This item was submitted to Loughborough's Institutional Repository (<https://dspace.lboro.ac.uk/>) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
<http://creativecommons.org/licenses/by-nc-nd/2.5/>

Further Attacks and Comments on 'Security of Two Remote User Authentication Schemes Using Smart Cards'

Raphael Chung-Wei Phan, Member, IEEE, and Bok-Min Goi

Abstract — We point out that Hsu's recent cryptanalysis of Sun's remote user authentication scheme is flawed. We also comment on Chien et. al's scheme and give more practical attacks than those presented by Hsu in the same paper¹.

Index Terms — remote user authentication, smart cards, cryptanalysis.

I. INTRODUCTION

A remote user authentication scheme serves to authenticate the legitimacy of remote users over an insecure channel. In 2000, Sun [5] proposed an efficient remote user authentication scheme using smart cards but this was later shown by Chien et. al [2] to only achieve unilateral authentication in that only the authentication server (AS) could authenticate the remote user and not vice versa. As a consequence, Chien et. al further proposed an improvement. Recently, Hsu [3] considered the security of both these schemes and presented two attacks on Sun's scheme and an attack on Chien et. al's scheme.

In this paper, we comment on Hsu's results, in particular we show that his attacks on Sun's scheme are flawed. We also present attacks on both Sun's and Chien et. al's schemes that are more practical compared Hsu's attack. Further, we give comments on Chien et. al's scheme.

II. TWO REMOTE USER AUTHENTICATION SCHEMES

This section describes Sun's and Chien et. al's remote user authentication schemes.

A. Sun's Scheme

This scheme basically involves any new user, U_i registering with the authentication server, AS , and being issued a smart card, SC_i and subsequently logging in with the smart card to be authenticated by AS . Denote h as a secure one-way hash function, x as the secret key of AS , T as the current time stamp, and $[\cdot]$ as a secure channel. Then, all steps of the scheme are described as follows:

Registration:

$U_i \rightarrow AS: ID_i$
 $AS \rightarrow U_i: [PW_i = h(ID_i, x)]$
 $AS \rightarrow SC_i: h$

Login:

$U_i \rightarrow SC_i: ID_i, PW_i$
 $SC_i \rightarrow AS: ID_i, T, C_1 = h(T \oplus PW_i)$

Authentication:

1. If ID_i invalid, reject login request.
2. If T expired, reject login request.
3. Compute $PW_i = h(ID_i, x)$.
4. Compute $h(T \oplus PW_i)$ and check if equal to C_1 . If YES, U_i is authenticated.

During the *Registration* phase, the new user, U_i presents his ID to the authentication server, AS , who then generates the user's password, PW_i by simply hashing the concatenation of the user's ID and AS 's long-term secret key, x . This password is then sent back to U_i through a secure channel. Further, AS also stores details of the hash function, h in the smart card, SC_i .

Now when the user logs in to the system during the *Login* phase, he inputs his ID and password, PW_i to this smart card which then interacts with the AS by forwarding the user's ID , the current timestamp, T and a computed value, C_1 that is the result of hashing the exclusive-OR (XOR) of T and PW_i .

With this, the protocol enters the *Authentication* phase where the AS checks the validity of the ID_i and the freshness of T , failure of which would result in the login request being rejected. Otherwise, the AS recomputes the password, PW_i and subsequently recomputes C_1 to check with the C_1 value received from the smart card. If they match, then the user is successfully authenticated.

B. Chien et. al's Scheme

The scheme due to Chien et. al similarly comprise the three above phases except that the user is allowed to choose his own password and hence gives more user convenience. In more detail:

Registration:

$U_i \rightarrow AS: ID_i, PW_i$
 $AS \rightarrow SC_i: [R_i = h(ID_i \oplus x) \oplus PW_i, h]$

Login:

$U_i \rightarrow SC_i: ID_i, PW_i$
 $SC_i \rightarrow AS: ID_i, T, C_1 = h(R_i \oplus PW_i \oplus T)$

Authentication:

Performed by $AS \Rightarrow$

1. If ID_i invalid, reject login request.
2. If T expired, reject login request.

¹ The first author acknowledges the Swinburne Sarawak internal grant.

Raphael C.-W. Phan is with the Swinburne Sarawak Institute of Technology, 93576 Kuching, Sarawak, MALAYSIA (e-mail: rphan@swinburne.edu.my).

Bok-Min Goi is with the Faculty of Engineering, Multimedia University, MALAYSIA (e-mail: bmgoi@mmu.edu.my).

Contributed Paper

Manuscript received April 1, 2004

3. Compute $h(h(ID_i \oplus x) \oplus T)$ and check if equal to C_1 . If YES, U_i is authenticated.
4. Compute $C_2 = h(h(ID_i \oplus x) \oplus T')$ and reply with the message:

$$AS \rightarrow U_i: [T', C_2]$$

Performed by $U_i \Rightarrow$

1. Compute $h(C_1 \oplus T')$ and check if equal to C_2 . If YES, AS is authenticated.

During the *Registration* phase, the new user, U_i presents his ID as well as a chosen password, PW_i to the authentication server, AS , who then computes a value R_i which is dependent on the user's ID , AS 's secret key, x and the user's password. This is stored in the user's smartcard along with details of the used hash function, h .

During the *Login* phase, the user inputs his ID and password, PW_i to his smart card which then interacts with the AS by forwarding the user's ID , the current timestamp, T and a computed value, C_1 that is the result of hashing the exclusive-OR of R_i , T and PW_i .

The protocol now enters the *Authentication* phase where the AS checks the validity of the ID_i and the freshness of T , failure of which would result in the login request being rejected. Otherwise, the AS recomputes the value C_1 and checks it with the C_1 received from the smart card. If they match, then the user is successfully authenticated.

Further, the AS computes another value, C_2 which is dependent on the user's ID , AS 's secret key, x and the latest timestamp, T' at that point. This C_2 is then sent back to the user who then recomputes C_2 and checks for a match in order to authenticate AS . Therefore, Chien et. al's protocol allows for mutual authentication of both parties.

III. FLAWS IN HSU'S ATTACKS ON SUN'S SCHEME

In this section, we point out flaws in Hsu's two password guessing attacks on Sun's scheme. In particular, Hsu's *off-line* password guessing attack is an obvious and trivial fact, and hence does not constitute an attack at all, while his *on-line* password guessing attack on Sun's scheme is heavily flawed.

A. Hsu's Off-line Password Guessing Attack

Hsu's off-line guessing attack requires that the attacker eavesdrop during the *login* phase in order to obtain the value of T and C_1 . He then needs to guess all possible values of the password, PW_i , and then verify if $h(T \oplus PW_i)$ equals C_1 .

Guessing all possible values of the password, and for each guess, checking if it is true is merely an exhaustive search of the password space and is an obvious fact and well-known weakness of any cryptographic scheme! Claiming it to be an attack is analogous to claiming to have re-invented the wheel. It is therefore not considered an attack at all.

B. Hsu's On-line Password Guessing Attack

Hsu's on-line guessing attack also requires that an attacker guesses all possible values of the password, PW_i , computing

the value of $C_1^* = h(T \oplus PW_i)$ and replacing the original C_1 in the *login* phase with C_1^* . This is then submitted to AS , and the attacker keeps repeating this until AS finally accepts it as valid.

Besides having the same flaw as the previous off-line attack in that it is merely a trivial exhaustive search of the password space, this attack also has stronger requirements since an attacker must perform an active attack, in contrast to the previous which merely required eavesdropping and hence is a passive attack. Furthermore, exhaustively guessing a password has only a very small probability of 2^{-k} (where k is the size of the password in bits) of being accepted by AS . After only a few unsuccessful guessing attempts, AS would have noticed something amiss and blacklisted the attacker!

In summary, both Hsu's attacks should be disregarded as they are heavily flawed.

IV. IMPROVED ATTACKS ON SUN'S AND CHIEN ET. AL'S SCHEMES

In this section, we present practical attacks on both Sun's and Chien et. al's schemes. Our attacks are more practical in the sense that they require only simple eavesdropping and hence are passive attacks, in contrast to active attacks that require an attacker to interfere with the communicated messages, for example Hsu's parallel session attack [3] on Chien et. al's scheme.

For this purpose, we recall the three phases of Chien et. al's scheme, as described in subsection II.B. Hsu's attack requires that the attacker eavesdrop on the communication during the *login* phase, in particular during the message sent from the user's smart card to AS , in order to obtain the values of T and C_1 . He then masquerades as the user, U_i and generates a new login request message to AS by making use of the eavesdropped values. This is an active attack since an attacker needs to introduce new messages into the communication.

We now describe our attack which is a passive attack. The attacker similarly eavesdrops during the *login* phase, but the difference is that he does so during the message sent from the user, U_i to the smart card and hence obtains PW_i . With the knowledge of this, he can then freely masquerade as U_i in any future login. Since our attack only requires an attacker to eavesdrop and not to interfere with any communicated messages, it is more practical and an attacker can remain undetected.

Similarly, our attack also applies to Sun's scheme where the attacker merely eavesdrops during the *login* phase during the message sent from U_i to his smart card, and the rest follows as in our attack on Chien et. al's scheme.

V. FURTHER REMARKS ON SECURITY

A. Remarks on Chien et. al's Scheme

First, we remark that Hsu's attack on Chien et. al's scheme appears to be sound, and works because parts of different messages (in this case C_1 and C_2) have the same structure – both being equal to $h(h(ID_i \oplus x) \oplus \text{timestamp})$ – which

allows an attacker to reuse a part of a previous message as a valid part in a new message. This is a very well-known weakness [4] of authentication schemes that allows for replay attacks and should be avoided entirely.

Also, this scheme is very insecure since both the user's identity, ID_i and password, PW_i are transmitted in the clear both during the *registration* and the *login* phases. This not only allows an attacker to eavesdrop and obtain these values, but also allows him to modify them according to his liking and lead to masquerades and denial of service attacks.

B. Remarks on Both Schemes

Both schemes use $C_1 = h(T \oplus z)$ for authentication, where z is PW_i for Sun's scheme, while it is $R_i \oplus PW_i$ for Chien et. al's scheme. Regardless, we observe that both schemes use the timestamp, T within the hash function, h and so T is not really tied to a unique C_1 since different T values with different z values could still result in the same $T \oplus z$ that is input to h and so produce the same C_1 . T therefore has lost its main objective as a "time stamp" since this shows that there is no way to bind a certain C_1 to a unique T to prove that it was generated only at that time.

For ease of discussion we suppose that the input, $T \oplus z$ to h is simply 3 bits in length. Then, defining $z = z_2z_1z_0$ and $T = T_2T_1T_0$, we would have the situation as in Table 1.

TABLE I
DIFFERENTIAL INPUTS TO HASH FUNCTION

$T_2T_1T_0$	$T \oplus z$
000	$z_2z_1z_0$
001	$z_2z_1\bar{z}_0$
010	$z_2\bar{z}_1z_0$
011	$z_2\bar{z}_1\bar{z}_0$
100	$\bar{z}_2z_1z_0$
101	$\bar{z}_2z_1\bar{z}_0$
110	$\bar{z}_2\bar{z}_1z_0$
111	$\bar{z}_2\bar{z}_1\bar{z}_0$

This simply means that at two different times corresponding to different timestamps, T , then the two inputs to h would differ by some exclusive-OR (XOR) relationship. Such scenarios are ideal for mounting differential cryptanalysis attacks [1] on hash functions.

VI. CONCLUSIONS

We have shown that Hsu's attacks on Sun's scheme are heavily flawed and hence should be disregarded. We have also presented passive attacks on both Sun's and Chien et. al's scheme which are more practical since an attacker merely needs to eavesdrop and does not need to interfere with the communicated messages. Finally, we have given further comments on the reasons behind Chien et. al's insecurity, plus

remarks on issues that might affect both schemes' security. Both schemes exhibit common weaknesses that should not exist in a standard authentication scheme. We therefore hope that our work here will highlight the importance of more detailed analysis of authentication schemes against these common weaknesses before they can be considered for practical applications.

REFERENCES

- [1] E. Biham, and A. Shamir, "Differential Cryptanalysis of FEAL and N-Hash", *Advances in Cryptology – Eurocrypt'91*, Lecture Notes in Computer Science, vol. 547, 1991, pp. 1-16.
- [2] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication," *Computers and Security*, vol. 21, no. 4, 2002, pp. 372-375.
- [3] C.-L. Hsu, "Security of two remote user authentication schemes using smart cards," *IEEE Trans. Consumer Electronics*, vol. 49, no. 4, 2003, pp. 1196-1198.
- [4] G. Lowe, "An attack on the Needham-Schroeder public-key protocol," *Information Processing Letters*, vol. 56, 1994, pp. 131-133.
- [5] H. M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electronics*, vol. 46, no. 4, 2000, pp. 958-961.

Raphael C.-W. Phan (M'03) became a Member (M) of IEEE in 2003. He obtained his Eng (Hons) degree in Computer Engineering from Multimedia University (MMU), Cyberjaya, Malaysia in 1999. He was an Engineering at MMU and a researcher at MMU's Center for Smart Systems & Innovation (CSSI) from 1999 to 2001, where he also pursued his Master of Engineering Science degree by research sponsored by Intel Corp.'s Fellowship Grant award, titled

"Cryptanalysis of the Advanced Encryption Standard (AES) and Skipjack". He is currently conducting his Ph.D research in "Cryptanalysis of Block Ciphers: Generalization, Extensions & Integration" at MMU. Raphael is Director of the Information Security Research (iSECURES) Lab and lecturer with the Department of Engineering, Swinburne Sarawak Institute of Technology, Kuching, Malaysia. He is reviewer for IEEE Transactions on Computers, IEEE Communication Letters, IEEE Signal Processing Letters, IEEE Spectrum, Cryptologia and Information Processing Letters. His research interests include cryptography, cryptanalysis, authentication and key exchange protocols, and smart card security.

Bok-Min Goi received the B.Eng. degree in Electrical Engineering from University of Malaya (MU) and the M. EngSc degree from Multimedia University (MMU), Malaysia, in 1998 and 2002, respectively. Since April 1998, he has been working as a lecturer in the Faculty of Engineering, MMU. Currently, he is working toward his Ph.D research and as a researcher at MMU's Centre for Cryptography and Information Security (CCIS). His current research interests include cryptography, incremental hash function, authentication and key exchange protocols.