# Huang-Wei의 키 교환 및 인증 방식에 대한 사전공격

## Dictionary Attack on Huang-Wei's Key Exchange and Authentication Scheme

김 미 진* 남 정 현** 원 동 호***
Mijin Kim Junghyun Nam Dongho Won

**요 약**

SIP(Session Initiation Protocol)는 인터넷상에서 멀티미디어 세션을 시작하고 컨트롤하기 위한 응용계층 프로토콜이다. SIP 서비스를 사용하기 위해 클라이언트는 서버로부터 우선 사용자 인증을 받아야 한다. 일반적으로 인증이란 통신 상대방이 제공하는 네트워크 서비스에 접근하기 위해 자신의 신원을 검증받는 과정을 말한다. 2005년, Yang 등은 SIP 응용을 목적으로 Diffie-Hellman 프로토콜에 기반한 키 교환 및 인증 방식을 제안하였다. 그러나 Yang 등이 제안한 방식은 상당한 양의 계산을 필요로 하기 때문에 계산능력이 떨어지는 클라이언트나 서버로 구성된 네트워크 환경에서 사용하기에는 부적합하다는 단점을 가지고 있다. 이에 Huang과 Wei는 최근 Yang 등이 제안한 방식을 개선하여 효율성을 증대시킨 새로운 키 교환 및 인증 방식을 제안하고 이의 안전성을 주장하였다. 하지만 본 논문에서는 Huang-Wei가 제안한 키 교환 및 인증 방식이 사전공격과 전방향 비밀성에 취약함을 보인다.

**Abstract**

Session initiation protocol (SIP) is an application-layer protocol to initiate and control multimedia client sessions. When clients ask to use a SIP service, they need to be authenticated in order to get service from the server. Authentication in a SIP application is the process in which a client agent presents credentials to another SIP element to establish a session or be granted access to the network service. In 2005, Yang et al. proposed a key exchange and authentication scheme for use in SIP applications, which is based on the Diffie-Hellman protocol. But, Yang et al.'s scheme is not suitable for the hardware-limited clients and servers, since it requires the protocol participants to perform significant amount of computations (i.e., four modular exponentiations). Based on this observation, Huang and Wei have recently proposed a new efficient key exchange and authentication scheme that improves on Yang et al.'s scheme. As for security, Huang and Wei claimed, among others, that their scheme is resistant to offline dictionary attacks. However, the claim turned out to be untrue. In this paper, we show that Huang and Wei's key exchange and authentication scheme is vulnerable to an offline dictionary attack and forward secrecy.

keyword : Session Initiation Protocol, Authentication, Key Exchange, Dictionary Attack, Forward Secrecy

## 1. Introduction

The Session Initiation Protocol (SIP) is an Internet Engineering Task Force (IETF) standard protocol for initiating an interactive client session that involves multimedia elements such as video, voice, chat, gaming, and Internet telephony calls, and modifying or terminating them [1, 2]. SIP supports name mapping and redirection services, so it makes it possible for clients to initiate and receive communications and services from any location, and for networks to identify the clients wherever they are. SIP is a challenge-response protocol, dealing with requests from clients and responses from servers. Protocol participants are identified by SIP URLs. Requests can be sent through any transport protocol, such as UDP, SCTP, or TCP. SIP determines the end system to be used

* 정 회 원 : 성균관대학교 정보통신공학부 박사과정
mjkim@securuty.re.kr
** 정 회 원 : 건국대학교 컴퓨터응용과학부 교수
jhnam@kku.ac.kr
*** 정 회 원 : 성균관대학교 정보통신공학부 교수
dhwon@security.re.kr
[2007/08/27 투고 - 2007/09/04 심사 - 2007/12/12 심사완료]

for the session, the communication media and media parameters, and the called party's desire to engage in the communication. Once these are assured, SIP establishes call parameters at either end of the communication, and handles call transfer and termination. It was originally designed by Henning Schulzrinne (Columbia University) and Mark Handley (UCL) starting 1996. In November 2000, SIP was accepted as a 3GPP signaling protocol for Voice over IP.

Security is an important consideration for SIP, as it is imperative to protect the communication from being eavesdropped, tampered in an open environment, such as the Internet. The SIP protocol concerns with various aspects of security: authentication, confidentiality and integrity. Authentication in a SIP network is the process in which a client agent presents credentials to another SIP element, e.g. a SIP server or other client agent, in order to establish a session or be granted access to the network service [2].

In 2005, Yang et al. [3] proposed a key exchange and authentication scheme for SIP. Yang et al.'s scheme is based on the Diffie-Hellman protocol [4], which bases its security on the difficulty of discrete logarithms. As for efficiency, the scheme requires the participants to perform four modular exponentiations. Thus, Yang et al.'s scheme is not suitable for the hardware-limited clients and the authentication server. 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. Based on this observation, Huang and Wei [5] have recently proposed a new, efficient authentication scheme for SIP. Huang and Wei's scheme is quite simple and requires only seven hash-function evaluations for the server and the client. Despite its efficiency, it turned out that the Huang-Wei scheme is not secure enough. In this paper we show that the Huang-Wei scheme is vulnerable to an offline dictionary attack and forward secrecy.

This paper is organized as follows: Section 2 describes Huang and Wei's key exchange and authentication scheme for SIP. Section 3.1 presents an offline dictionary attack and Section 3.2 shows a lack of forward secrecy on the Huang-Wei scheme. Finally, Section 4 concludes this work.

## 2. Review of Huang-Wei's Scheme

In order to facilitate future references, frequently used notations are listed below with their descriptions.

- S : the server
- C : the client
- I : an attacker
- ID : C's distinct identity
- PW : C's password
- H : a public one-way hash function
- K : session key
- $\oplus$ : the exclusive-or operation

Assume that two communication parties, the client C and the server S share common information $H(PW)$ before the protocol begins. When the client logs on to the server, Huang and Wei's key exchange and authentication scheme for SIP is described as follows.

**Step 1.** C $\rightarrow$ S : $< a_1 \oplus H(PW), ID >$

The client C selects a random secret number $a_1$, and then sends $a_1 \oplus H(PW)$ and ID to the server S.

**Step 2.** S $\rightarrow$ C : $< a_2 \oplus H(PW), \alpha_s >$

After receiving the $a_1 \oplus H(PW)$ and ID from C, S obtains $a_1$ by computing $(a_1 \oplus H(PW)) \oplus H(PW)$. Next S selects a random secret number $a_2$ and computes $K = a_1 a_2$. Then, S sends $a_2 \oplus H(PW)$ and $\alpha_s = H(a_1, K)$ to C.

**Step 3.** C → S : $< \beta_c , ID >$

C obtains $a_2$ by computing $(a_2 \oplus H(PW)) \oplus H(PW)$, and then gets $K = a_1 a_2$. Eventually, C computes $\alpha_c = H(a_1, K)$ and verifies that $\alpha_c$ is equal to $\alpha_s$. If the verification succeeds, then C sends $\beta_c = H(a_2, K)$ to S.

**Step 4.** S authenticates the identity of C using $\beta_c$. After receiving $\beta_c$ from C, S first computes $\beta_s = H(a_2, K)$ and then verifies that $\beta_s$ is equal to $\beta_c$. If the verification succeeds, S gives C permission to access the resource of S. Moreover, S and C share the common secret session key $K = a_1 a_2$ for securing subsequent communications.

In Huang-Wei's scheme given above, only seven hash-function evaluations and four exclusive-or operations are performed for the procedure. In addition, the procedure of the scheme is quite simple. So, the simplicity and low-computation properties make the scheme very suitable for both the hardware-limited clients and the authentication server.

# 3. Security Analysis

## 3.1 Dictionary Attack

In password authentication schemes that the client is allowed to choose its password, the client tends to choose a password that can be easily remembered for its convenience. These easy-to-remember passwords are vulnerable to dictionary attacks, in which an attacker attempts to find out a real password by repeatedly making a guess for the password and verifying the correctness of the guess. In general, the dictionary attacks can be classified into two types: online dictionary attacks and offline dictionary attacks. In online dictionary attacks, an attacker attempts to use a guessed password in an online transaction and tries to verify the correctness of its guess using the response from the server. While in offline dictionary attacks, the attacker intercepts communication messages during an honest protocol execution and stores them locally, and then iteratively makes a guess for the client's password and verifies whether the guess is correct or not in an offline manner. Online dictionary attacks can be easily eliminated by limiting the number of continuous login attempts. But, in an offline dictionary attack, since there is no need for server to participate in the verification, the server cannot easily recognize the existence of the attacker.

As mentioned in the Introduction, we found that Huang-Wei's scheme suffers from an offline dictionary attack. The attack proceeds as follows:

1. In the first step of Huang-Wei's scheme, a client C sends $< a_1 \oplus H(PW), ID >$ to the server S and in the second step S sends $< a_2 \oplus H(PW), H(a_1, K) >$ to C. But, an attacker $I$ eavesdrops these messages.

2. Let

$$c_1 = a_1 \oplus H(PW),$$

$$c_2 = a_2 \oplus H(PW),$$
$$c_3 = H(a_1, K).$$

Then $I$ makes a guess $PW'$ for the password $PW$ and computes:

$$a'_1 = c_1 \oplus H(PW'),$$
$$a'_2 = c_2 \oplus H(PW').$$

After that, the attacker $I$ computes:

$$K' = a'_1 a'_2 \text{ and } c'_3 = H(a'_1, K').$$

3. If $c'_3$ is equivalent to $c_3$, then $I$ gets the correct password $PW(= PW')$. If not, $I$ repeats the above process until it ends up with the correct password.

General clients, when permitted to choose their own password, pick one that is absurdly short. The results of one study at Purdue University observed almost 3% of the passwords were three characters or fewer in length and 85% of the passwords were between six characters and eight characters [6]. When the passwords were eight alphanumeric (not case-sensitive) characters, there are $36^8$ choices choosing a password. If the system performs hundred-million calculations per second, it might take few hours to recover the password by dictionary attack [7]. Therefore, once the attacker has obtained the client's password, he could access the legal server impersonating the client.

### 3.2 Forward Secrecy

The forward secrecy property says that earlier session keys are protected against loss of some underlying information at the present time. The Huang-Wei scheme does not provide forward secrecy: as soon as the long-term password $PW$ is leaked, all the previous session keys can be recovered.

Let $x_1 = a_1 \oplus H(PW)$ and $x_2 = a_2 \oplus H(PW)$ be the messages transmitted in the target session. Then, with the password $PW$ and the messages $x_1$ and $x_2$, $I$ can trivially compute previous session key $K$ as follows:

$$a_1 = x_1 \oplus H(PW) \oplus H(PW),$$
$$a_2 = x_2 \oplus H(PW) \oplus H(PW),$$
$$K = a_1 a_2.$$

Therefore, once a client's password is exposed, there is nothing to prevent an attacker with the password from accessing privileged information communicated in earlier sessions.

## 4. Conclusion

An efficient key exchange and authentication scheme for session initiation protocol has been proposed in the recent work of Huang and Wei [5]. Despite its simplicity and low-computation properties, we found that the Huang-Wei scheme is vulnerable to an offline dictionary attack and forward secrecy. So far, it seems to be impossible to design a secure password-authenticated key exchange scheme without relying on public-key cryptography. To avoid the vulnerability of the Huang-Wei scheme to dictionary attack, we refer the readers to Yang et al.'s scheme [3] and other well-known password-authenticated key exchange protocols [8, 9, 10, 11].

## Reference


[1] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP: Session Initiation Protocol", IETF RFC 2543, March 1999. Available from: http://www.ietf.org/rfc/rfc2543.txt

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", IETF RFC 3261, June 2002. Available from: http://www.ietf.org/rfc/rfc3261.txt

[3] C. C. Yang, R. C. Wang, W. T. Liu, "Secure Authentication Scheme for Session Initiation Protocol", Computers & Security, vol.24, no.5, pp.381-386, August 2005.

[4] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol.22, no.6, pp.644-54, November 1976.

[5] H. F. Huang, W. C. Wei, "A New Efficient Authentication Scheme for Session Initiation Protocol", Joint Conference Information Sciences, October 2006.

[6] William Stallings, Network Security Essentials: Applications and Standards, Prentice-Hall, 2000, Chapter 9.

[7] D. Shin, Y. Choi, S. Park, "Cryptanalysis on the Authentication Mechanism of the NateOn Messenger", Korea Institute Of Information Security And Cryptology, vol.17, no.1, pp.67-80, February 2007.

[8] M. Bellare, D. Pointcheval, P. Rogaway, "Authenticated Key Exchange Secure against Dictionary Attacks", Proc. of Eurocrypt 2000, LNCS vol.1807, pp.139-155, Springer-Verlag, May 2000.

[9] S. Bellovin, M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure against Dictionary Attacks", Proc. of the Symposium on Security and Privacy, IEEE, pp.72-84, May 1992.

[10] V. Boyko, P. MacKenzie, S. Patel, "Provably secure password-authenticated key exchange using Diffie-Hellman", Proc. of Eurocrypt 2000, LNCS vol.1807, pp.156-171, Springer-Verlag, May 2000.

[11] R. Ostrovsky, M. Yung, "Efficient Password-Authenticated Key Exchange Using Human-Memorizable Passwords", Proc. of Eurocrypt 2001, A preliminary full version is available from: http://eprint.iacr.org/2001/031.pdf

## ◐ 저 자 소 개 ◑

**김 미 진(Mijin Kim)**
1985년 성균관대학교 수학교육학과 졸업(학사)
1997년 Computing, Northeastern University, at Boston (M.S.)
2006~현재 성균관대학교 대학원 전자전기컴퓨터공학과 박사과정
관심분야 : 정보보호, 암호 프로토콜, 네트워크 보안
E-mail : mjkim@security.re.kr

**남 정 현(Junghyun Nam)**
1997년 성균관대학교 정보공학과 졸업(학사)
2002년 Computer Science, University of Louisiana, at Lafayette(M.S.)
2006년 성균관대학교 대학원 컴퓨터공학과 졸업(박사)
2007~현재 건국대학교 충주캠퍼스 컴퓨터응용과학부 컴퓨터시스템전공 조교수
관심분야 : 정보보호, 네트워크 보안
E-mail : jhnam@kku.ac.kr

**원 동 호(Dongho Won)**
1976년~1988년 성균관대학교 전자공학과 졸업(학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1985년~1986년 일본 동경공업대 객원연구원
1988년~2003년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장,
정보통신대학원장, 정보통신신기술연구소장, 연구처장
2002년~2003년 한국정보보호학회장
현재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장,
정보통신부지정 정보보호인증 기술연구센터 센터장
관심분야 : 암호이론, 정보이론, 정보보호
E-mail : dhwon@security.re.kr