这是我的第一份 LaTeX 论文文档

Ruini Yang (yangruinii@foxmail.com)
Department of Communication
UESTC, Chengdu, Sichuan, 611731

2021 年 4 月 14 日

Abstract

A user identity anonymity is an important property for roaming services. In 2011, Kang et al. proposed an improved user authentication scheme that guarantees user anonymity 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 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 schemes [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.

Table 1: Notation

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
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 of A
$S_{S_A}(X)$	Signature on message X using private key of A
$h(\cdot)$	A one-way hash function
$\|\|$	Concatenation
$\oplus$	Bitwise exclusive-or operation

2.1 Initial Phase

Where 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.

$$PW_{MU} = h(N||ID_{MU}) \tag{1}$$

$$r_1 = h(N||ID_{HA}) \tag{2}$$

$$r_2 = h(N||ID_{MU}) \oplus ID_{MU} \tag{3}$$

where 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,$(h(ID_{MU})||x_0||x)_L$,ID_{HA},T_{MU}}
   If MU inputs ID_{MU} and PW_{MU} to MU's mobile device chooses secret random values x_0 and x and computes n and L as follows.

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

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

   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.

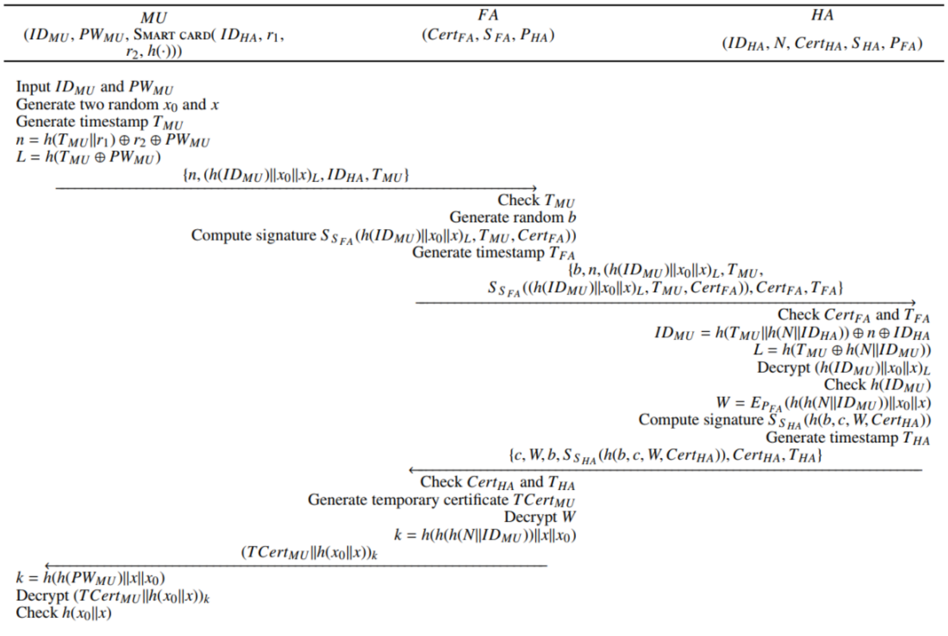

图 1: First phase of Kang et al.'s scheme.

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. $HA \rightarrow FA$: $\{c, W, b, S_{S_{HA}(h(b,c,W,Cert_{HA})),Cert_{HA},T_{HA}}\}$
   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.

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

   HA computes $L = h(T_{MU} \oplus h(N||ID_{MU}))$ with his/hersecret N and decrypts $(h(ID_{MU})||x_0||x)_L$. Then, *HA* verifies if *MU* is a legal user by checking $h(ID_{MU}) = h(ID_{MU})'$, 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 emporary 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 the 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.

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

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 Phrase

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

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

   $$k = h\left(h\left(h\left(N \| ID_{MU}\right)\right) \| x \| x_{i-1}\right) \tag{8}$$

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

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 Wei et 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 r1for 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_1 in his/her smart card because $r_1 = h(N||ID_{HA})$ from the Eq.(2)

2. The legal user *MU* can collect the messages $\{n', (h\left(ID'_{MU}\right) \| x'_0 \| x')_{L'}, ID_{HA}, T'_{MU}\}$ 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.

$$\begin{aligned} n' =& h\left(T'_{MU} \| r_1\right) \oplus r'_2 \oplus PW'_{MU} \\ =& h\left(T'_{MU} \| r_1\right) \oplus h\left(N \| ID'_{MU}\right) \oplus ID_{HA} \\ & \oplus ID'_{MU} \oplus PW'_{MU} \\ =& h\left(T'_{MU} \| r_1\right) \oplus h\left(N \| ID'_{MU}\right) \oplus ID_{HA} \\ & \oplus ID'_{MU} \oplus h\left(N \| ID'_{MU}\right) \\ =& h\left(T'_{MU} \| r_1\right) \oplus ID_{HA} \oplus ID_{MU} \end{aligned} \tag{9}$$

3. With obtained $r_1 = h(N||ID_{HA})$ and collected messages$\{n', ID_{H\Lambda}, T'_{MU}\}$,$MU$ 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.

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

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

4 Conlusions

Reference

[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.

[10] Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, Enabling public audibility and data dynamics for storage security in cloud computing, IEEE Trans. Parallel Distrib. Syst., 22 (2011) 847-859.

[11] C. Wang, S.S. Chow, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for secure cloud storage, IEEE Transactions on Computers, 62 (2013) 362-375.

[12] J. Ni, Y. Yu, Y. Mu, Q. Xia, On the security of an efficient dynamic auditing protocol in cloud storage. IEEE Transactions on Parallel and Distributed Systems. (2013) Doi: 10.1109/TPDS.2013.199.

[13] Y. Yu, L. Niu, G. Yang, Y. Mu, and W. Susilo, On the security of auditing mechanism for secure cloud storage, Further Generation Computer Systems, 30 (127-132), 2014.

[14] X. Fan, G. Yang, Y. Mu, Y. Yu, On Indistinguishability in Remote Data Integrity Checking, The Computer Journal, doi: 10.1093/comjnl/bxt13, 2013.

[15] L. Chen, S. Zhou, X. Huang, L. Xu, Data dynamics for remote data possession checking in cloud storage, Computers and Electrical Engineering, 39, pp. 2413-2424, 2014.

[16] Y. Yu, J. Ni, H. Wang, C. Xu, Improved security of a dynamic remote data possession checking protocol for cloud storage, Expert System with Applications, doi: http:// dx.doi.org/ 10.1016/j.eswa. 2014.06.027, 2014.

[17] H. Wang, Q. Wu, B. Qin, and D.-F. Josep, FRR: Fair remote retrieval of outsourced private medical records in electronic health networks, Journal of Biomedical Informatics, http://dx.doi.org/10.1016/j.jbi.2014.02.008, 2014.