Cryptanalysis of A One-Time Password Authentication Protocol

Wei-Chi Ku and Chien-Ming Chen
Department of Computer Science and Information Engineering
Fu Jen Catholic University
TEL: (886) 2-29031111~3894
E-mail: wcku@csie.fju.edu.tw, ie865144@csie.fju.edu.tw

Abstract

Recently, Sandirigama *et al.* propose a simple one-time password authentication protocol, SAS, which is intended to be superior to other similar protocols in the aspects of security and efficiency. In this paper, we show that the SAS protocol is still vulnerable to the modification attack. Then, an improved version of the SAS protocol is described.

Key words: password, authentication, security, modification attacks, hash function.

I. Introduction

In most information systems, the identities of part of all of the involved entities should be verified ahead of other operations can be performed. Although such an authentication problem is an old security issue, the researches on developing simple and secure authentication methods never stop. Up to now, password authentication is still regarded as one of the simplest and the most convenient authentication methods [1][2][4][5][7]. Conventional static password authentication methods are not suitable for open network environments because the adversary can easily obtain the bare password by wiretapping the communications between the user (prover) and the host (verifier) and then to impersonate the prover. To solve this problem, Lamport [3][6] proposed a one-time password authentication protocol based on cryptographic hash functions. However, high hash overhead and the necessity for password resetting decrease its suitability for practical use.

To eliminate the drawbacks of Lamport's protocol, Shimizu [9][10] proposed a one-time password authentication protocol, CINON protocol. The one time characteristic is gained by using two variable random numbers that are changed at each authentication. However, the prover has to either memorize two variable random numbers or carry with some sort of portable storage tokens, e.g., floppy disk or IC card. This inconvenience obstructs the deployment of the CINON protocol.

Next, Shimizu *et al.* [11] proposed a token-free one-time password authentication protocol, PERM protocol. The prover doesn't need to either memorize any random number or carry with a portable storage token; instead, a random number is stored in the verifier for authenticating the prover. During each authentication, this random number is sent from the verifier to the prover. It is only when the verifier receives the correct reply corresponding to the sent random number he will believe that the prover is authentic and refresh the stored random number. Un-

fortunately, PERM protocol is subject to the *man-in-the-middle attack* [8][11] in that the adversary can impersonate the prover by modifying two consecutive sessions between the prover and the verifier.

Recently, Sandirigama *et al.* [8] propose a simple one-time password authentication protocol, SAS protocol, which can defeat the man-in-the-middle attack exist in the PERM protocol. In addition, SAS protocol is superior to Lamport's protocol, the CINON protocol, and the PERM protocol in the aspects of storage utilization, processing time, and transmission overhead. However, we find that the SAS protocol is still vulnerable to the modification attack. In the rest of this paper, we will first briefly describe the SAS protocol, and then address its security flaw. Finally, an improved version of SAS protocol will be described.

II. Cryptanalysis of SAS Protocol

First, we briefly describe the notation used to express the SAS protocol as in the following:

- P denotes the prover who is authenticated by the verifier V.
- ID_P and S_P represent the identity and password of P, respectively.
- E denotes a cryptographic hash function. $E(X)$ means X is hashed once, and $E^2(X)$ means X is hashed twice.
- N_n represents a random number corresponding to nth authentication.
- $\oplus$ denotes the bitwise XOR operation.
- $||$ denotes the concatenation.
- The expression '$A \rightarrow B$: X' represents that A sends X to B through a common channel.
- The expression '$A \Rightarrow B$: X' represents that A sends X to B through a secure channel.

A. Protocol Description

The SAS protocol has two phases, the registration phase and the authentication phase. The registration phase is invoked only once for registering each prover while the authentication phase is invoked whenever the prover authenticates himself to the verifier. These two phases can be described as in the following:

Registration Phase

Step R1. P: calculates $E^2(S_P||N_0)$.

Step R2. $P \Rightarrow V$: ID_P, $E^2(S_P||N_0)$, N_0.

Step R3. V: stores ID_P, $E^2(S_P||N_0)$, N_0.

Authentication Phase

Step A1. $P \rightarrow V$: service request.

Step A2. $V \rightarrow P$: N_0.

Step A3. $P \rightarrow V$: x_1, x_2, N_1,

where

$x_1 = E(S_P||N_0) \oplus E^2(S_P||N_0)$, and

$x_2 = E^2(S_P||N_1) \oplus E^2(S_P||N_0)$.

Note that x_1 is used for the current authentication session, and x_2 and N_1, which is the random number generated by P, will be used for next authentication session.

Step A4. V: Retrieves the stored $E^2(S_P||N_0)$ to compute $y_1 = x_1 \oplus E^2(S_P||N_0)$ and $y_2 = x \oplus E^2(S_P||N_0)$.

Step A5. V:

(1) Computes $E(y_1)$, and then compares the result with the stored $E^2(S_P||N_0)$. If they are equal, V believes that P is authentic; otherwise, V rejects P and terminates the protocol.

(2) Replaces $E^2(S_P||N_0)$ and N_0 with y_2 and N_1 for next authentication session.

B. Protocol Cryptanalysis

We show that SAS protocol is subject to the *modification attack* as in the following:

Upon seeing x_1, x_2, and N_1 sent by P in Step A3, the adversary can replace x_2 with an equal-sized random string, say x_2'. In Step A4, V retrieves the stored $E^2(S_P||N_0)$ to compute the following two terms:

$$y_1 = x_1 \oplus E^2(S_P||N_0)$$

$$y_2' = x_2' \oplus E^2(S_P||N_0).$$

Since the equation $y_1^2 = E^2(S_P||N_0)$ holds, V will believe that P is authentic and then replaces $E^2(S_P||N_0)$ and N_0 with y_2' and N_1 for next authentication session. Clearly, P has been successfully authenticated in current session, but he will be rejected in future authentication sessions. Although the adversary cannot find a string z satisfying $E(z) = y_2'$ for impersonating P in next authentication session, he can still fool V into believing this wrong y_2', i.e., he can easily prevent P from successful authentication in the future.

On the other hand, if the adversary replaces N_1 in Step A3 with an equal-sized string, say N_1', V will also believe that P is authentic, and then replace $E^2(S_P||N_0)$ and N_0 with y_2 and N_1' for next authentication session. Because the y_2 and N_1' stored in V are inconsistent, P will be rejected in next authentication session. Although the adversary cannot find a string z satisfying $E(z) = y_2$ for impersonating P in the next authentication session, the authentication request from P will still be denied.

III. An Improved Version of SAS Protocol

We now describe an improved version of the SAS protocol, which is abbreviated as ISAS protocol. In the ISAS protocol, the authentication steps are partly modified while the registration steps are left unchanged. The weakness of SAS protocol is due to the lack of integrity protection for the data that is to be used in next authentication session. That is, the verifier V cannot judge the correctness of $E^2(S_P||N_1)$ and N_1 from the messages received in Step A3 of the SAS protocol. In the ISAS, this problem will be solved. The notation used in the ISAS protocol is directly adopted from the SAS protocol.

A. Protocol Description

The registration phase is the same as the one in SAS protocol [8] while the authentication phase is modified as in the following:

Authentication Phase

Steps A1 and A2 are left unchanged.

Step A3. $P \rightarrow V$: x_1, x_2, x_3, N_1,

where

$x_1 = E(S_P||N_0) \oplus E^2(S_P||N_0)$,

$x_2 = E^2(S_P||N_1) \oplus E^2(S_P||N_0)$,

$x_3 = E(E(S_P||N_0)||E^2(S_P||N_1)||N_1)$.

Note that x_1 is used for the current authentication session while x_2, x_3, and N_1 are used for the next authentication session.

Step A4. V: Retrieves the stored $E^2(S_P||N_0)$ to compute $y_1 = x_1 \oplus E^2(S_P||N_0)$ and $y_2 = x \oplus E^2(S_P||N_0)$.

Step A5. V:

(1) Computes $E(y_1)$, and then compares the result with

the stored $E^2(S_P||N_0)$. If they don't match, V rejects P and terminates the protocol.

(2) Computes $E(y_1||y_2||N_1)$, and then compares the result with the received x_3. If they match, V believes that P is authentic; otherwise, V rejects P and terminates the protocol.

(3) Replaces $E^2(S_P||N_0)$ and N_0 with y_2, which should be $E^2(S_P||N_1)$, and N_1 for the next authentication session.

B. Protocol Cryptanalysis

In the ISAS protocol, we use $x_3 = E(E(S_P||N_0)||E^2(S_P||N_1)||N_1)$ to protect the integrity of x_2 and N_1 transmitted in Step A3. To fool V into believing the bogus x_2', the adversary also has to replace the transmitted x_3 with

$$x_3'=E(E(S_P||N_0)||(x_2' \oplus E^2(S_P||N_0))||N_1).$$

However, since the adversary doesn't know $E(S_P||N_0)$ and $E^2(S_P||N_0)$, x_3' cannot be forged unless the employed hash function E is broken, a contradiction to our assumption. Hence, the improved protocol can resist the modification attack. Furthermore, since we only add integrity protection to the SAS protocol while the remaining parts are left unchanged, other security features of the ISAS protocol are directly inherited from the original SAS protocol.

IV. Conclusions

In this paper, we have addressed the weakness of a newly proposed one-time password authentication protocol, the SAS protocol [8]. In addition, an improved version of it, the ISAS protocol, has been described. The ISAS protocol can resist the modification attack exist in the original SAS protocol at the cost of transmitting one more hashed message. For each authentication, the numbers of hash operations performed by the prover and the verifier are two and five, respectively. Hence, the hash overhead of the ISAS protocol is the same as that of another two similar one-time password authentication protocols, the CINON protocol [9][10] and the PERM protocol [11]. However, the ISAS protocol doesn't require that the prover should either memorize random numbers or carry with a portable storage token. Furthermore, the ISAS protocol can defeat the man-in-the-middle attack, which makes the PERM protocol infeasible for practical use.

Acknowledgement

This research was supported by the National Science Council, Republic of China, under Grant NSC-90-2213-E-030-016.

Reference

[1] S. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks", *IEEE Symposium on Research in Security and Privacy*, pp.72-84, 1992.

[2] S. Bellovin and M. Merritt, "Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password-file compromise", *ACM Conference on Computer and Communications Security*, pp.244-250, 1993.

[3] N. Haller, "The S/KEY (TM) one-time password system", *Proc. Internet Society*

symposium on Network and Distributed System Security, pp.151-158, 1994.

[4] D. Jablon, "Strong password-only authenticated key exchange", *ACM Computer Commun. Review*, vol.26, no.5, pp.5-26, 1996.

[5] T. Kwon, "Ultimate Solution to Authentication via Memorable Password", *A proposal for IEEE P1363a: Password-based authentication*, May 2000.

[6] L. Lamport, "Password authentication with insecure communication", *Commun. ACM*, vol.24, no.11, pp.770-772, 1981.

[7] M. Lomas, L. Gong, J. Saltzer, and R. Needham, "Reducing risks from poorly chosen keys", *ACM Symposium on Operating System Principles*, *ACM Operating Systems Review*, pp.14-18, 1989.

[8] M. Sandirigama, A. Shimizu, "Simple and secure password authentication protocol (SAS)", *IEICE Trans. Commun.*, vol.E83-B, no.6, pp1363-1365, June 2000.

[9] A. Shimizu, "A dynamic password authentication method by one-way function", *IEICE Trans.*, vol.J73-D-I, no.7, pp.630-636, July 1990.

[10] A. Shimizu, "A dynamic password authentication method by one-way function", *System and Computers in Japan*, vol.22, no.7, 1991.

[11] A. Shimizu, T. Horioka and H. Inagaki, "A password authentication method for contents communication on the internet", *IEICE Trans. Commun.*, vol.E81-B, no.8, pp.1666-1763, Aug.1998.