An Enhanced Secure Authentication Scheme with User Anonymity in Mobile Cloud Computing

Dr. R. Madhusudhan
Associate Professor

K. S. Suvidha
Research Scholar

Department of Mathematical and Computational Sciences
National Institute of Technology Karnataka
Srinivasnagar PO, Surathkal,
Mangalore-575025

IEEE International Conference on PKI and Its Applications (PKIA-2017)
November 14-15, 2017
Hotel Chancery Pavilion, Bangalore

Security weaknesses of Lee et al.'s scheme

- Vulnerable to replay attack
- No perfect forward secrecy
- Vulnerable to impersonation attack
- Vulnerable to man in the middle attack
- No local password verification

Vulnerable to replay attack

When a legal mobile user MU sends message $M_1=\{EID', V_M, Q_M, N_M\}$ to the foreign agent FA through public channel, attacker can intercept the message M_1 if he/she has the stolen smart card personalised with the parameters {SPW, s}, then attacker can compute

$$h(ID_{MU} \oplus PW_{MU}) = EID' \oplus s$$

$EID'' = h(ID_{MU} \oplus PW_{MU}) \oplus s$. Attacker can send modified message $M'_1=\{EID'', V_M, Q_M, N_M\}$ to HA, HA without verifying computes $S = h(EID''||h(SK_{HA}))$ and session key can be revealed by an attacker by intercepting the messages $M_1=\{EID', V_M, Q_M, N_M\}$ and $M_4=\{Q_{F2}, V_{F2}, N_{F2}\}$. Session key can be computed as $K_{MF}=h(N_M|| N_{F2} || S)$. Thus the scheme is vulnerable to replay attack.

No perfect forward secrecy

By masquerading as a legal MU, attacker will be successful in getting the secret parameter s from HA. Session key is composed of $\{N_M || N_{F2} || S\}$ where N_M, N_{F2} are the random numbers selected at each authentication session. If an attacker intercepts the messages $M_1=\{EID', V_M, Q_M, N_M\}$ and $M_4=\{Q_{F2}, V_{F2}, N_{F2}\}$ transmitting on the public channel during the authentication and session key phase he/she can easily get random numbers N_M, N_{F2} and can compute

$K_{MF}= h(N_M || N_{F2} || S)$. Thus the scheme does not achieve perfect forward secrecy.

Vulnerable to impersonation attack

When a legal mobile user MU sends message M_1={EID', V_M, Q_M, N_M} to the foreign agent FA through public channel, attacker can intercept the message M_1 if he/she has the stolen smart card personalised with the parameters {SPW, s}, then attacker can compute

$$h(ID_{MU} \oplus PW_{MU}) = EID' \oplus s$$

EID"=$h(ID_{MU} \oplus PW_{MU}) \oplus s$. Attacker sends modified message M'_1={EID", V_M, Q_M, N_M} to FA. FA chooses random no. N_F and sends message M_2 = {EID', V_M, Q_M, N_M, Q_F,V_F} to HA. HA without verifying computes

$S = h(EID"||h(SK_{HA}))$. HA believes that the modified EID" comes from a legal mobile user and computes the secret value S. Thus the scheme is vulnerable to impersonation attack.

Vulnerable to man in the middle attack

Attacker who is listening to the public channel can eavesdrop the message $M_1=\{EID', V_M, Q_M, N_M\}$ transmitting on public channel during login and authentication phase, if he/she has the stolen smart card personalised with the parameters {SPW, s}, then attacker can compute

$$h(ID_{MU} \oplus PW_{MU}) = EID' \oplus s$$

$EID'' = h(ID_{MU} \oplus PW_{MU}) \oplus s$. Attacker sends the modified message $M'_1=\{EID'', V_M, Q_M, N_M\}$ to HA. HA on receiving the message M'_1 believes that the modified M'_1 comes from a legal mobile user and proceeds with further computation. Thus the scheme is vulnerable to man in the middle attack.

No local password verification

In case, if a mobile user wants to change his/her password, he/she inputs his/her ID_{MU} , PW^{old}_{MU} then smart card computes $EID=h(ID_{MU} \oplus PW^{old}_{MU}) \oplus s_{new}$ and for the new password PW^{new}_{MU}, the smart card computes

$EID_{new}=h(ID_{MU} \oplus PW^{new}_{MU}) \oplus s_{new}$. In Lee et al.'s scheme for any arbitrary password, EID_{new} is computed, no password verification is done by the smart card and $SPW_{new} = S_{new} \oplus h(PW_{MU})$ is computed. Finally smart card is updated with parameters $\{SPW_{new}, S_{new}\}$. Thus the scheme provides no local password verification.

Proposed scheme

1. Registration phase

Mobile User (MU)

Home Agent (HA)

Step1: MU chooses his/her identity and password [ID_{MU} , PW_{MU}] of his/her choice and nonce M

$\{ID_{MU}, PW_{MU}, M\}$ →

Step 2: HA computes $f=h(ID_{MU} || x)$, where x is a long term secret key of HA.

$S = h(h(ID_{MU} || PW_{MU}) \oplus M \oplus PW_{MU})$.

HA stores $h(PW_{MU} || M)$ in its database

Proposed scheme contd...

1. Registration phase

Mobile User (MU)

Home Agent (HA)

Smart card personalised with parameters $\{S, M, f, ID_{HA}, h(.)\}$

Step 3: MU computes $f^* = f \oplus h(PW_{MU} \| M)$. Finally MU stores $\{S, M, f^*, ID_{HA}, h(.)\}$ in the smart card

Proposed scheme contd....

2. Login and authentication phase

Mobile User (MU)

Foreign Agent (FA)

Step 1: MU enters [ID_{MU} , PW_{MU}]
smartcard Computes
$S^* = h(h(ID_{MU} \| PW_{MU}) \oplus M \oplus PW_{MU})$ verifies $S^* = S$ or not , if true smart card generates random number r, r_{new} and computes
$SID = f^* \oplus r$
$V = SID \oplus h(f^* \| r_{new})$.

$M_1 = \{V, r_{new}, ID_{HA}\}$ →

Proposed scheme contd....

2. Login and authentication phase

Foreign Agent (FA)

Home Agent (HA)

Step 2: FA generates random number d and computes

$Q=d \oplus h(r_{new} || SK_{fh})$

$T=Q \oplus h(r_{new} || Sk_{fh} || ID_{HA})$.

$M_2=\{T, V, r_{new}, ID_{HA}\}$ →

Step 3: HA computes

$SID= V \oplus h(f \oplus h(PW_{MU} || M) || r_{new})$

$V^*=SID \oplus h(f \oplus h(PW_{MU} || M) || r_{new})$

HA verifies whether $V^*=?V$. If true, HA computes

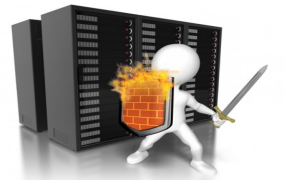
$Q=T \oplus h(r_{new} || Sk_{fh} || ID_{HA})$

$d=Q \oplus h(r_{new} || Sk_{fh})$

$B=h(d || Sk_{fh} || ID_{FA}) \oplus ID_{HA}$

Proposed scheme contd....

2. Login and authentication phase



Foreign Agent (FA)

Home Agent (HA)

Step 4: FA computes
$B^*=h(d \,||\, Sk_{fh} \,||\, ID_{FA}) \oplus ID_{HA}$
verifies if B*=?B. If true, FA chooses random number N_F and computes
$C = h(V \,||\, r_{new}) \oplus N_F$
$C^* = h(V \,||\, r_{new}) \oplus N_F$.

M3 = {B}

Proposed scheme contd....

2. Login and authentication phase

$M_4 = \{C\}$

Step 5 : MU computes
$N_F = C \oplus h(V \| r_{new})$
$C^* = h(V \| r_{new}) \oplus N_F$ verifies if $C^* = ?C$. If true, MU selects random no. N_M and computes
$F = h(N_F \| V) \oplus N_M$
$sk = h(N_F \| N_M \| V)$

Proposed scheme contd....

2. Login and authentication phase

Mobile User (MU)

Foreign Agent (FA)

$M_5=\{F, V\}$

Step 6 : MU computes
$N_M = F \oplus h(V \| N_F)$
$F^* = h(V \| N_F) \oplus N_M$
Verifies if $F^* = ?F$. If true, FA computes
$sk=h(N_F \| N_M \| V)$

Proposed scheme contd....

3. Password change phase

Mobile User (MU)

MU inserts smart card into the card reader and submits his/her identity ID_{MU} and old password PW^{old}_{MU} , then smart card computes $S' = h(h(ID_{MU} || PW^{old}_{MU}) \oplus M \oplus PW^{old}_{MU})$, verifies if $S' = S$. If true, smart card allows user to update old password PW^{old}_{MU} with the new password Pw^{new}_{MU} . Smart card computes $S^* = h(h(ID_{MU} || PW^{new}_{MU}) \oplus M \oplus PW^{new}_{MU})$. Finally S is replaced with S* in the smart card.

Security analysis.

- Security against replay attack
- Perfect forward secrecy
- Security against man in the middle attack
- Security against impersonation attack
- User anonymity is protected
- Local password verification

Security against replay attack

In case if an attacker, who is listening to the public channel eavesdrop the message $M_1=\{V, r_{new}, ID_{HA}\}$ transmitting during login and authentication phase and after learning about the random number pattern, if he/she injects his/her own random number r'_{new} in the message $M'_1=\{V, r'_{new}, ID_{HA}\}$ and sends the modified message M'_1 to FA. FA sends to HA. HA on receiving the message M'_1 will compute $SID = V \oplus h(f \oplus h(PW_{MU} || M) ||r'_{new})$. Verifies if $V=?\ SID \oplus h(f \oplus h(PW_{MU} || M) ||r'_{new})$. Which is certainly not true, hence HA terminates the request made by the MU. Thus the proposed scheme provides security against replay attack.

Perfect forward secrecy

In the proposed scheme session key sk is computed as $sk = h(N_M||N_F||V)$. Though the parameter V is available in the messages $M_1=\{V, r_{new}, ID_{HA}\}$ and $M_2=\{T, V, r_{new}, ID_{HA}\}$ that are transmitting on the public channel during login and authentication phase which can be eavesdropped by an attacker easily, with the parameter of V attacker will not be able to arrive at the value of session key as the session key sk is compromised of two random numbers N_M and N_F of MU and FA respectively and these random numbers are kept confidential during the message transmission on the public channel. Thus the proposed scheme achieves perfect forward secrecy.

Security against man in the middle attack

In case if an attacker gets the stolen smart card personalised with the parameters $\{S, M, f^*, ID_{HA}, h(.)\}$ and listens to the communication channel to intercept the messages $M_1=\{V, r_{new}, ID_{HA}\}$ and $M_2=\{T, V, r_{new}, ID_{HA}\}$. Even then an attacker will fail to compute the following.

$SID= V \oplus h(f \oplus h(PW_{MU} || M) || r_{new})$

$Q=T \oplus h(r_{new} || Sk_{fh} || ID_{HA})$

$d=Q \oplus h(r_{new} || Sk_{fh})$. Thus the proposed scheme provides security against man in the middle attack.

Security against impersonation attack

- Impersonate as MU

In the proposed scheme, during login and authentication phase MU sends message $M_1=\{V, r_{new}, ID_{HA}\}$ to FA. FA sends message $M_2=\{T, V, r_{new}, ID_{HA}\}$ to HA. HA computes the following

$SID= V \oplus h(f \oplus h(PW_{MU} || M) || r_{new})$. Verifies if

$V^*=?$ $SID \oplus h(f \oplus h(PW_{MU} || M) || r_{new})$. HA verifies if $V^*=?V$. If true, HA accepts. Otherwise HA terminates the request.

Security against impersonation attack contd...

- Impersonate as FA

FA sends message $M_2=\{T, V, r_{new}, ID_{HA}\}$ to HA. If an attacker intercepts this message and sends to HA. HA will compute the following

$Q=T \oplus h(r_{new} || Sk_{fh} || ID_{HA})$

$d=Q \oplus h(r_{new} || Sk_{fh})$.

If an attacker tries to impersonate as FA, it is difficult for him/her to know the secret key SK_{fh} which is shared between FA and HA. Due to the complexity of Diffie-Hellman key exchange protocol, attacker will not be successful in impersonating as a FA. Thus the proposed scheme provides security against impersonation attack.

User anonymity is protected.

In case of stolen smart card attack, if an attacker tries to compute ID_{MU} with the smart card parameters {S, M, f*, ID_{HA}, h(.)} where
$S = h(h(ID_{MU} || PW_{MU}) \oplus M \oplus PW_{MU})$. Then he/she will not be successful in revealing the identity of the user since the ID_{MU} is concatenated with the PW_{MU} and guessing two unknown parameters at the same time is difficult. Thus the proposed scheme protects user anonymity.

Local password verification

MU inserts smart card into the card reader and submits his/her identity ID_{MU} and old password PW^{old}_{MU} , then smart card computes $S' = h(h(ID_{MU} || PW^{old}_{MU}) \oplus M \oplus PW^{old}_{MU})$, verifies if $S'^* = S$. If true, smart card allows user to update old password PW^{old}_{MU} with the new password Pw^{new}_{MU} . Smart card computes $S^* = h(h(ID_{MU} || PW^{new}_{MU}) \oplus M \oplus PW^{new}_{MU})$. Finally S is replaced with S* in the smart card. Thus the proposed scheme provides local password verification.

Performance comparison

Phase	Fan wu et al.'s scheme	Lee et al.'s scheme	Proposed scheme
Registration phase(MU)	$2T_h+1T_{\oplus}+2T_{\|\|}$	$2T_h+3T_{\oplus}$	$1T_h+1T_{\oplus}+1T_{\|\|}$
Registration phase(HA)	$3T_h+2T_{\oplus}+4T_{\|\|}$	$2T_h+1T_{\|\|}$	$2T_h+2T_{\oplus}+2T_{\|\|}$
Login and authentication phase (MU)	$10T_h+8T_{\oplus}+21T_{\|\|}$	$10T_h+8T_{\oplus}+8T_{\|\|}$	$7T_h+7T_{\oplus}+7T_{\|\|}$
Login and authentication phase (FA)	$5T_h+1T_{\oplus}+16T_{\|\|}$	$8T_h+3T_{\oplus}+9T_{\|\|}$	$6T_h+5T_{\oplus}+9T_{\|\|}$
Login and authentication phase (HA)	$11T_h+5T_{\oplus}+31T_{\|\|}$	$8T_h+4T_{\oplus}+10T_{\|\|}$	$7T_h+7T_{\oplus}+9T_{\|\|}$

Conclusion

- The proposed work emphasizes on the need of secure authentication in mobile cloud computing.
- We have analysed Lee et al.'s scheme thoroughly and some of the weaknesses of the their scheme is highlighted.
- In order to remove the security weaknesses of Lee et al.'s scheme and to achieve the security goals, a new scheme is proposed.
- The proposed scheme eliminates all the security attacks made in Lee et al.'s scheme. Further, mutual authentication between FA and HA in the proposed scheme is achieved based on their secret keys exchanged with each other.
- FA and HA uses this secret key to provide communication security on the public channel.

References

[1] C. Chen, D. He, S. Chan, J. Bu, Y. Gao, and R. Fan, “Lightweight and provably secure user authentication with anonymity for the global mobility network,” International Journal of Communication Systems, vol. 24, no. 3, pp. 347–362, 2011.

[2] T.-H. Chen, H.-I. Yeh, and W.-K. Shih, “An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing,” in Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on. IEEE, 2011, pp. 155–159.

[3] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, “A strong user authentication framework for cloud computing,” in Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific. IEEE, 2011, pp. 110–115.

[4] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, and R. Baliyan, “A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks,” Security and Communication Networks, vol. 9, no. 16, pp. 3527–3542, 2016.

[5] C.-C. Lee, Y.-M. Lai, C.-T. Chen, and S.-D. Chen, “Advanced secure anonymous authentication scheme for roaming service in global mobility networks,” Wireless Personal Communications, pp. 1–16.

CCA

IEEE

PKIA-2017

Questions?

सी डैक
CDAC

CCA

IEEE

PKIA-2017

Thank You

सी डैक
CDAC