A new efficient authentication scheme for Session Initiation Protocol

Hui-Feng Huang[1] and Wei-Chen Wei[2]

[1]Department of Information Management
National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.
E-mail:phoenix@ntit.edu.tw
[2]Institute of Computer Science and Information Technology
National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.
E-mail: s18943111@ntit.edu.tw

Abstract

Today, the efficiency and security of session initiation protocol is becoming more and more important. In 2005, Yang et al. proposed a secure authentication scheme for session initiation protocol. However, it is not suitable for the limited computation capacities of users such as smart cards or mobile units. To guarantee the quality of the growing communication services, we propose an efficient authentication scheme for session initiation protocol. In our scheme, only seven hash functions are performed in the procedure. It is efficient and convenient for both the hardware-limited users and the authentication server.

Keywords: Authentication, Session initiation protocol

1. Introduction

Computer networks have had widespread applications in recent years. To prevent information and communication systems from illegal delivery and modification, message privacy and authentication need to be examined through some of the certificated mechanisms.

Recently, the Internet Engineering Task Force (IETF) proposed the Session Initiation Protocol (SIP) as the IP-based telephony protocol [1,2]. The SIP provides an expandable and easy conquest to the surrounding IP-based telephony. SIP is based on the application-layer and is a text-based client—server protocol. The architecture of SIP consists of a proxy server, redirect server, user agent, register server, and location server. We briefly depict each of the components as follows [1,2].

- **Proxy server:**

A proxy server forwards a request and response between a callee and a caller. When the proxy server receives a request, it sends the request to the current location of the callee, and then forwards the response from the callee to the caller.

- **Redirect server:**

When a redirect server receives a request, it informs the caller about the current location of the callee. Then the caller contacts the callee directly.

- **User agent:**

A user agent is a logical entity, such as a callee or a caller.

- **Register server:**

The register server helps the user agent update the information of the user agent's location in the location server.

- **Location server:**

The responsibility of the location server is to maintain information on the current location of the user agent. It provides the proxy server, redirect server, and register server for them to look up or register the location of the user agent.

The security of SIP is becoming more and more important in today's computer environment [3,4,5,7,8,9]. When a user requests to use an SIP service, he needs to be authenticated first before getting the service from the server. Similarly, the user also has to verify the identity of the server. For example, if the user does not verify the identity of the server, an attacker can forge the identity of the server to obtain some secret information of the user. However, the previous SIP authenticated schemes were proposed by Handley (1999) [1], Rosenberg (2002) [2], and Veltri et al. (2002) [5] are not secure [10]. In 2005, based on Diffe-Hellman [6], Yang et al. proposed a secure authentication scheme for session initiation protocol [10]. In their procedure, four modular exponentiations are computed for the server and user. It is not suitable for the limited computation capacities of users such as smart cards or mobile units. To guarantee the quality of the growing communication services, it is necessary to reduce the computation load for both parties of the server and client. Therefore, we propose an efficient authentication scheme for session initiation protocol.

In total, only seven hash functions are required for our protocol. It is very efficient for both the user and the authentication server. In addition, the procedure of our SIP scheme is quite simple. So, the simplicity and low-computation properties make our scheme very suitable for smart cards and mobile users.

The remainder of this paper is organized as follows. In the next section, we present a new authentication scheme for session initiation protocol. The security analyses and the performances of our scheme are discussed in Section 3. And some conclusions will be made in the last section.

2. The Proposed Scheme

In this section, we will present a new efficient and secure SIP authentication procedure using a one-way function. Assume that two communication parties, the client and the server share common information $F(PW)$ before the protocol begins, where $F(\ )$ is a public one-way hash function and PW is a password of the client. When a user logs in on the server, the procedure of our SIP authentication processes are described as follows.

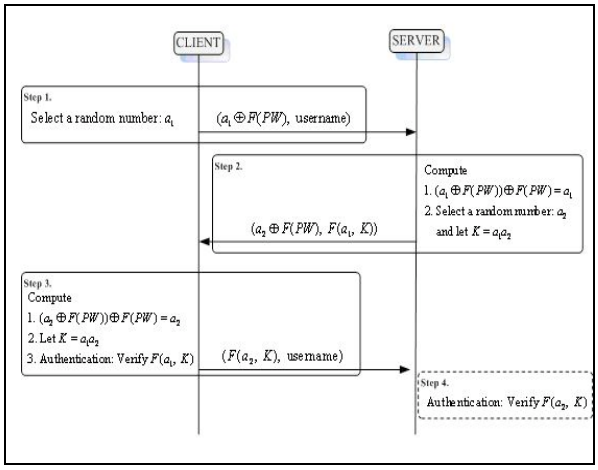

Fig. 1: SIP authentication processes

Step 1. client→server:

The user randomly selects a secret integer a_1, and then sends $a_1 \oplus F(PW)$ and a username to the server, where $F(\ )$ is a one-way hash function and $\oplus$ signifies the XOR operation.

Step 2. server→client:

After receiving the $a_1 \oplus F(PW)$ and username from the user, the server obtains a_1 by computing $F(PW) \oplus (a_1 \oplus F(PW))$. Next, the server selects a random secret number a_2 and computes $K = a_1 a_2$. Then, the server sends $a_2 \oplus F(PW)$ and $F(a_1, K)$ to the user.

Step 3. client→server:

The user computes $(a_2 \oplus F(PW)) \oplus F(PW)$ to obtain a_2, and then gets $K = a_1 a_2$. Eventually, the user verified the identity of the server by computing $F(a_1, K)$. If $F(a_1, K)$ is true, then the user delivers $F(a_2, K)$ to the server.

Step 4. Authentication: The server authenticates the identity of the user by means of $F(a_2, K)$.

After receiving the $F(a_2, K)$ from the user, the server computes and verifies $F(a_2, K)$. If $F(a_2, K)$ is true, the server authenticates the identity of the user, where $K = a_1 a_2$. Moreover, K could be used as this session key for two communication parties and maintains important information. The above processes are briefly illustrated in Figure 1.

3. Discussions

In this section, we are going to explore the securities and the performances of our scheme.

3.1. Security Analysis

The security of the presented scheme is based on the one-way hash function. According to the one-way specialty of a hash function, the presented scheme can withstand the following three attacks.

- **Replay attack**

Supposing that an adversary replays $(a_1 \oplus F(PW))$ to the server, and then the server delivers $(a_2 \oplus F(PW),\ F(a_1, K))$ back. However, the adversary doesn't know $F(PW)$ and he cannot derive a_2 by computing $(a_2 \oplus F(PW)) \oplus F(PW)$ and send $F(a_2, K)$ to the server in step 3. Therefore, the proposed scheme can withstand the replay attack.

- **Masquerade attack**

Without knowing $F(PW)$, the adversary cannot derive a_1 and a_2 from Step 1 and Step 2, respectively. In addition, from the information $a_1 \oplus F(PW)$ and $a_2 \oplus F(PW)$, the adversary can get $a_1 \oplus a_2$ by computing $(a_1 \oplus F(PW)) \oplus (a_2 \oplus F(PW))$. With $a_1 \oplus a_2$, he also obtains nothing about a_1 and a_2. Thus, the adversary could not masquerade as the identity of the client and the server. Therefore, the proposed scheme can withstand the masquerade attack.

- **Password guessing attack**

Supposing that an adversary obtains the messages $(a_1 \oplus F(PW),$ username$)$, $(a_2 \oplus F(PW),\ F(a_1, K))$, and $(F(a_2, K),$ username$)$ from steps 1, 2, and 3. To implement the password guessing attack, an adversary first guesses a password PW', and computes $F(PW')$, and then he tries to compute $F(PW') \oplus (a_1 \oplus F(PW)) = a_1'$, $F(PW') \oplus (a_2 \oplus F(PW)) = a_2'$ and $K' = a_1' a_2'$. If $F(a_1', K') = F(a_1,$ K$)$ and $F(a_2', K') = F(a_2,$ K$)$,

then the adversary guesses the correct password. However, he should do an exhausted search for guessing the password. Thus, the proposed scheme can also withstand the password guessing attack.

3.2. Performances and Comparisons

Yang et al.'s scheme pointed out that the procedure of previous SIP authentication schemes are not secure [10]. For this reason, we only compare the computational complexity of our scheme with Yang et al.'s scheme. As shown in Table 1, our scheme is more efficient than Yang et al.'s scheme. Only seven hash functions and four exclusive operations are performed for the procedure. It is obvious that the proposed scheme can reduce many computations and communications for both the server and client. However, Yang et al.'s scheme requires to four modular exponentiations, and ten amounts of transmitted data. Thus, our scheme is more efficient than Yang et al.'s scheme.

Table 1: Comparisons of Yang et al.'s scheme and the proposed scheme

	Yang et al.'s scheme	The proposed scheme
Exponentiation	4	0
One-way hash function	7	7
Exclusive or	4	4
The amount of transmissions	10	5

4. Conclusions

In this paper, we have proposed a new SIP scheme by using a public one-way hash function for the authentication procedure. By comparison, our method is not only more efficient but also requires less communication. Furthermore, because of the simplicity and low-computation properties, our scheme is very suitable for smart cards or mobile wireless users.

5. References

[1] Handley M, et al. "SIP: session initiation protocol," *IETF RFC2543*, March, 1999.

[2] Rosenberg J, et al. "SIP: session initiation protocol," *IETF RFC3261*, June, 2002.

[3] Thomas M, "SIP security requirements," *IETF Internet draft* (draft-thomas-sip-sec-reg-00.txt), November, 2001 (work in progress).

[4] Arkko J, et al. "Security mechanism agreement for SIP sessions," *IETF Internet draft* (draft-ietf-sip-sec-agree-04.txt), June, 2002.

[5] Veltri L, Salsano S, and Papalilo D, "SIP security issues: the SIP authentication procedure and its processing load," *IEEE Network,* Vol. 16, pp. 38-44, 2002.

[6] Diffe Whitfield and Hellman M, "New directions in cryptology," *IEEE Transaction on Information Theory*, Vol. 22, pp. 644-654, 1976.

[7] Amit K Awasthi, "On the Authentication of the User from the Remote Autonomous Object," *International Journal of Network Security*, Vol. 1, No. 3, pp. 166-167, 2005.

[8] Min-Shiang Hwang and Chi-Yu Liu, "Authenticated Encryption Schemes: Current Status and Key Issues," *International Journal of Network Security*, Vol. 1, No. 2, pp. 61-73, 2005.

[9] Hsien-Chu Wu, Chi-Yu Liu, and Shu-Fen Chiou, "Cryptanalysis of a Secure One-time Password Authentication Scheme with Low-communication for Mobile Communications," *International Journal of Network Security*, Vol. 1, No. 2, 2005, pp. 74-76

[10] C.C. Yang, R.C. Wang, and W.T. Liu, "Secure Authentication Scheme for Session Initiation Protocol," *Computers & Security*, Vol. 24, August, pp. 381-386, 2005.