

# 这是任振华的第一份L<sup>A</sup>T<sub>E</sub>X文档

任振华

2452503780@qq.com

计算机学院

数据科学与大数据专业

UESTC, Chengdu, Sichuan, 611731

2019 年 11 月 26 日

## 摘要

A user identity anonymous is an important property for roaming services. In 2011, Kang et al. proposed an improved user authentication scheme that guarantees user in wireless communications. This letter shows that Kang et al.'s improved scheme still cannot provide user anonymity as they claimed.

**Keywords:** cryptanalysis, authentication, anonymity, wireless communications, security

## 1 Introduction

In wireless communication environments, wireless roaming is rapidly becoming an important network feature because of the widespread use of mobile devices such as cellular phones or smart phones. To provide effective global roaming service for a legitimate mobile user between the home network and a visited foreign network, strong mobile user authentication measures are required. Moreover, anonymity of the mobile users should be also guaranteed to protect the privacy of mobile users.

In 2004, Zhu and Ma [1] proposed an authentication scheme with anonymity for wireless communication environments. Later, Lee et al. [2] showed several security flaws of Zhu-Ma's scheme and then improved it. However, in 2008, Wu et al. [3] showed that both Zhu-Ma's scheme and Lee et al.'s scheme still cannot provide anonymity and then proposed an improvement to preserve anonymity. Nevertheless Zeng et al. [4] and Lee et al. [5] showed that Wu et al.'s scheme also cannot provide anonymity, respectively.

In 2011, Kang et al. [7] proposed an improved user authentication scheme based on both Wu et al.'s and Wei et al.'s scheme [3], [6] that guarantees strong user anonymity in wireless communications. However, this letter shows that the Kang et al.'s improved scheme also cannot provide user anonymity as they claimed.

## 2 Review of Kang et al.'s Scheme

Throughout the paper, notations are employed in Table 1. There are three phases in the Kang et al.'s scheme-initial phase, first phase, and second phase. In the initial phase, a mobile user MU sends his/her home agent HA and HA delivers a password and a smart

表 1: Notations

$HA$	Home Agent of a mobile user
$FA$	Foreign Agent of the network
$MU$	Mobile User
$PW_{MU}$	A password of MU
$N$	A strong secret key of HA
$ID_A$	Identity of an entity A
$T_A$	Timestamp generated by an entity A
$Cert_A$	Certificate of an entity A
$(X)_K$	Encryption of message X using symmetric key K
$E_{P_A}(X)$	Encryption of message X using public key A
$S_{S_A}$	Encryption of message X using private key A
$h(-)$	A one-way hash function
$\parallel$	Concatenation
$\oplus$	Bitwise exclusive-or operation

card to MU through a secure channel. In the first phase, foreign agent FA authenticates MU and establishes a session. In the second phase, whenever MU visits —FA, FA serves for MU. The detailed phases are shown in the following.

## 2.1 Initial Phase

When an MU registers with his/her HA, the MU's identity  $ID_{MU}$  is submitted to the HA. After receiving  $ID_{MU}$  from MU, HA generates  $PW_{MU}$ ,  $r_1$  and  $r_2$  as follows.

$$PW_{MU} = h(N \parallel ID_{MU}) \quad (1)$$

$$r_1 = h(N \parallel ID_{HA}) \quad (2)$$

$$r_2 = h(N \parallel ID_{MU}) \oplus ID_{NA} \oplus ID_{MU} \quad (3)$$

When N is a secret value kept by HA. HA stores  $ID_{HA}$ ,  $r_1$ ,  $r_2$  and  $h(\cdot)$  in the smart card of MU and then sends it with  $PW_{MU}$  to MU through a secure channel.

## 2.2 First Phase

Figure 1 illustrates the first phase of Kang et al.'s scheme. A foreign agent FA authenticates MU by interacting with HA as follows.

1.  $MU \rightarrow FA : n, (h(ID_{MU}) \parallel x_0 \parallel x)_L, ID_{HA}, T_{MU}$  If MU inputs  $ID_{MU}$  and  $PW_{MU}$  to MU's mobile device, then MU's mobile device chooses secret random values  $x_0$  and

$x$  and computes  $n$  and  $L$  as follows.

$$n = h(T_{MU} \| r_1) \oplus r_2 \oplus PW_{MU} \quad (4)$$

$$L = h(T_{MU} \oplus PW_{MU}) \quad (5)$$

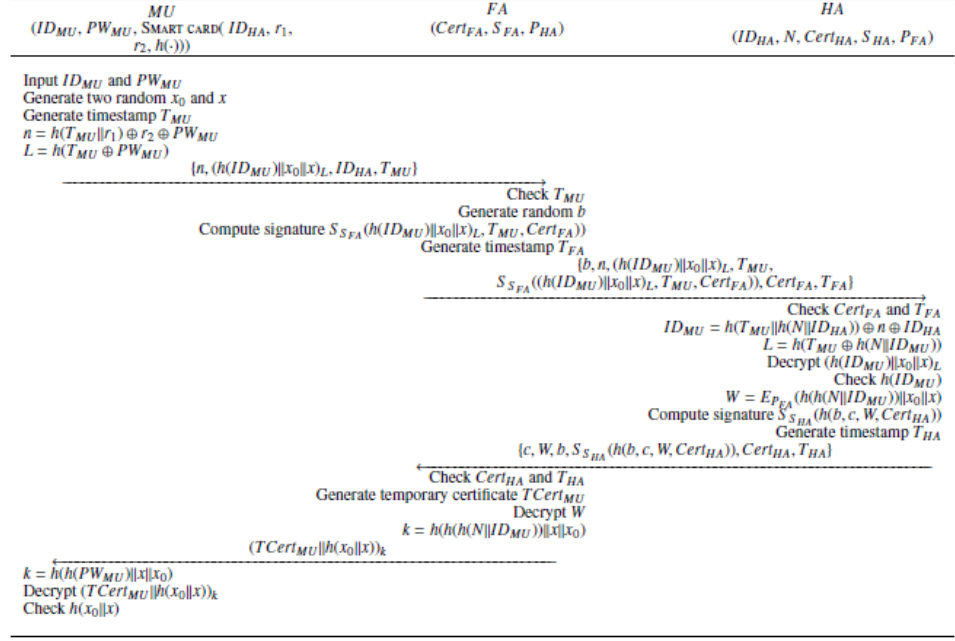


图 1: First phase of Kang et al.'s scheme

$MU$ 's mobile device sends  $MU$ 's login message  $n, (h(ID_{MU}) \| x_0 \| x_L, ID_{HA}, T_{MU})$  to  $FA$ , where  $T_{MU}$  is a current timestamp.

2.  $FA \rightarrow HA$ :  $b, n, (h(ID_{MU}) \| x_0 \| x)_L, T_{MU}, S_{S_{FA}}((h(ID_{MU}) \| x_0 \| x)_L, T_{MU}, Cert_{FA})), Cert_{FA}, T_{FA}$   
 $FA$  checks the validity of  $T_{MU}$ . If it is valid, then  $FA$  chooses secret random number  $b$ .  $FA$  then sends  $b$ , the  $MU$ 's login message containing  $n, (h(ID_{MU}) \| x_0 \| x_L, ID_{HA}, T_{MU})$ , a certificate  $Cert_{FA}$ , timestamp  $T_{FA}$ , and the corresponding signature on the login message by using  $FA$ 's private key  $S_{FA}$  to  $HA$ .
3.  $HA \rightarrow HA$ :  $c, W, b, S_{S_{HA}}(h(b, c, W, Cert_{HA})), Cert_{HA}, T_{HA}$   $HA$  checks the validity of certificate  $Cert_{FA}$  and timestamp  $T_{FA}$ . If they are valid, then  $HA$  computes  $MU$ 's real identity  $ID_{MU}$  as follows.

$$ID_{MU} = h(T_{MU} \| h(N \| ID_{HA})) \oplus n \oplus ID_{HA} \quad (6)$$

$HA$  computes  $L = h(T_{MU} \oplus h(N \| ID_{MU}))$  with his/her secret  $N$  and decrypts  $(h(ID_{MU}) \| x_0 \| x)_L$ . Then,  $HA$  verifies if  $MU$  is a legal user by checking  $h(ID_{MU}) = h(ID_{MU})'$ s, where  $h(ID_{MU})$  is computed with  $ID_{MU}$  on the login message and  $h(ID_{MU})'$  of the decrypting result  $h(ID_{MU})' \| x'_0 \| x'$ . If so, then  $HA$  computes  $W = E_{P_{FA}}(h(h(N \| ID_{MU}) \| x_0 \| x))$  and generates its signature using his/her private key  $S_{HA}$ . Then,  $HA$  sends random

number  $c$ ,  $W$ , the certificate of  $HA$ ,  $Cert_{HA}$ , current timestamp  $T_{HA}$  and signature  $S_{S_{HA}}(h(b, c, W, Cert_{HA}))$  to  $FA$ .

4.  $FA \rightarrow MU : (TCert_{MU} || h(x_0 || x))_k$   $FA$  checks whether or not the certificate  $Cert_{HA}$  and timestamp  $T_{HA}$  are valid. If They are valid, then  $FA$  issues the temporary certificate  $TCert_{MU}$ , which includes a timestamp and other information to  $MU$ . To obtain  $(h(h(N || ID_{MU})) || x_0 || x)$ ,  $FA$  decrypts  $W$  with the secret key corresponding to  $P_{FA}$ . To establish session key  $k_i$  for  $i$ -th session,  $FA$  first saves  $(TCert_{MU}, h(PW_{MU}, x_0))$ .  $FA$  encrypts  $(TCert_{MU} || h(x_0 || x))$  with session key  $k$  and gives  $(TCert_{MU} || h(x_0 || x))_k$  to  $MU$ . Here, the session key is computed as follows.

$$\begin{aligned} k &= h(h(h(h(\Phi N || ID_{MU})) || x || x_0)) \\ &= h(h(PW_{MU})) || x || x_0 \end{aligned} \quad (7)$$

5.  $MU$  computes  $k$  and obtains  $TCert_{MU}$ .  $MU$  also authenticates  $FA$  by computing  $h(x_0 || x)$  with the decrypted  $h(x_0 || x)$ . Therefore,  $MU$  can be sure that it is communicating with a legal  $FA$ .

### 2.3 Second Phase

When  $MU$  visits  $FA$  at the  $i$ -th session,  $MU$  sends the following login message to  $FA$ .

1.  $MU \rightarrow FA : TCert_{MU}, (x_i || TCert_{MU} || OtherInformation)_{k_i}$  The new  $i$ -th key  $k_i$  can be derived from the unexpired previous secret value  $x_{i-1}$  and the fixed secret value  $x$  as

$$k_i = h(h(h(h(N || ID_{MU})) || x || x_{i-1})) \quad (8)$$

where  $i = 1, \dots, n$ .

2. Upon receiving a login message from  $MU$ ,  $FA$  decrypts  $(x_i || TCert_{MU} || OtherInformation)_{k_i}$  with  $k_i$  and newly saves  $(TCert_{MU}, h(PW_{MU}), x_i)$  for the next communication.

## 3 Anonymity Problem of Kang et al.s Scheme

Kang et al. [7] improved Wu et al.'s scheme[3] and Weiet al's scheme [6] to provide anonymity. Based on the general interest of mobile users, user anonymity should be kept from any eavesdroppers including the foreign agents [5]. However, Kang et al.'s scheme still cannot provide anonymity. The main reason is that  $HA$  always computes  $r_i$  for each  $MU$  with the same secret key  $N$ . The detailed anonymity broken attack scenario is as follows.

1. Any legal user  $MU$  can directly obtain  $h(N || ID_{HA})$  from  $r_i$  in his/her smart card because  $r_i = h(N || ID_{HA})$  from the Eq.[2].
2. The legal user  $MU$  can collect the messages  $\{n', h(ID'_{MU} || x'_0 || x')_{L'}, ID_{HA}, T'_{MU}\}$  sent from any other legal mobile user  $MU'$  to  $FA$  at step [1] in the first phase (see Fig.1). From the Eqs.[1-4], we can see that  $n'$  is equal to  $h(T'_{MU} || r_1) \oplus ID_{HA} \oplus ID'_{MU}$  as follows.

$$\begin{aligned}
n' &= h(T'_{MU} \| r_1 \oplus PW'_{MU}) \\
&= h(T'_{MU} \| h(N \| ID'_{MU}) \oplus ID_{HA} \\
&\quad \oplus ID'_{MU} \oplus PW'_{MU}) \\
&= h(T'_{MU} \| r_1) \oplus h(N \| ID'_{MU} \oplus ID_{HA}) \\
&\quad \oplus ID'_{MU} \oplus h(N \| ID'_{MU}) \\
&= h(T'_{MU} \| r_1) \oplus ID_{HA} \oplus ID_{MU}
\end{aligned} \tag{9}$$

3. With obtained  $r_1 = h(N \| ID_{HA})$  and collected messages  $\{n', ID_{HA}, T'_{MU}\}$ ,  $MU$  can get the real identity  $ID'_{MU}$  of the other mobile user  $MU'$  as  $HA$  does at step [3] in the first phase as follows.

$$\begin{aligned}
ID'_{MU} &= n' \oplus (T'_{MU} \| r_1) \\
&= h(T'_{MU} \| r_1) \oplus ID_{HA} \oplus ID'_{MU} \\
&\quad \oplus ID_{HA} \oplus h(T'_{MU} \| r_1) \\
&= ID'_{MU}
\end{aligned} \tag{10}$$

As a result, legal mobile user  $MU$ 's anonymity cannot be preserved in Kang et al.'s scheme.

## 4 Conclusions

This letter demonstrated that recently published wireless authentication scheme by Kang et al.'s scheme did not solve the problem of user anonymity that was pointed out Zeng et al.[4] and Lee al.[5].

## Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2010-0010106) and partially supported by the MKE(The Ministry of Knowledge Economy),Korea under the ITRC(Information Technology Research Center) support program (NIPA-2012-H0301-12-2004) supervised by the NIPA (National IT Industry Promotion Agency).

## 参考文献

- [1] L. Ming, Y. Shucheng, R. Kui, and L. Wenjing, Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings, in: Processing of SecureComm 2010, LNICST 50, pp. 89-106, 2010.
- [2] R. Zhang, and L. Liu, Security Models and Requirements for Healthcare Application Clouds, in: Processing of Cloud 2010, pp. 268-275, 2010.

- [3] H. Lohr, A.-R. Sadeghi, and M. Winandy, Securing the e-health cloud, in: Processing of IHI 2010, pp. 220-229, 2010.
- [4] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, in: Processing of IEEE INFOCOM 2010, San Diego, CA, 14-19 March, 2010, pp. 525-533.
- [5] A. F. Barsoum, and M. A. Hasan, On Verifying Dynamic Multiple Data Copies over Cloud Servers, Cryptology ePrint Archive: Report 2011/447, <https://eprint.iacr.org/2011/447>.
- [6] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, D. Song, Remote data checking using provable data possession, ACM Trans. Inf. Syst. Security, 14 (1) (2011) 12.
- [7] Y. Zhu, H. Hu, G. J. Ahn, M. Yu, Cooperative provable data possession for integrity verification in multicloud storage, IEEE Trans. Parallel Distrib. Syst., 23 (12) (2012) 2231-2244.
- [8] A. Juels, B. S. Kaliski, PORs: proofs of retrievability for large files, in: Proceeding of ACM CCS'07, Alexandria, Virginia, USA, Oct.29-Nov.2, 2007, pp. 584-597.
- [9] H. Shacham, B. Waters, Compact proofs of retrievability, Journal of Cryptology, 26 (3) (2013) 442-483.