Guessing Attacks on Strong-Password Authentication Protocol

Cheng-Chi Lee[1], Chia-Hsin Liu[2], and Min-Shiang Hwang[3]
(Corresponding author: Min-Shiang Hwang)

Department of Library and Information Science, Fu Jen Catholic University[1]
510 Jhongjheng Road, Taipei 24205, Taiwan, R.O.C.
Department of Computer Science and Information Engineering, Asia University[2]
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung 41354, Taiwan, R.O.C. (Email: mshwang@asia.edu.tw)
(Received June 24, 2012; revised and accepted Dec. 11, 2012)

Abstract

Password authentication is the most important and convenient protocol for verifying users to get the system's resources. Lin et al. had proposed an optimal strong-password authentication protocol (OSPA) which is a one-time password method. It can protect against the replaying attacks, impersonation attacks, and denial of service attacks. However, the authors shall show that the OSPA protocol is vulnerable to the guessing attacks in this paper.

Keywords: Authentication, cryptography, guessing attack, hash function, password.

1 Introduction

Password authentication is one of the simplest and the most convenient authentication mechanisms to prevent an illegal user from using the system's resources. To access the systems's resources, each user should have an identifier (ID) and a password (PW) [3, 21, 27]. The ID and PW are maintained by the remote system. When a user wants to login to a remote server, he/she has to submit his/her ID and PW to the server [5, 11, 17]. On receiving the login message, the remote server checks if the ID and PW is legal [1, 6, 7, 8, 12, 13, 16, 19, 20, 22, 25, 26].

Recently, a simple strong-password authentication scheme (SAS) had been proposed by Sandirigama et al. [15, 18, 24]. The authors claimed that it had low storage, processing, and transmission overheads, without more advanced public-key cryptosystem and other key exchange techniques. However, Lin et al [14] showed that SAS is not secure against the replaying attacks and denial of service attacks. Thus, Lin et al. proposed an optimal strong-password authentication protocol (OSPA protocol for short). It can protect the system against the stolen-verifier attacks, the replaying attacks, and denial of service attacks. Nevertheless, Chen and Ku [2] pointed out that the OSPA is also not secure against stolen-verifier attacks. Later, Tsuji and Shimizu [23] pointed out that the stolen-verifier attacks would be easily solved if the server could provide the maturity management. Then, Tsuji and Shimizu proposed another impersonation attacks on the OSPA if they can intercept the transmitted messages from the $(n-1)$th to $(n+1)$th authentication sessions. That is to say, the adversary should intercept three times of transmitted messages. In this paper, we shall propose another password guessing attacks to intercept only one time of transmitted messages. Then, the adversary can break password by playing off-line guessing attacks [4, 9, 10]. He/she can easily obtain the correct password of a user from public channel.

This paper is organized as follows: In next section, we shall review the OSPA protocol. Then, the guessing attacks is shown in Section 3. Finally, our brief conclusion will be drawn in Section 4.

2 A Review of OSPA Protocol

In this section, we review the OSPA protocol. It consists of two phases: the registration phase and the authentication phase. The registration phase is invoked and initialed only once in a secure channel. When a user wants to get the resources of certain system, the authentication phase should be performed.

We fist define the notations used in this paper in the following:

- A: an identity of a user;
- S: an authentication server;
- P: the password of a user;
- $h(\cdot)$: a secure one-way function, where $h(message)$ is hashed once, and $h^2(message)$ is hashed twice;
- n: an integer which indicates times of authentication sessions;

- $\oplus$: a bit-wise XOR operation;
- $A \longrightarrow m \longrightarrow S$: A sends m to S through an insecure channel;
- $A \Longrightarrow m \Longrightarrow S$: A sends m to S through a secure channel.

The initial registration phase is shown in the following steps:

Step 1. A calculates $h^2(P \oplus 1)$.
Step 2. $A \Longrightarrow A$, $h^2(P \oplus 1) \Longrightarrow S$, where A registers on S.
Step 3. S stores A, $h^2(P \oplus 1)$, and $n = 1$.

In the authentication phase, the user A performs the nth login. The steps of authentication phase are in the following:

Step 1. $A \longrightarrow A, login\ request \longrightarrow S$.
Step 2. $S \longrightarrow n \longrightarrow A$.
Step 3. $A \longrightarrow c_1, c_2, c_3 \longrightarrow S$, where A calculates $c_1 = h(P \oplus n) \oplus h^2(P \oplus n)$, $c_2 = h^2(P \oplus (n + 1)) \oplus h(P \oplus n)$, and $c_3 = h^3(P \oplus (n + 1))$.
Step 4. Upon receiving c_1, c_2 and c_3, S checks if $c_1 \neq c_2$ holds. If it does, S calculates $h(P \oplus n) = c_1 \oplus h^2(P+n)$ and $h^2(P \oplus (n+1)) = c_2 \oplus h(P \oplus n)$. Then, S checks if $c_3 = h(h^2(P \oplus (n+1)))$. If it holds, S can authenticate A and replaces $h^2(P \oplus (n))$ with $h^2(P \oplus (n + 1))$. S then calculates $n = n + 1$ for next login.

3 Guessing Attacks on OSPA Protocol

In this section, we shall show that the OSPA protocol is not robust enough against off-line password guessing attacks from an evil E. An evil E can intercept transmitted messages from public channel and then break password by playing off-line guessing attacks. E can guess a password P' until the guessing password P' is equal to the correct password P. Otherwise, E repeatedly guesses a new P' off-line. Suppose that E tends to get A's password P. E can intercept n, c_1, c_2, and c_3 from public channel. Then, E can choose any c_1, c_2, or c_3 for checking the correct password. We list three methods to guess the correct password as follows.

- Select c_1 for guessing attack:

  Step 1. Compute $c_1' = h(P' \oplus n) \oplus h^2(P' \oplus n)$.
  Step 2. Check if $c_1 \stackrel{?}{=} c_1'$.
  Step 3. If it is correct, E obtains the correct password of A.

- Select c_2 for guessing attack:

  Step 1. Compute $c_2' = h^2(P' \oplus (n+1)) \oplus h(P' \oplus n)$.
  Step 2. Check if $c_2 \stackrel{?}{=} c_2'$.
  Step 3. If it is correct, E obtains the correct password of A.

- Select c_3 for guessing attack:

  Step 1. Compute $c_3' = h^3(P' \oplus (n + 1))$.
  Step 2. Check if $c_3 \stackrel{?}{=} c_3'$.
  Step 3. If it is correct, E obtains the correct password of A.

If it is correct, E believes that he/she had guessed a correct password P; otherwise, E repeatedly guesses a new P' off-line till E can guess a correct password P. As analyzed above, an adversary can choose any intercepted c_1, c_2, or c_3 to guess the correct password of the legal user. Thus, the OSPA protocol is vulnerable to the guessing attacks.

4 Conclusion

In this paper, we have shown that the OSPA protocol is vulnerable to the guessing attacks. Any adversary can guess a legal user's password without computing the complex algorithm.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC98-2221-E-005-050-MY3. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] J. Botting, "Security on the Internet: Authenticating the user," *Telecommunications*, vol. 31, no. 12, pp. 77–80, 1997.
[2] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," *IEICE Transactions on Communications*, vol. E85-B, pp. 2519–2521, November 2002.
[3] D. He, J. Chen, and J. Hu, "Weaknesses of a remote user password authentication scheme using smart card," *International Journal of Network Security*, vol. 13, no. 1, pp. 58–60, 2011.
[4] D. He, J. Chen, and J. Hu, "Weaknesses of a remote user password authentication scheme using smart card," *International Journal of Network Security*, vol. 13, no. 1, pp. 58–60, 2011.
[5] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," *International Journal of Computer Mathematics*, vol. 70, pp. 657–666, 1999.
[6] M. S. Hwang, S. K. Chong, and T. Y. Chen, "Dos-resistant id-based password authentication scheme using smart cards," *Journal of Systems and Software*, vol. 83.
[7] M. S. Hwang, C. C. Lee, and Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack," *International Journal of Informatica*, vol. 12, no. 2, pp. 297–302, 2001.

[8] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[9] M. Kumar, "An enhanced remote user authentication scheme with smart card," *International Journal of Network Security*, vol. 10, no. 3, pp. 175–184, 2010.

[10] M. Kumar, "A new secure remote user authentication scheme with smart cards," *International Journal of Network Security*, vol. 11, no. 2, pp. 88–93, 2010.

[11] M. Kumar, M. K. Gupta, and S. Kumari, "An improved efficient remote password authentication scheme with smart card over insecure networks," *International Journal of Network Security*, vol. 13, no. 3, pp. 167–177, 2011.

[12] L. H. Li, I. C. Lin, and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks," *IEEE Transactions on Neural Networks*, vol. 12, no. 6, pp. 1498–1504, 2001.

[13] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727–740, 2006.

[14] C. L. Lin, H. M. Sun, and T. Hwang, "Attacks and solutions on strong-password authentication," *IEICE Transactions on Communications*, vol. E84-B, pp. 2622–2627, September 2001.

[15] C. W. Lin, C. S. Tsai, and M. S. Hwang, "A new strong-password authentication scheme using one-way hash functions," *International Journal of Computer and Systems Sciences*, vol. 45, no. 4, pp. 623–626, 2006.

[16] I. C. Lin, M. S. Hwang, and L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13–22, 2003.

[17] R. Ramasamy and A. P. Muniyandi, "An efficient password authentication scheme for smart card," *International Journal of Network Security*, vol. 14, no. 3, pp. 180–186, 2012.

[18] M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol (SAS)," *IEICE Transactions on Communications*, vol. E83-B, pp. 1363–1365, June 2000.

[19] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414–416, 2003.

[20] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards," *Computers & Security*, vol. 22, no. 7, pp. 591–595, 2003.

[21] S. K. Sood, A. K. Sarje, and K. Singh, "Inverse cookie-based virtual password authentication protocol," *International Journal of Network Security*, vol. 13, no. 2, pp. 98–108, 2011.

[22] Y. L. Tang, M. S. Hwang, and C. C. Lee, "A simple remote user authentication scheme," *Mathematical and Computer Modelling*, vol. 36, pp. 103–107, 2002.

[23] T. Tsuji and A. Shimizu, "An impersonation attack on one-time password authentication protocol OSPA," *IEICE Transactions on Communications*, vol. E86-B, no. 7, pp. 2182–2185, 2003.

[24] H. C. Wu, M. S. Hwang, and C. H. Liu, "A secure strong-password authentication protocol," *Fundamenta Informaticae*, vol. 68, pp. 399–406, 2005.

[25] C. C. Yang, T. Y. Chang, and M. S. Hwang, "The security of the improvement on the methods for protecting password transmission," *Informatica*, vol. 14, no. 4, pp. 551–558, 2003.

[26] C. C. Yang, T. Y. Chang, J. W. Li, and M. S. Hwang, "Security enhancement for protecting password transmission," *IEICE Transactions on Communications*, vol. E86-B, no. 7, pp. 2178–2181, 2003.

[27] L. Yang, J. F. Ma, and Q. Jiang, "Mutual authentication scheme with smart cards and password under trusted computing," *International Journal of Network Security*, vol. 14, no. 3, pp. 156–163, 2012.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 1999 and in 2001. He researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He received the Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He was a Lecturer of Computer and Communication, Asia University, from 2004 to 2007. From 2007, he is an assistant professor of Photonics and Communication Engineering, Asia University. From 2009, he is an Editorial Board member of International Journal of Network Security and International Journal of Secure Digital Information Age. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 60+ articles on the above research ?elds in international journals.

Chia-Hsin Liu was born in Miao-Li, Taiwan, Republic of China, on August 1, 1979. He received the B.S. and M.S. degree in Department of Information Management and Graduate Institute of Networking and Communication Engineering from Chaoyang University of Technology, Taichung, Taiwan, in 2002 and 2004. He is currently a System Engineer in OmniWise International Inc. His research interests include Cryptography, Information Security, Database Security and Network Security.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, 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

eld "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in eld "Information Engineering", qualied as advanced technician the rst class in 1990. He was a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He obtained 1997, 1998, 1999, 2000, and 2001 Outstanding Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 170+ articles on the above research elds in international journals.