Efficient and Secure Authenticated Key Exchange

Jong-Min Park, *Member, KIMICS*

Abstract—The Key exchange protocols are very crucial tools to provide the secure communication in the broadband satellite access network. They should be required to satisfy various requirements such as security, Key confirmation, and Key freshness. In this paper, Two authenticated key exchange protocols TPEKE-E(Two Pass Encrypted Key Exchange-Exchange-Efficient) and TPEKE-S(Two Pass Encrypted Key Exchange-Secure) are introduced. A basic idea of the protocols is that a password can be represented by modular addition *N*, and the number of possible modular addition *N* representing the password is 2^N.

The TPEKE-E is secure against the attacks including main-in-the-middle attack and off-line dictionary attack, and the performance is excellent so as beyond to comparison with other authenticated key exchange protocols. The TPEKE-S is a slight modification of the TPEKE-E. The TPEKE-S provides computational in feasibility for learning the password without having performed off line dictionary attack while preserving the performance of the TPEKE-E.

Index Terms—TPEKE-E, TPEKE-S, main-in-the-middle attack, off-line dictionary attack

I. INTRODUCTION

Two entities, who only share a password, and who are communicating over an insecure network, want to authenticate each other and agree on a large session key to be used for protecting their subsequent communication. This is called the password authenticated key exchange problem.

The EKE(Encrypted Key Exchange) protocol was the first password authenticated key exchange protocol [3]. The idea of EKE was to use the password to encrypt the protocol messages of a public key. Then an attacker guessing a password could decrypt the symmetric encryption, but could not break the asymmetric encryption in the messages, and thus could not verify the guess. The EKE became the basis for many of the subsequent works in this area[2, 4, 5, 7-13, 15].

The authenticated key exchange protocol is to be guarded against the attacks such as reply, pre-play attack, eavesdropping, man-in-the-middle attack, partition attack and off line dictionary attack. An attacker may get access to sensitive data which is supposed to be kept secret at the principals. Some of the proposed authenticated key exchange protocols have been broken [14]. Some of the proposed authenticated key exchange protocols were designed to protect against password file compromise, so that an attacker that was able to steal data from a server could not later masquerade as a user without having performed a dictionary attack.

Any proposed protocol required at least three passes and performed modular exponentiation at least twice.

In this paper, we present two authenticated key exchange protocols TPEKE-E(Two Pass Encrypted Key Exchange-Exchange-Efficient) and TPEKE-S(Two Pass Encrypted Key Exchange-Secure). A basic idea of the protocols is that a password can be represented by modular addition *N*, and the number of possible modular addition N representing the password is 2^N.

The TPEKE-E is secure against the attacks such as replay attack, pre-play attack, eavesdropping, man-in-the-middle attack and off-line dictionary attack, but vulnerable to password file comprise. The number of pass of the TPEKE-E is two, and the TPEKE-E does not require modular exponentiation. The TPEKE-S is a slight modification of the TPEKE-E so that to be secure against password file compromise for learning the password without having performed off line dictionary attack while preserving the performance of the TPEKE-E and the security against the attacks guarded in the TPEKE-E.

We describe TPEKE-E in Section III and TPEKE-S Section IV.

II. PRELIMINARIES

A. Notation

Our notation is shown in the following :

A, *B* : System participants.

P : A shared password for *A* and *B*.

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

N, *M* : Positive integer suitable for symmetric key cryptosystem.

R_1, R_2 : Random numbers.

E_k : Symmetric encryption with key *K*.

D_k : Symmetric decryption with key *K*.

H_1, H_2 : One way hash functions.

SK : session key shared between participants after completion of the protocols.

Manuscript received August 29, 2005.

Jong-Min Park is with field school of computer, Dongshin University, Office of Planning 252 Daeho-dong, Naju, Jeonnam, 520-714 Republic of Korea(e-mail : pjm5234@lycos.co.kr)

B. Security of Authenticated Key Exchange

We present a list of basic attacks that authenticated key exchange protocol needs to guard against.

- Replay : The attacker records messages which were sent in past communications and re-sends them at a later time.
- Pre-play : The attacker records messages which were sent in past communications and determines a message from the recorded messages for current communication.
- Eavesdropping : The attacker listens messages on the line and tries to learn some useful information from the ongoing communication.
- Man-in-the-middle : The attacker intercepts the messages sent between the parties and replaces them with its own messages.
- Password guessing attacks : The attacker is assumed to have access to a relatively small dictionary containing common choices of password. there are primarily two ways in which the attacker can use the dictionary that are on-line dictionary attack and off-line dictionary attack.
- 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.
- 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 this reason, in this paper, we consider only off line dictionary attack.
- Password file compromise : The attacker gets access to sensitive data which is supposed to be kept secret at the password file to masquerade as a user.

C. NP-complete

The square root modulo n (SQROOT) problem is to find a square root of a modulo 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 [16], and the factoring problem of n is NP-complete [1, 6].

Property 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.

III. TPEKE-E

The TPEKE-E is describes at Fig. 1.

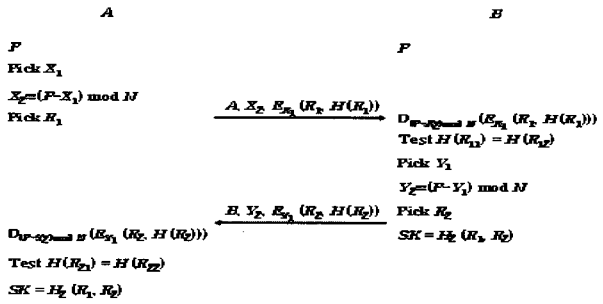

Fig. 1 TPEKE-E protocol

In the TPEKE-E, each participant stores P in clear. A chooses X_1 and R_1 in random ($0 \le X_1 \le N-1$, $0 \le R_1 \le M-1$) and determines X_2 such that $(X_1 + X_2) \bmod N \equiv P$. B can learn X_1 even if he has received only X_2. B accepts A only when $H(R_{11}) = H(R_{12})$ is hold where $(R_{11}, H(R_{12})) = D_{(P-X_2) \bmod N}(E_{X_1}(R_1, H(R_1)))$. Similarly with B, A verifies B. Only the parties recovering R_1 and R_2 should share a session key.

For this reason, we demonstrate that TPEKE-E is secure against the attacks, when the security of TPEKE-E comes a conclusion of Property.

The TPEKE-E is secure against replay attack, because the keys and the messages are chosen in random. Also, the TPEKE-E is secure against pre-play attack, because it is computationally infeasible to produce a message for current communication without learning the keys in past communications. The TPEKE-E is secure against an attacker who tries to lean useful information from the eavesdropped messages, because each key was chosen in random, and the transmitted messages that were used to derive a session key were encrypted by the key. The TPEKE-E is secure against man-in-the middle attack, because it is computationally infeasible to replace the messages sent between the parties to his own messages without learning the keys in past communications. The TPEKE-E is secure against partition attack, because any un-chosen integer can be chosen as a key. The TPEKE-E is secure against off-line dictionary attack, because it is too huge to store all possible candidates for ciphertexts. The TPEKE-E is vulnerable to password file compromise.

Obviously, the performance of the TPEKE-E is excellent so as beyond to comparison with other authenticated key exchange protocols (See Table 1). In Table 1, the random number generator produces one random number, and a part of the random number is used for a key and another part a message.

Table 1 The performance of TPEKE-E

	A	*B*
Pass	1	1
Symmetric key crypto system	2	2
Hash function	3	3
Random number generation	1	1

IV. TPEKE-S

Slight modification of the TPEKE-E makes TPEKE-S that is secure against password file compromise for learning the password without having performed off line dictionary attack. In the TPEKE-S, A chooses X_1 and determines X_2 such that (X_1+X_2) mod N≡P, and then stores $(X_1^2+2X_1X_2)$ mod N and X_2^2. Similarly, B chooses Y_1 and determines Y_2 such that (Y_1+Y_2) mod N≡P, and then stores $(Y_1^2+2Y_1Y_2)$ mod N and Y_2^2. The TPEKE-S is described in Fig. 2.

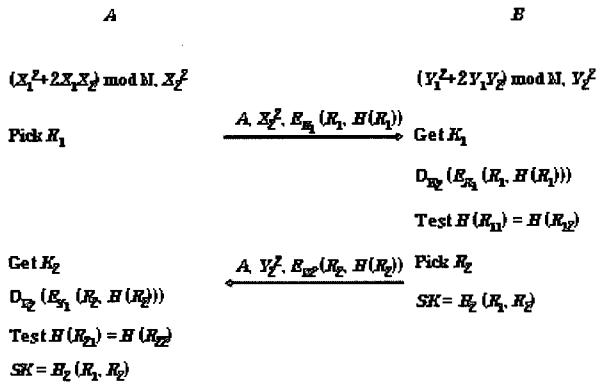

Fig. 2 TPEKE-S protocol

In the TPEKE-S, K_1 is $(X_1^2+2X_1X_2)$ mod N and K_2 is $(Y_1^2+2Y_1Y_2)$ mod N. B gets K_1 by using the fact that $(X_1+X_2)^2$ mod N≡ $(Y_1+Y_2)^2$ mod N, and then tests whether $H(R_{11})$=$H(R_{12})$ is hold or not where (R_{11}, $H(R_{12}) = D_{K_1}(E_{K1}(R_1, H(R_1)))$. Similarly with B, A verifies B.

The TPEKE-S is secure against attacks such as replay, pre-play, eavesdropping, man-in-the- middle and off line dictionary attack. The TPEKE-S is secure against the partition attack, because any un-chosen integer can be chosen as a message even if one key is used repeatedly.

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 a special case of the problem finding x in $(x+t)^2$ mod n for a given t, quadratic residue a modulo n and n.

The attacker may get access to sensitive data which is supposed to be kept secret at the password file. From the property mentioned, the TPEKE-S provides computational in feasibility to determine the password without having performed off line dictionary attack even if the password file is compromised.

Table 1 is also the performance of the TPEKE-S.

V. CONCLUSIONS

We have presented two authenticated key exchange protocols called TPEKE-E and TPEKE-S. A basic idea of the protocols was that a password can be represented by modular addition N, and the number of possible modular addition N representing the password is 2^N.

The TPEKE-E explains our idea suitably and is secure against attacks including off line dictionary attack, the performance of the TPEKE-E was excellent so as beyond to comparison with other authenticated key exchange protocols.

The TPEKE-S is a slight modification of the TPEKE-E, and the TPEKE-S provides computational in feasibility for learning the password without having performed off line dictionary attack while preserving the performance of the TPEKE-E and the security against the attacks guarded in the TPEKE-E. The performance of the TPEKE-S is equal to that of the TPEKE-E.

REFERENCES

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

[2] M. Bellare, D. Pointcheaval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks", Advances in Cryptology Eurocrypt'00, LNCS Vol. 1807, Springer-Verlag, pp. 139-155, 2000.

[3] S. M. Bellovin and M. Merrit, "Encrypted key exchange : Password-based protocols secure against dictionary attack", In Proceedings of IEEE Security and Privacy, pp. 72-84, 1992.

[4] S. M. Bellovin and M. Merrit, "Augmented encrypted key exchange : Password-based protocol secure against dictionary attack and password file compromise", In ACM Security (CCS'93), pp. 244. 250, 1993.

[5] V. Boyko, P. MacKenzie, and S. Prenel, "Probably secure password authenticated key exchange using Diffie-Hellman", In B. Prenel, editor, Advances in Cryptology Eurocrypt'00, LNCS Vol. 1807, Springer -Verlag, pp. 156-171, 2000.

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

[7] O. Goldreich and Y. Lindell, "Session key generation using heman passwords only", Advances in Cryptology, Crypto'01, LNCS Vol. 2137, S[romger-Verlag, pp. 408-432, 2001.

[8] L. Gong, "Optimal authentication protocols resistant to password guessing attacks", In 8th IEEE Computer Security Foundations Workshop, pp. 24-29, 1995.

[9] L. Gong, T. M. A. Lomas, R. M. Needham, and J. H. Saltzer, "Protecting poorly chosen secrets from guessing attacks", IEEE Journal on Selected Areas in Communications, 11(5), pp. 648-656, June 1993.

[10] D. Jablon, "Strong password-only authenticated key exchange", ACM Computer Communication Review, ACM SIGCOMM, Vol. 26, No. 5, pp. 5-20, October 1996.

[11] J. Katz, R. Ostrovsky, and M. Yung, "Efficient password authenticated key exchange using human memorable passwords", Advances in Cryptology Eurocrypt'01, LNCS Vol. 2045, Springer-Verlag, pp. 475-494, 2001.

[12] S. Lucks, "Open key exchange : How to defeat dictionary attacks without encrypting public keys", In Proceedings of the Workshop on Security Protocols, 1997.
[13] P. MacKenzie, S. Patal and S. Swaminathan, "Password authenticated key exchangebased on RSA", Advances in Cryptology Asiacrypt'00, LNCS Vol. 1976, Springer-Verlag, pp. 599-613, 2000.
[14] S. Patal, "Number theoretic attacks on secure password schemes", In proceedings of IEEE Security and Privacy, pp. 236-247, 1997.
[15] M. Steiner, G. Tsudik, and M. Waidner, "Refinement and extension of encrypted key exchange", ACM Operating System Review, 29, pp. 22-30, 1995.
[16] H. Woll, "Reductions among number theoretic problems, Information and Computation, Vol. 72, pp. 167-179, 1987.

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.