논문번호 12-37C-08-08

한국통신학회논문지 '12-08 Vol.37C No.08
http://dx.doi.org/10.7840/kics.2012.37C.8.697

안전한 원격사용자 인증스킴에 대한 취약성 분석

Jin Qiuyan◆, 이 광 우*, 원 동 호°

Cryptanalysis of a Secure Remote User Authentication Scheme

Jin Qiuyan◆, Kwangwoo Lee*, Dongho Won°

ABSTRACT

In 2011, C.-T. Li et al. proposed a secure user authentication scheme, which is an improvement over Kim et al.'s scheme to resolve several security flaws such as off-line password guessing attack and masquerading attack. C.-T. Li et al. claimed that their scheme prevents smart card security related attacks. Moreover, it provides mutual authentication and session key establishment. However, we found that their scheme is vulnerable to password guessing attack through password change phase, smart card forgery attack and stolen verifier attack. Moreover, C.-T. Li et al.'s scheme is not secure against password guessing attack as they claimed. In this paper, we also point out that their scheme is not practical to use.

요 약

2011년, C.-T. Li et al.은 Kim et al. 스킴의 문제점인 오프라인 패스워드 추측 공격과 신분 위장 공격을 해결한 향상된 안전한 사용자 인증 스킴을 제안하였다. C.-T. Li et al.은 그들이 제안하는 방식이 패스워드 추측 공격과 신분 위장 공격 등의 스마트카드 보안 관련 공격들을 막을 수 있다고 주장하였다. 또한 상호 인증과 세션 키 생성을 제공한다는 장점을 가지고 있었다. 하지만, 본 논문에서 분석한 결과, C.-T. Li et al.의 스킴은 패스워드 변경 단계에서의 패스워드 추측 공격이나 스마트카드 위조 공격, 훔친 검증자 공격(stolen verifier attack)에 취약함이 발견되었다. 본 논문에서는 C.-T. Li et al.의 스킴이 패스워드 추측 공격에 대해 안전하지 않으며, 실용적이지 않다는 것을 지적하고자 한다.

Key Words : 취약점 분석, 스마트카드, 패스워드 추측 공격, 네트워크 보안, 원격 사용자 인증

Ⅰ. Introduction

A remote user authentication mechanism is a procedure which using password and smart card to verify if the communication parties are trustable and legitimate. In the past couple of decades, there have been many researches [1-12] about remote user authentication over insecure network.

In 2002, Chien et al[1]. proposed an efficient password based remote user authentication scheme which can provide mutual authentication. In Chien et al.'s scheme, users are allowed to choose the password without registering with the server. In 2004, Lee et al[2]. gave a cryptanalysis to Chien et al.'s scheme and proposed an enhanced scheme. Lee et al.'s scheme has the merits of preventing parallel session attack. In 2005, Yoon and Yoo [3] pointed out that Lee et al.'s scheme is vulnerable to the masquerading server attack. Moreover, they also showed Lee et al.'s scheme is not secure against

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학IT연구센터육성 지원사업의 연구결과로 수행되었음(NIPA-2012-H0301-12-3007)
◆ 주저자 : 성균관대학교 정보통신공학부 정보보호연구소, qyjin@security.re.kr, 준회원
° 교신저자 : 성균관대학교 정보통신공학부 정보보호연구소, dhwon@security.re.kr, 종신회원
* 성균관대학교 정보통신공학부 정보보호연구소, kwlee@security.re.kr
논문번호 : KICS2012-03-151, 접수일자 : 2012년 3월 30일, 최종논문접수일자 : 2012년 7월 6일

password guessing attack through password change phase. To remedy these disadvantages, they proposed an enhanced scheme. In 2009, Kim and Chung [4] proposed an improvement to Yoon-Yoo's scheme, which can cope with some security flaws. In 2010, Horng and Lee [5] presented a cryptanalysis of Kim et al.'s scheme and showed their scheme is vulnerable to off-line password guessing attack and masquerading attack. In 2011, C.-T. Li et al[6]. proposed a secure user authentication scheme, which is an improvement to Kim et al.' scheme.

In this paper, we present C.-T. Li et al.'s scheme is vulnerable to password guessing attack through password change phase, smart card forgery attack and stolen verifier attack. In addition, we found that their scheme is not secure against password guessing attack as they claimed. Furthermore, we point out that their scheme is unjustifiable and not practical to use.

The rest of the paper is organized as follows. In Section 2, we review C.-T. Li et al.'s scheme. In Section 3, we show security analysis of C.-T. Li et al.'s scheme. Finally, we conclude this paper in Section 4.

Ⅱ. A Review of C.-T. Li et al.'s Scheme

In this section, we briefly review the remote user authentication scheme proposed by C.-T. Li et al.. Their scheme consists of four phases; registration, login, verification and password change phase. The registration, login and verification phase of C.-T. Li et al.'s scheme are summarized in Fig.1. For convenience of description, Notations used in the paper are summarized as Table 1.

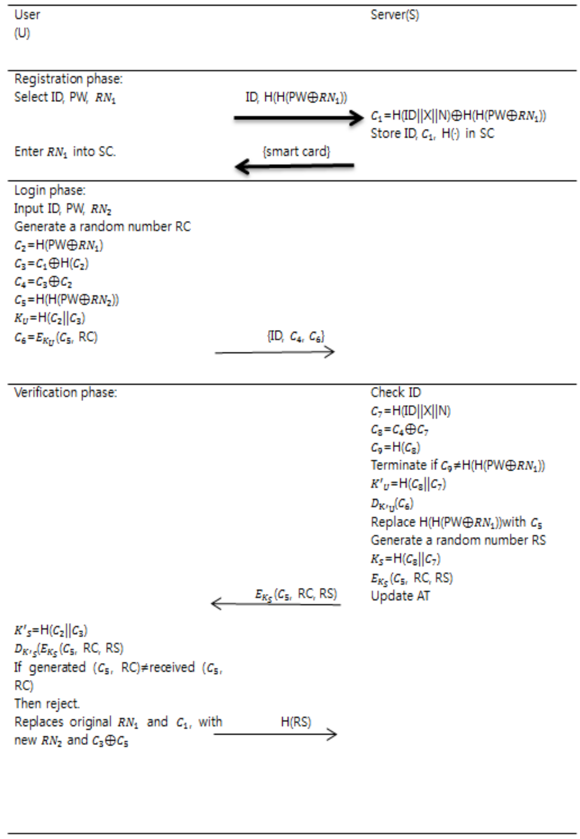

Fig. 1. C.-T. Li et al.' s remote user authentication scheme

Table 1. Notations used in this paper

Notation	Description
U	A user
ID, PW, SC	U's identity, password and the smart card of U
S	A remote server
X	S's master secret key, which is kept secret and only known by S. $X \in \{0,1\}^{256}$
N	The number of times U re-registers to S
SK	The common session key
RN_i	Random number generated by U. $RN_i \in \{0,1\}^{256}$
AT	Account table maintained by S for a registration service
$\oplus$	The bitwise XOR operation
$H(.)$	A collision free one-way hash function
$\Vert$	String concatenation
$E_K(.)/D_K(.)$	The symmetric encryption / decryption function with key K
$\Rightarrow$	A secure channel
$\rightarrow$	A public channel

2.1. Registration phase

In this phase, the user U registers with the server S by performing the following steps.

R.1. $U \Rightarrow S: ID, H(H(PW \oplus RN_1))$

U selects his ID, PW and generates RN_1. Then U computes $H(H(PW \oplus RN_1))$ and sends ID and $H(H(PW \oplus RN_1))$ through a secure communication channel to S.

R.2. $S \Rightarrow SC: ID, C_1, H(.)$

After receiving ID and $H(H(PW \oplus RN_1))$, S maintains an account table AT and the format of AT is shown as follows:

User identity	Registration times	Verification parameter
ID	$N=0$	$H(H(PW \oplus RN_1))$

Here, if it is U's initial registration, $N=0$, otherwise, S sets $N=N+1$. The verification parameter is used for a later login request. S computes: $C_1 = H(ID \| X \| N) \oplus H(H(PW \oplus RN_1))$. Afterward, S sends the SC with parameters ID, C_1, $H(.)$ through a secure communication channel to S.

R.3. $U \Rightarrow SC: ID, C_1, H(.), RN_1$

After receiving SC, U stores RN_1 into SC. Note that U's SC contains $\{ID, C_1, H(.), RN_1\}$.

2.2. Login phase

If U wants to login S, firstly, he inserts his own SC into a card reader or the terminal and enters his ID, PW and RN_2. Where RN_2 is a new generated random number used for next login request. Then SC performs the following steps:

L.1. SC generates a random number RC and computes:

$$C_1 = H(PW \oplus RN_1) \quad (1)$$

$$C_3 = C_1 \oplus H(C_2) \quad (2)$$

$$C_4 = C_3 \oplus C_2 \quad (3)$$

$$C_5 = H(H(PW \oplus RN_2)) \quad (4)$$

$$K_U = H(C_2 \| C_3) \quad (5)$$

$$C_6 = E_{K_U}(C_5, RC) \quad (6)$$

L.2. $SC \rightarrow S: ID, C_4, C_6$

2.3. Verification phase

Upon receiving the login request, S has to perform the following steps to authenticate U:

V.1. $S \rightarrow SC: E_{K_S}(C_5, RC, RS)$

S rejects U's login request if ID is invalid. Otherwise, S computes:

$$C_7 = H(ID \| X \| N) \quad (7)$$

$$C_8 = C_4 \oplus C_7 \quad (8)$$

$$C_9 = H(C_8) \quad (9)$$

S successfully authenticates U if the third entry $H(H(PW \oplus RN_1))$ is equal to C_9 and computes:

$$K_U' = H(C_8 \| C_7) \quad (10)$$

Here, K_U' is equal to K_U, S obtains C_5 and RC by decrypting C_6. Then S replaces the third entry $H(H(PW \oplus RN_1))$ with $C_5 = H(H(PW \oplus RN_2))$ and generates a random number RS, then computes:

$$K_S = H(C_8 \| C_7) \quad (11)$$

Finally, S sends $E_{K_S}(C_5, RC, RS)$ to SC and the format of AT is shown as follows:

User identity	Registration times	Verification parameter
ID	$N=0$	$H(H(PW \oplus RN_2))$

V.2. $SC \rightarrow S: H(RS)$

After receiving the message from S, SC computes:

$$K_S' = H(C_2 \| C_3) \quad (12)$$

K_S' is equal to $K_S = H(C_8 \| C_7)$ and SC obtains C_5, RC, RS by decrypting the received message $E_{K_S}(C_5, RC, RS)$. Then SC rejects communication if generated (C_5, RC) is not equal to received (C_5, RC). Otherwise, SC successfully authenticates S, and replaces original RN_1 and C_1 with new RN_2 and $C_3 \oplus C_5$. Finally, SC sends $H(RS)$ to S, so that S can make sure that he is communicating with U.

Note that the agreement session key

$SK = H(RC \oplus RS)$ computed by S and U is used for future secure communications.

2.4. Password change phase

When a user wants to change his password PW with the new password PW', U inserts his SC into the smart card reader and enters his ID, PW, PW' and a new random number RN_3.

Then SC computes:

$$C_2 = H(PW \oplus RN_2) \tag{13}$$

$$C_3 = C_1 \oplus H(C_2) \tag{14}$$

$$C_4 = C_3 \oplus C_2 \tag{15}$$

$$C_5' = H(H(PW' \oplus RN_3)) \tag{16}$$

$$K_U = H(C_2 \| C_3) \tag{17}$$

$$C_6 = E_{K_U}(C_5', RC) \tag{18}$$

Finally SC sends ID, C_4, C_6 to S and S performs verification phase and changes the AT as follows:

User identity	Registration times	Verification parameter
ID	$N=0$	$H(H(PW' \oplus RN_3))$

Ⅲ. Problems of C.-T. Li et al.'s Scheme

3.1. Password guessing attack through password change phase

An attacker UA can guess the password PW of U through initiating the password change phase if he steals or obtains SC of a user U. UA inserts the SC of U into the smart card reader or the terminal, enters ID of U which he can get from intercepting the login request and a guessed PW^*, a new password PW' and a random number RN_3. If the verification phase has been successfully performed, SC will receive an encryption message, it means UA guessed the password of U correctly; otherwise, UA tries again. Although the success probability of password guessing attack during the password change phase which is operated online is not high, this attack still causes the security issues.

3.2. Smart card forgery attack

Some false changes of values in SC are not detectable, because there is no verification by SC in login phase. If an attacker who gets the SC and changes the value of C_1 into $C_1^* = C_1 \oplus Y$, where Y is a random number, and sends it back to SC. Then SC computes:

$$C_3^* = C_1^* \oplus H(C_2) \tag{19}$$

$$C_4^* = C_3^* \oplus C_2 \tag{20}$$

SC does the computing as regular pattern then sends ID, C_4^*, C_6 to the server. Consequently U can not pass the verification phase since S computes C_9 using the C_4^* and check it as follows:

$$C_7 = H(ID \| X \| N) \tag{21}$$

$$C_8^* = C_4^* \oplus C_7 \tag{22}$$

$$C_9^* = H(C_8^*) \tag{23}$$

If $C_9^* \neq H(H(PW \oplus RN_1))$, S rejects the current session.

Therefore U has to face denial of service due to the smart card forgery.

3.3. Stolen verifier attack

S maintains an account table, which contains user identity, registration times and verification parameter. However, there may be some malicious modification, when the account table is revealed through some accident. Moreover, an attacker who obtains the smart card can get some important data from the account table. In case, the modification of account table has not be detected by the server, there will become a serious threat and U has to face denial of service in the verification phase. Suppose an attacker UA obtains the verification parameter $H(H(PW \oplus RN_1))$ from the account table. Moreover, a strong attacker can get C_1 and $H(.)$ from stolen smart card SC, also he can obtain C_4 and C_6 from intercepting the message which is sent to S in login phase. UA can compute out the key which is used for encryption and decryption even he can obtain the session key.

$$C_3 = C_1 \oplus H(C_2) = C_1 \oplus H(H(PW \oplus RN_1)) \quad (24)$$
$$C_2 = C_3 \oplus C_4 \quad (25)$$
$$K_U = H(C_2 \| C_3) \quad (26)$$

Suppose UA obtains $E_{K_S}(C_5, RC, RS)$ from intercepting in verification phase, he can get both RC and RS by decrypting $E_{K_S}(C_5, RC, RS)$, since $K_U = K_S$. Even he can compute the session key $SK = H(RC \oplus RS)$.

3.4. Off-line password guessing attack

An attacker UA can obtain C_1 and RN_1 from the stolen SC. By intercepting the login phase, he can get C_4. With the guessing password PW^*, UA computes as follows:

$$C_2^* = H(PW^* \oplus RN_1) \quad (27)$$
$$C_3^* = C_1 \oplus H(C_2^*) \quad (28)$$
$$C_4^* = C_3^* \oplus C_2^* \quad (29)$$

Herein, UA can do this until C_4^* is equal to C_4.

3.5. Drawbacks

During the registration phase, U selects a random number RN_1 and has to remember it until he gets his own smart card from S to store it. Because RN_1 is hard to be remembered by U, he may record it by writing down on a slip of paper and protect it. It is an unjustifiable and impractical to use.

Ⅳ. Conclusion

In this paper, we have presented cryptanalysis of C.-T. Li et al.'s scheme. We point out that their scheme is vulnerable to password guessing attack through password change phase, smart card forgery attack and stolen verifier attack. In addition, C.-T. Li et al.'s scheme is not secure against password guessing attack as they claimed. Furthermore, we point out that their scheme is not practical to use. To remedy these security flaws, we suggest that when a user wants to enter the smart card, his identity and password should be verified. At the same time, some secure parameters should not be stored in the account table without any encryption. Moreover, some technologies such as PKI(Public-key infrastructure) and OTP(one time password) can be used to improve the security of the remote user authentication scheme.

References

[1] H.Y. Chien, J.K. Jan, Y.M. Tseng, An efficient and practical solution to remote authentication: smart card, *Computers & Security* 21 (4) (2002) 372–375.

[2] S. Lee, H. Kim, K. Yoo, Improvement of Chien et al.'s remote user authentication scheme using smart cards, *Computer Standards & Interfaces* 27 (2004) 181–183.

[3] E. Yoon, K. Yoo, More efficient and secure remote user authentication scheme using smart cards, in: *Proceedings of 11th International Conference on Parallel and Distributed System*, vol. 2, 2005, pp. 73–77.

[4] Kim, S.K., Chung, M.G.: More secure remote user authentication scheme. *Computer Communications* 32(6), 1018–1021 (2009)

[5] W.-B.Horng, C.-P. Lee, J.-W. Peng Cryptanalysis of a More Secure Remote User Authentication Scheme, *Computer symposium (ICS), 2010 International* 16-18 Dec.2010 284 – 287

[6] C.-T. Li, C.-C. Lee, C.-J. Liu, C.-W. Lee A Robust Remote User Authentication Scheme against Smart Card Security Breach. Data and Applications Security and Privacy XXV, LNCS 6818, pp. 231–238, 2011.c_*IFIP International Federation for Information Processing 2011*

[7] S. K. Sood, A.K. Sarje, K. Singh. An Improvement of Hsiang-Shih's Authentication Scheme Using Smart Cards. *International Conference and Workshop on Emerging Trends in Technology* (ICWET 2010) – TCET, Mumbai, India 19-25

[8] C.-L. Chen, Y.-F. Lin, N.-C. Wang, Y.-L. Chen. An Improvement on Hsiang and Shih's Remote User Authentication Scheme Using Smart Cards. *2011 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel*/Distributed Computing 53-57.

[9] M. KUMAR, M.K. GUPTA, S. KUMARI. An Improved Smart Card Based Reote user Authentication Scheme with Session Key Agreement During the Verification Phase. *Journal of Applied Computer Science & Mathematics*, no. 11 (5) /2011, Suceava 38-46

[10] C.I. Fan, Y.C. Chan, Z.K. Zhang, Robust remote authentication scheme with smart cards, *Computers & Security* 24 (8) (2005) 619–628.

[11] Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: *Proceedings of Advances in Cryptology*, pp. 388–397(1999)

[12] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, *IEEE Transactions on Computers* 51 (5)(2002) 541–552.

[13] Namje Park, Seungjoo Kim, Dongho Won, Secure group communication over combined wired and wireless networks, *Lecture Note in Computer Science*, Vol.3592, Springer-Verleg, pp.90-99 (2005)

[14] Kwangwoo Lee, Dongho Won, and Seungjoo Kim, A Secure and Efficient E-Will System Based on PKI, Information - *An International Interdisciplinary Journal, International Information Institute*, Vol. 14, No 7, pp.2187-2206 (2011)

[15] Namje Park, Seungjoo Kim, Dongho Won, *Lecture Note in Computer Science*,Vol.4217, Springer-Verleg, pp.494-505 (2006)

Jin Qiuyan

2011년 Dalian Nationalities University, China 소프트웨어공학 졸업(학사)
2011년~현재 성균관대학교 대학원 정보통신대학 석사 과정
<관심분야>암호이론, 프로토콜

이 광 우 (Kwangwoo Lee)

2005년 성균관대학교 정보통신공학부 졸업(학사)
2007년 성균관대학교 대학원 컴퓨터공학과 졸업(공학석사)
2011년 성균관대학교 대학원 전자전기컴퓨터공학과 졸업(공학박사)
<관심분야> 암호이론, 프로토콜 안전성 분석, 정보보호제품 보안성 평가, 전자투표, 디지털 복합기 보안

원 동 호 (Dongho Won)

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1992년~1994년 성균관대학교 전자계산소 소장
1995년~1997년 성균관대학교 교학처장
1997년~1998년 정보화추진위원회 자문위원 (발령 정보화추진위원회 위원장 국무총리)
1999년~2001년 성균관대학교 정보통신대학원 원장
2002년~2003년 한국정보보호학회 회장
2002년~2004년 대검찰청 컴퓨터 범죄 수사 자문위원
2002년~2004년 성균관대학교 연구처장
2002년~2003년 감사원 IT 감사 자문위원
2002년~2004년 산학연 정보보안협의회 회장
2005년~2008년 한국정보보호진흥원 이사
2005년~현재 정보보호인증기술연구소 소장
2009년~현재 성균관대학교 BK21 사업단장
<관심분야> 암호이론, 정보이론, 정보보호