (a), the attacker knows t_j, t_i, x_{2j} and $(x_{1j}+t_j)^2 \bmod n$ and can determine x_{2i}, and also he knows that $(x_{1j} + x_{2j}) \bmod n=(x_{1i} + x_{2i}) \bmod n$ and t such that $t_i=t_j+t$.

At $(x_{1j} + x_{2j}) \bmod n=(x_{1i} + x_{2i}) \bmod n$, the attacker can select x_{2i} and obtains $(x_{1j} - x_{1i}) \bmod n=(x_{2i} - x_{2j}) \bmod n$. Let $x_{1i}=(x_{1j}-D) \bmod n$. We have to consider whether it is possible that the attacker can determine $((x_{1j}-D)+(t_j+t))^2 \bmod n$ at t_j+t, x_{2i} and $((x_{1j}-D)+(t_j+t))^2 \bmod n$. The attacker can determine $D_1 \bmod n$ and $D_3 \bmod n$ at $(D_1-2x_{1j}D_2+D_3) \bmod n=((x_{1j}-D)+(t_j+t))^2 \bmod n$ where $D_1=(x_{1j}+t_j)^2 \bmod n$, $D_2=(D-t)$ and $D_3=(D-t)^2 -2t_j(D-1)$, but the hardness finding $2x_{1j}D_2 \bmod n$ at $(D_1-2x_{1j}D_2+D_3) \bmod n$ depends on Property 1. For the case of (b), the attacker knows t_j, t_i, x_{2j} and $(x_{1j}+t_j)^2 \bmod n$. The attacker can determine $D_1 \bmod n$ and $E \bmod n$ at $(D_1-2x_{1j}t+E) \bmod n=(x_{1j}+(t_j+t))^2 \bmod n$ where $t=t_i-t_j$ and $E=2\ t_j +t^2$, and D_1 is that of the case (a). But the hardness finding $2x_{1j}t \bmod n$ at $(D_1-2x_{1j}t+E) \bmod n$ depends on other is mentioned in Section 4.

Theorem 1 The verifier permits the prover to access the system resource in OPI.

Proof $(x_{1i} - y_1 + t_i)^2 \bmod n=(x_{2i} - y_2 + t_i)^2 \bmod n$ because of $x_{2i} \equiv (pwd-x_{1i}) \bmod n$ and $y_2 \equiv (pwd-y_1) \bmod n$. Therefore, $C \bmod n=2y_1(x_{1i} + t_i) \bmod n$ where $C=((x_{1i}+t_i)^2 \bmod n)+(y_1^2 \bmod n)-(x_{2i}^2 + y_2^2 + t_i^2)+(2x_{2i}y_2+2x_{2i}t_i-2y_2t_i))$. The verifier receive t_i , x_{2i} and $(x_{1i} + t_i)^2 \bmod n$ from the prover and had stored $y_1^2 \bmod n$ and y_2 at the password file, so the verifier can calculates C. Therefore, the verifier permits the prover to access the system resource if $C^2 \bmod n=(4(y_1^2 \bmod n)(x_{1i} + t_i)^2 \bmod n) \bmod n$, because the verifier convinces that the prover inputs pwd.

IV. ANALYSIS OF OPI

In this section, we analysis the security and the performance of OPI.

A. Security

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 in polynomial time [9], and the factoring problem of *n* is NP□complete [10, 11].

Property 1 Let n=*pq*, and two primes *p* and *q* be selected such that n is computationally infeasible to factor. Then, the problem finding *x* in $(x+t)^2$ mod n, for a given *t*, quadratic residue *a* modulo n and n, is NP-complete.

We can easily know 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 special case of the problem finding x in $(x + t)^2$ mod n for a given t, quadratic residue a modulo n. For this reason, we demonstrate that OPI is secure against the attacks, when the security of OPI comes a conclusion of Property 1.

In OPI, there are two secret information x_{1i} and pwd, but the secret information on the unsecured channel and at the verifier is x_{1i}. We will mention how the identification scheme prevents the attacker trying to learn pwd in on line dictionary attack in the following, and we Property 1. Therefore, OPI is secure against pre-play attack[13] for the cases (a) and (b).

In eavesdropping, the attacker listens messages on the line and tries to learn some useful information from the ongoing communication. The hardness to learn useful information x_{1j} from $(x_{1j} + t_j)^2$ mod n depends on Property 1, when the attacker tries to learn x_{1i} at t_i, x_{2i} and $(x_{1i} + t_i)^2$ mod n from t_j , x_{2j} and $(x_{1j} + t_j)^2$ mod n for $1 \leq i$ and $j \leq i$. Therefore, OPI is secure against eavesdropping.

In man-in-the-middle attack[13], the attacker intercepts the message sent between the parties and replaces them with its own message. It plays the role of the prover in the messages which it sends to the server.

The security of OPI against man-in-the-middle attack is same with the security of OPI against eavesdropping, because a number of pass of OPI is one, and the attacker has to decide x_{1j} to replace x_{1i} at t_i, x_{2i} and $(x_{1i} + t_i)^2$ mod n with his own message. Therefore, OPI is secure against the man-in-the-middle attack[13].

In password guessing attacks, the attacker is assumed to have access to a relatively small dictionary containing common choices of passwords. There are primarily two ways in which the attacker can use the dictionary that are on-line dictionary attack and off-line dictionary attack.

In on-line dictionary attack, the attacker repeatedly picks a password from the dictionary and tries to use it in order to impersonate as the user. If the impersonation fails, the attacker eliminates this password from the dictionary and tries again, using a different password. The standard ways of preventing such on line dictionary attack in practice are to either limit the number of failed runs that a user is allowed to have before the password is expired, or reduce the rate in which the user is allowed to make login attempts.

For off-line dictionary attack, the attacker records past communication, and then goes over the dictionary and looks for a password which is consistent with the recorded communication. If such a password is found, the attacker concludes that this is the password of the attack. To be possible off-line dictionary attack to OPI, the attacker has to maintain the dictionary before looking for a password which is consistent with the recorded communication. There are 2^{n-1} possibilities for a pwd, because the prover selects x_{1i} in random and $1 \leq x_{1i} \leq n-1$, and it is impracticable to store 2^{n-1} records, because n is of some size such that n is computationally infeasible to factor. Therefore, OPI is secure against off-line dictionary attack.

Server compromise is possible to identification scheme, if the verifier can impersonate the prover. In OPI, the verifier has stored y_1^2 mod n and y_2, but it is NP-complete problem determining y_1 from y_1^2 mod n. Therefore, OPI is secure against server compromise.

B. Performance

Obviously, OPI satisfies the following facts:

(1)A number of pass of OPI is one. The number of passes is related to the traffic overhead, and the traffic overhead is directly related to whether the identification scheme can be used in commercial; (2) OPI does not need the key. Identification scheme bears another problem if that needs the key. As an example, the identification scheme using confidential key needs techniques for distributing confidential keys. (3) OPI processes the password inputted by the prover. The prover has to store his secret information to all systems used by him, if identification scheme does not process the password.

The prover performs one modular multiplication $(x_{1i}+t_i)^2$ mod n. The verifier performs one modular multiplication to obtain the result of the right term in Equ. 1 in on line state, because the verifier can calculates y_1^2 mod n in off line state and receives $(x_{1i}+t_i)^2$ mod n from the prover. And also, the verifier performs one modular addition to obtain C in Equ. 1 after performing three square multiplication and three multiplications and one

Table 1 Summarization of the number of the operations

Prover	Verifier (off line state)	Verifier (on line state)
modular square multiplication:1	modular square multiplication:1	Square multiplication:3 multiplication:3 modular addition:1 modular square multiplication:1

modular square multiplication to obtain the result of the left term of Equ. 1. We summarize in Table 1 the numbers of the operations performed in OPI.

V. CONCLUSIONS

We have presented a new identification scheme called OPI. The OPI 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 OPI, 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 OPI is one, OPI processes the password and does not use the key. We think that OPI is excellent in the consuming time to verify the prover.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

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

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

[11] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, New York, 1993.

[12] 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. 1790-1795, 2004.

[13] Jong-Min Park, "Efficient and Secure Authenticated Key Exchange", The Korean Institute of Maritime Information & Communication Science, Vol. 3, No. 3, pp. 163-166, 2005.

Byung-Jn Park
He received the Apply Statistics and Ph.D.
degrees in the Dept. of Computer & Statistics from Chosun University.
His research interests in information security, information statistics, quality control, fourier series.

Jong-Min Park
He received the A.I and Ph.D.
degrees in the Dept. of computer Engineering from Chosun University.
His research interests information security, bio metrics, pattern recognition, artificial intelligence.