INFORMATICA, 2000 Vol. 0, No. 0, 1–0

An Improvement of SPLICE/AS in WIDE Against Guessing Attack

Min-Shiang HWANG, Cheng-Chi LEE, Yuan-Liang TANG

Department of Information Management
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Fax: 886-4-3742337 E-mail: mshwang@mail.cyut.edu.tw

Abstract. Yamaguchi, Okayama, and Miyahara proposed a simple but efficient authentication system, SPLICE/AS. In this article, we show that their method is vulnerable to the guessing attack. An attacker can obtain the password, private-key, and public-key of the user. To overcome the vulnerability of SPLICE/AS to the guessing attack, we propose an improvement of their system. In our scheme, we not only prevent the guessing attack to obtain secret messages but also enhance the security of the SPLICE/AS authentication system in WIDE.

Key words: Authentication, Private key, Public key, Password, Internet, Guessing attack, Security.

1. Introduction

Today, password authentication systems are wide spread. To prevent a password from being compromised is an important work (Abadi, 1997, Hwang, 1999, Hwang, 2000). The WIDE (Widely Integrated Distributed Environment) started in 1988 as a research project (Murai, 1989). In WIDE, the access level to the server each user holds can be determined. In 1990, Yamaguchi et al. proposed an efficient authentication system SPLICE/AS for WIDE (Yamaguchi, 1990).

In this article, we show that there is a weakness in the SPLICE/AS. An unauthorized person can use the guessing attack (Li, 1993) to obtain a legal user's password and then obtain the legal user's private and public keys. Furthermore, we propose an improved method to prevent this guessing attack.

The remainder of this paper is organized as follows. In the next section, we give a brief review of the SPLICE/AS authentication system and point out the vulnerability of the system. In Section 3, we propose an improved method to overcome the vulnerability of the SPLICE/AS system. In Section 4, we discuss the security of our scheme. Finally, conclusions are given in Section 5.

Table 1. The abbreviations and notations.

C	Client identity.
S	Server identity.
AS	Authentication Server.
SK_A	Secret key of entity A.
PK_A	Public key of entity A.
PW_A	Password of entity A.
$[M]^K$	Encrypt the message M using symmetric cryptosystem with secret key K.
$A \rightarrow B : msg$	Send the message msg from A to B.

2. The Weakness of the SPLICE/AS

In this section, we discuss the key acquisition session in SPLICE/AS (Yamaguchi, 1990). In Table 1, we give the abbreviations and the notations used in SPLICE/AS.

To login SPLICE/AS system for network services, each user must have his/her identity which is authenticated by the authentication server (AS), and then obtain the private and public keys. If a user has his/her keys, he/she can request services to the server with his/her keys. The procedures for getting keys are described in Figure 1.

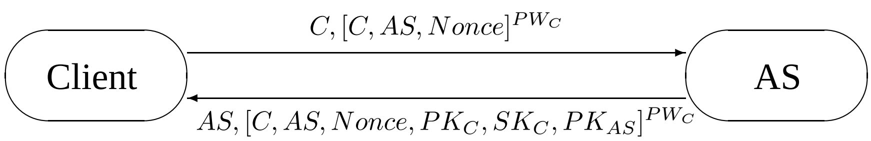

Fig. 1. SPLICE/AS protocol for getting keys.

- Step 1: Through a client program, the user inputs his/her password PW_C to construct ($[C, AS, Nonce]^{PW_C}$) and then sends his/her identity C and the message $[C, AS, Nonce]^{PW_c}$ to AS.
- Step 2: When AS receives these messages from the client, AS analyzes C and obtains his/her password PW_C which is stored in the database. AS uses the password PW_C to decrypt the message $[C, AS, Nonce]^{PW_C}$. If the decrypted user's identity is correct, AS admits the client as a legal

user and then sends the messages, AS, $[C, AS, Nonce, PK_C, SK_C, PK_{AS}]^{PW_C}$, to the client. The client can obtain his/her private key, public key, and AS's public key using password PW_C. Therefore, the user can acquire the keys in a secure manner.

The cryptosystem between the client and AS uses a conventional encryption/decryption algorithm.

The SPLICE/AS system can be attacked using the guessing attack (Li, 1993). In fact, an unauthorized person can intercept the message C, $[C, AS, Nonce]^{PW_C}$ of another user from the open network in Figure 1. The unauthorized person can then guess a candidate PW'_C to try to decrypt the message. If the decrypted user's identity is correct, the unauthorized person assumed that $PW_C = PW'_C$. Otherwise, he/she tries the next candidate password PW'_C until the decrypted user's identity is correct.

Most passwords are a meaningful short string of numbers. A guessing attack can be used against SPLICE/AS off-line (Li, 1993). Therefore, the guessing attack is computationally feasible.

Once the unauthorized person obtains an authorized user's PW_C through the guessing attack, he/she can intercept the messages AS, $[C, AS, Nonce, PK_C$, SK_C, $PK_{AS}]^{PW_C}$ in Figure 1, to decrypt the message using PW_C. Therefore, he/she can obtain the private key SK_C and public key PK_C of the user.

If the unauthorized person has an authorized user's keys, he/she can forge his/her identity to request services from the server. Therefore, the system is insecure.

3. Our Improvement Method

To overcome the guessing attack in SPLICE/AS system, an improved method is proposed in this paper. The main idea of the method is to use a long random number r to immunize the guessing attack. In this section, we define that a one-way function $f(x)$ is equal to $g^x \bmod p$, where x is an integer; p is a large prime and g is a generator for Z_p^*. The parameters g, p, and $f(\cdot)$ are opened. The parameter x is secret. The procedures of the method are described as follows and shown in Figure 2.

- Step 1: Through a client program, user inputs a private value $f(PW_C + r)$ to construct ($[C, AS, Nonce]^{f(PW_C+r)}$), where PW_C is the user's password; and r is a very long random number. Next, the user sends his/her identity, $R \oplus PW_C$, and $[C, AS, Nonce]^{f(PW_C+r)}$ to AS, where $R = f(r)$ (i.e., $R = g^r \bmod p$).

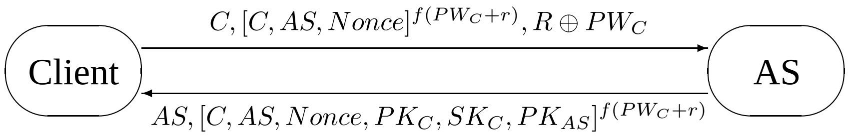

Fig. 2. Our improved protocol for getting keys.

- Step 2: When AS receives these messages from the client, AS analyzes C and obtains his/her password PW_C which is stored in the database. AS derives R from $R \oplus PW_C \oplus PW_C$. AS then obtains $f(PW_C + r)$ as follows.

$$\begin{aligned} & f(PW_C) \times R \\ &= g^{PW_C} \times g^r \bmod p, \\ &= g^{PW_C+r} \bmod p, \\ &= f(PW_C + r). \end{aligned} \tag{1}$$

  Next, AS uses $f(PW_C + r)$ to decrypt the message $[C, AS, Nonce]^{f(PW_C+r)}$. AS thus obtains C, AS, and Nonce. If the user's identity C is correct, AS trusts the client as a legal user and sends the messages, AS, $[C, AS, Nonce, PK_C, SK_C, PK_{AS}]^{f(PW_C+r)}$, to client. The client can obtain his/her private key, public key, and AS's public-key using $f(PW_C + r)$. Therefore, the user can acquire the keys in a secure manner.

The cryptosystem between the client and AS is a symmetric encryption/decryption algorithm, such as DES, AES, IDEA, etc. (Schneier, 1996).

4. Security Analysis

The security of our method is based on discrete logarithms (Diffie, 1976). It is difficult to obtain $f(PW_C+r)$ without knowing PW_C and r. If an attacker wants to obtain $f(PW_C + r)$, he/she must guess an integer x such that $x = PW_C + r$. Since r is a long random number (i.e., 512 bits in length), the probability of guessing x is less than $\frac{1}{2^{512}}$.

Since the attacker cannot obtain $f(PW_C + r)$, he/she cannot decrypt the transmitted message and obtain the private and public keys of the user. Therefore, our method is secure.

5. Conclusions

In this paper, we have shown a weakness in SPLICE/AS. An unauthorized person can use guessing attack to obtain a legal user's password and then obtain the legal user's private and public keys. In addition, we proposed an improved method against the guessing attack. The security of our method is based on discrete logarithms.

Acknowledgements The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC89-2213-E-324-053.

REFERENCES

Abadi, M., T.M.A. Lomas, and R. Needham (1997). Strengthening passwords. *http://ftp.digital.com/pub/DEC/SRC/technical-notes/SRC-1997-033-html/*.

Diffie, W. and M. Hellman (1976). New direction in cryptography. *IEEE Transactions On Information Theory*, **22**(6), 472–492.

Hwang, M.S. (1999). A remote password authentication scheme based on the digital signature method. *International Journal of Computer Mathematics*, **70**, 657–666.

Hwang, M.S. and L.H. Li (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions On Consumer Electronics*, **46**(1), 28–30.

Li, G., T.M.A. Lomas, R. Needham, and J.H. Saltzer (1993). Protecting poorly chosen secrets from guessing attacks. *IEEE Journal on Selected Areas in Communications*, **11**, 648–656.

Murai, J., A. Kato, H. Kusumoto, S. Yamaguchi, and T. Sato (1989). Construction of a Widely Integrated Distributed Environment. *Proc. of IEEE Region 10 Conference on Computer and Communication System*.

Schneier B. (1996). Applied Cryptography. *John Wiley & Sons*.

Yamaguchi S., K. Okayama, and H. Miyahara (1990). Design and implementation of an authentication system in WIDE internet environment. *Proc. of IEEE Region Conf. on Computer and Communication System*.

M.-S. Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao

Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

C.-C. Lee received the B.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999. He is currently pursuing his master degree in Information Management from CYUT. His current research interests include information security, cryptography, and mobile communications.

Y.-L. Tang received the B.S. degree in Electronic Engineering from Chung Yuan Christian University, Chung-Li, Taiwan, Republic of China, in 1986; the M.S. degree in Electrical Engineering from the Pennsylvania State University, U.S.A., in 1991; and the Ph.D. degree in Computer Engineering from the Pennsylvania State University, U.S.A., in 1994. He was with TAISEL (Taiwan International Standards Elecronics, Ltd.) from 1988 to 1989, where he worked as a software designer for electronic exchange systems. He participated several research projects supported by NASA (National Aviation and Aerospace Administration), U.S.A., from 1990 to 1994. In those projects, he worked as a research assistant to study the possibility of utilizing computer vision techniques to enhance landing safety of an aircraft. He is currently an associate professor in the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. His current research interests include information security, mobile communications, image processing, computer vision, pattern recognition, information management, and artificial intelligence.