ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2015, T. 44, Nr. 3

Security Weaknesses on a Delegation-Based Authentication Protocol for PCSs

Prosanta Gope, Tzonelih Hwang

Department of Computer Science and Information Engineering
National Cheng Kung University, Tainan, Taiwan, R.O.C.
e-mail: prosanta.nitdgp@gmail.com, hwangtl@ismail.csie.ncku.edu.tw

crossref http://dx.doi.org/10.5755/j01.itc.44.3.9777

Abstract. Rapid development of wireless networks brings about many security problems in Portable Communication Systems (PCS), which can provide mobile users with an opportunity to enjoy global roaming services. In this regard, designing a secure user authentication scheme, especially for recognizing legal roaming users is indeed a challenging task. Recently, C-C Lee et al. proposed such scheme, which is claimed to be an improvement of T. F. Lee et al.'s protocol. However, in this article, we reveal that the scheme proposed by C-C Lee et al. still suffers from certain weaknesses like vulnerability to DoS attack, no perfect forward secrecy, loss of untraceability, etc. Hence, C-C Lee et al.'s delegation-based protocol cannot guarantee secure communication for PCS environment.

Keywords: Delegation-based authentication; DoS attack; Untraceability.

1. Introduction

Portable Communication Systems (PCS) provide roaming services among wireless communication networks [1-4]. In this regard, a mobile user (MU) at first registers his/her legality in some home location register (HLR). Before, roaming MU logins some visiting location register (VLR) and VLR validates the user's legality with the help of the HLR. If the MU is legal of some HLR, VLR offers services and charges the roaming fee. In recent years, many protocols used the public-key systems to provide the privacy of the MU. In 2005, Lee and Yeh [5] proposed a new delegationbased authentication protocol for PCSs. Their protocol is also based on the public-key cryptosystems to provide user anonymity, non-repudiation, mutual authentication. Moreover, their protocol used off-line authentication process to reduce the communication overhead between the VLR and HLR and mobile users'. However, T. F. Lee et al. [6] pointed out that Lee and Yeh's off-line authentication process is vulnerable to masquerade user attacks. To overcome this flaw, T. F. Lee et al. proposed an enhanced protocol. Unfortunately, Youn and Lim [7], and Wang et al. [8] pointed out that T. F. Lee et al.'s protocol suffers from linkable problem. Independently, C-C Lee et al. [9] thoroughly investigated T. F. Lee et al.'s protocol. Subsequently, they pointed out that apart from linkable problem T. F. Lee et al.'s protocol also cannot achieve the forward secrecy property, and because of that once the session key is disclosed in an off-line authentication, the adversary can obtain the next session key. In order to resolve this problem they proposed an improved protocol. However, in this article, we show that the scheme proposed by C-C Lee et al. has some serious weaknesses which have been overlooked during design. So, the contribution of this article is to disclose the weaknesses of the C-C Lee et al.'s scheme, which have not been revealed yet.

Therefore, the remainder of this article is organized as follows. Section 2 reviews the protocol of [9] whose weaknesses are pinpointed in Section 3. Finally, a concluding remark is given in Section 4. The abbreviations and cryptographic functions used in this article are defined in Table 1.

2. Review of C-C Lee et al.'s Delegation-Based Authentication Protocol

In this section, we will review C-C Lee et al.'s delegation-based authentication protocol [9]. Their scheme is divided into three phases: the setup phase, the on-line authentication phase, and the off-line authentication phase. In the setup phase, MU registers with the HLR and obtains a SIM card through a secure channel. In the on-line authentication phase, when MU roams in a new VLR, the VLR authenticates the identity of the MU with the help of HLR. Finally, in the off-line authentication phase, the VLR can authenticate the MU without interacting with HLR. The

details of the phases are described in the following sub-sections.

Table 1. Notation and Abbreviations

Symbol	Definition
MU	Mobile User
VLR	Visited Location Register
HLR	Home Location Register
K_{vh}	Secret Key between the VLR and HLR
ID_H	Identity of the HLR
ID_V	Identity of the VLR
SK	Session key between VLR and MU
p	A large prime
q	A prime factor of p-1
g	A generator in group Z_p^*
$[M]E_K$	Encryption of a message M using secret key K
$h(.)$	One-way hash function
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation

2.1. Phase I: Setup Phase

The HLR computes its public key $v = g^x \bmod p$, where x is the HLR's private key. When MU sends requests to the HLR for registration, then the HLR computes the MU's public key $K = g^k \bmod p$ and the private key $\sigma = x + kK (\text{mod } p)$ and subsequently decides an initialized temporary identity T_{ID}, where k is the random number generated by the HLR. Afterwards, the HLR personalizes the SIM card with (σ, K) and T_{ID} and issues it to MU. Upon receiving the SIM card, MU generates a nonce $n1$, and pre-computes a hash chain $h^{(1)}(n1), h^{(2)}(n1), ..., h^{(n+1)}(n1)$ and stores them in its database, where $h^{(1)}(n1) = h(n1)$ and $h^{(i+1)}(n1) = h(h^{(i)}(n1))$ for $i = 1, 2, ..., n$.

2.2. Phase II: On-line Authentication Phase

Step 1. M_1: MU $\rightarrow$ VLR : $\{T_{ID}\}$

The MU acquires the initialized temporary identity T_{ID} from the SIM card and then sends it to VLR.

Step 2. M_2 : VLR $\rightarrow$ MU : $\{n2, ID_V\}$

After receiving M_1 from the MU, the VLR generates a random number *n2* and responses *n2*, and ID_V to MU.

Step 3. M_3 : MU $\rightarrow$ VLR : $\{r, s, T_{ID}, N_1, ID_H, ID_V\}$

Upon receiving the message M_2, MU computes $r = g^t \bmod p$ and picks T_{ID}, N_1 from his/her database to compute $s = \sigma.h(N_1 \| n2 \| ID_V) + t.r (\text{mod p})$, where t is a random number and $N_1 = h^{(n+1)}(n1)$. Finally, MU forms a response message M_3 and sends it to VLR.

Step 4. M_4 : VLR $\rightarrow$ HLR : $\{[N_1 \| n2 \| T_{ID}]E_{K_{vh}}, ID_H, ID_V\}$

After receiving the message M_3, the VLR acquires K by checking T_{ID} from his/her database. It is assumed that the VLR maintains a table mapping between the public key K and the corresponding initial temporary identity T_{ID}. Then the VLR computes g^s and $(vK^K)^{h(N1\|n2\|ID_V)} r^r (\text{mod } p)$. If they are same, that means the VLR successfully authenticated the MU and then VLR forms a request message M_4 and sends it to the HLR. Otherwise, the VLR rejects the MU's request.

Step 5. M_5 : HLR $\rightarrow$ VLR : $\{[[N_1, n2, ID_V, T_{IDnew}]E_\sigma \| n2 \| l \| C_1 \| T_{IDnew}]E_{K_{vh}}, ID_H, ID_V\}$

Upon receiving the request message M_4 from the VLR, the HLR decrypts $[N_1 \| n2 \| T_{ID}]E_{K_{vh}}$ and obtains T_{ID}. Subsequently, the system (HLR) finds σ from its database according to T_{ID}. If it is not found, then the HLR rejects the VLR request. Otherwise, the HLR generates a random number *n3*, and then computes $C_1 = h(N_1 \| n2 \| n3 \| \sigma)$ and $l = N_1$. Hereafter, the HLR further generates a temporary identity T_{IDnew} and forms a response message M_5 and sends it to the VLR, where K_{vh} denotes the long-term shared secret key between VLR and HLR.

Step 6. M_6 : VLR $\rightarrow$ MU : $\{[N_1, n3, ID_V, T_{IDnew}]E_\sigma, ID_V\}$

After receiving the message M_5 from HLR, the VLR decrypts the message and subsequently obtains $[N_1, n3, ID_V, T_{IDnew}]E_\sigma$, *n2*, *l*, C_1, T_{IDnew}. Then the VLR checks *n2* and *l* and sets C_1 as the current session key *SK*. Finally, the VLR replaces T_{ID} with T_{IDnew} in its database and subsequently forwards the $[N_1, n3, ID_V, T_{IDnew}]E_\sigma$ to the MU.

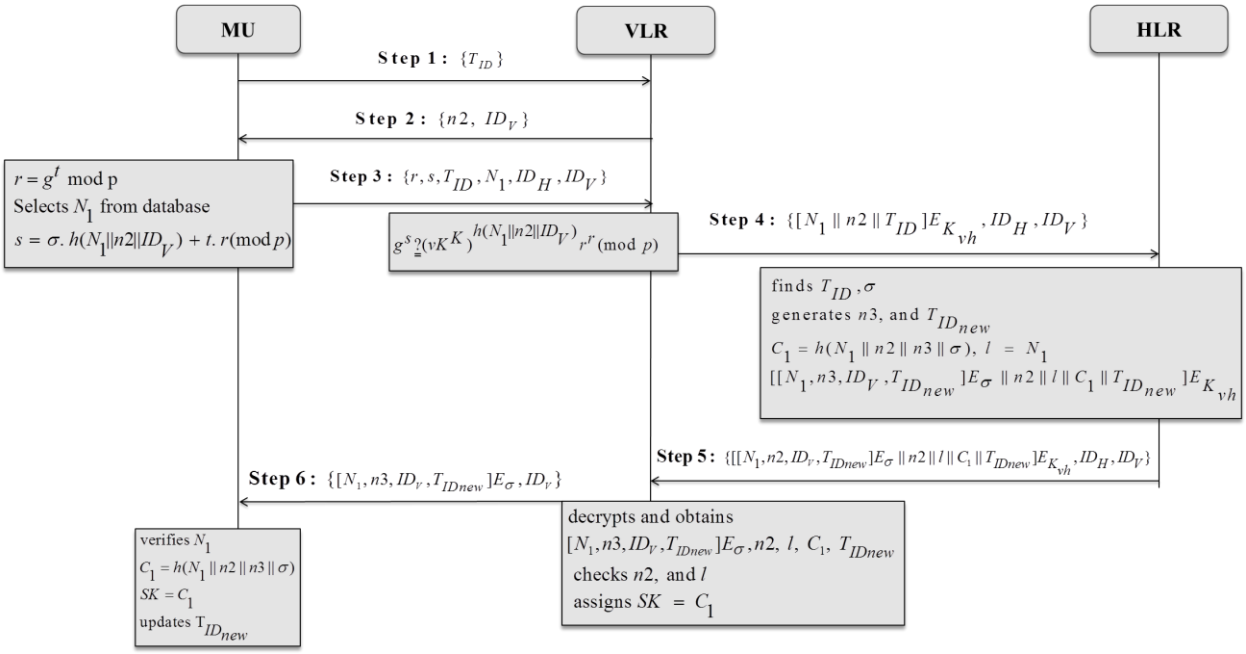

Figure 1. The on-line authentication process of the C-C Lee et al.'s protocol

Upon receiving the message M_6 from VLR, MU at first decrypts the message and checks whether N_1 is the same as previously sent in Step 3. If so, then MU successfully authenticates the VLR and computes $C_1 = h(N_1 \| n2 \| n3 \| \sigma)$ as the current session key and updates his/her database for next communication. Otherwise, MU terminates the connection and starts with a new request. Details of this phase are shown in Fig. 1.

2.3. Phase III: *Off-line Authentication Phase*

$$\text{MU} \rightarrow \text{VLR} : [h^{(n-i+1)}(n1) \oplus T_{IDnew}]E_{C_i}$$

MU picks $h^{(n-i+1)}(n1)$ and T_{IDnew} stored in his/her database and sends $[h^{(n-i+1)}(n1) \oplus T_{IDnew}]E_{C_i}$ to the VLR . After receiving these messages from the MU, the VLR obtains $h^{(n-i+1)}(n1)$ by using the session key T_{IDnew}. Subsequently, the VLR checks whether $h^{(n-i+1)}(n1)$ is the same as l or not. If so, then the VLR updates $l = h^{(n-i+1)}(n1)$ and $i = i+1$, where the count $i \le n$. The VLR computes the session key $C_{i+1} = h(l, C_i)$ and randomly decides a new temporary identity T_{IDnew^i} and updates the verification table. Afterwards, the VLR sends $[T_{IDnew^i} \oplus T_{IDnew}]E_{C_{i+1}}$ to MU and sends $[T_{IDnew^i}]E_{K_{vh}}$ to HLR. Upon receiving these messages, the MU obtains T_{IDnew^i} and updates the SIM card for next communication process. Similarly, after receiving $[T_{IDnew^i}]E_{K_{vh}}$ from VLR HLR decrypts the message and subsequently, updates its database with the new temporary identity.

3. Security weaknesses in the C-C Lee et al.'s delegation-based authentication protocol

In this section, we present several weaknesses of the C-C Lee et al.'s protocol, which certainly cause an insecure wireless communication system.

3.1. Vulnerable to DoS Attacks

DoS attack [10,11] is an imperative concern, which may occur because of the loss of synchronization between MU and HA. That can be comprehended if the last authentic response message sent by VLR has been interrupted by an adversary, so that MU cannot receive the message within a specific time period. Unfortunately, C-C Lee et al.'s protocol cannot resist DoS attack, where if an adversary interrupts the response message M_6 then MU cannot receive $[N_1, n3, ID_V, T_{IDnew}]E_\sigma, ID_V$. In that case, both the HLR and VLR may update their databases with T_{IDnew} but MU cannot. Now, if the MU attempts to execute the "*On-line Authentication Phase"* with the old T_{ID} then the HLR will not comprehend that. On the other hand, because of the interruption of the message M_6 , MU cannot even acquire the random number *n3* and without *n3*, it is not possible for MU to

compute the session key $SK = C_1 = h(N_1 \| n2 \| n3 \| \sigma)$. Therefore, without having session key and the temporary id T_{IDnew}, the MU cannot even execute the "*Off-line Authentication Phase"*.

3.2. Loss of Untraceability

An orthogonal security arising as a result of mobility is the confidentiality of the mobile subscriber's any identity and movements. For obvious reasons, it is desirable to keep this information secret. In other words, passive eavesdroppers and active intruders should not be able to identify or keep track the user. In fact, it can be argued that even the visited locations (VLRs) should not be privy to know any identification of the user. Unfortunately, in Step 5 of the C-C Lee et al.'s protocol, the VLR receives the MU's latest temporary identity T_{IDnew} from HLR. Now, if the MU moves to a new VLR, the old VLR can still track him/her. In this way, the protocol cannot maintain the domain separation [3, 4, 12, 13, 14, 15] that means conspiracy of the all visited domains may cause to identify the movement of the user. Therefore, C-C Lee et al.'s protocol cannot ensure the untraceability property, which is greatly important for the privacy of the mobile user.

3.3. No Perfect Forward Secrecy

Perfect forward secrecy [13] is a form of security requirements in network systems. In general, a protocol that provides perfect forward secrecy (PFS) can resist an adversary from learning any previous session key, especially when the long term secret keying material is compromised by the adversary. However, we found that C-C Lee et al.'s protocol for PCSs fails to provide PFS. In the C-C Lee et al.'s delegation-based protocol, once the secret key pair (K, σ) is disclosed, then all the previous session keys established based on the execution "*On-line Authentication Phase"* will be exposed. Precisely, an adversary can learn the previous session key if the home agent is compromised by the adversary. So that, the adversary may acquire secret key pair (K, σ) and/or the shared secret key K_{vh}. Therefore, the session key in this scheme is not secure. In fact, Lee and Yeh's scheme [5] and T. F. Lee et al.'s scheme [6] also cannot ensure PFS.

3.4. Vulnerable to Side Channel Attacks

In practice, it is possible to read some sensitive information from SIM card by executing the side channel attacks [13, 17], and the information can be used for breaking the whole system. Hence, it is highly desirable to use countermeasures for securing the secret values stored in SIM card. However, sometimes, developers do not use countermeasures due to expensive production cost. In this regard, the best alternative plan is to ensure the security of unspoiled SIM cards by restricting the damage caused by the revelation of sensitive information. Unfortunately, the C-C Lee et al.'s delegation-based protocol can be entirely broken, since an adversary always can recover the key pair (σ, K), the latest temporary identity of the MU i.e. T_{IDnew}, and even the latest hash chain values with the session key C_i from the SIM card. Once the adversary obtains these parameters, then he/she can easily impersonate as MU, which is a serious threat against the privacy of the mobile user. Similar problem can also be found in [5-9].

4. Conclusion

In this article, we have demonstrated that the C-C Lee et al.'s delegation-based protocol fails to ensure several security properties like perfect forward secrecy, resistance to DoS and side-channel-attacks. In addition to that, the protocol also cannot provide untraceability, where a VLR can still trace the MU, even if the MU moves to a new VLR. Therefore, the C-C Lee et al.'s delegation-based protocol fails to guarantee the privacy of the mobile user, which is greatly desirable in PCS.

Acknowledgments

This work is financially supported by the Ministry of Science and Technology, under Contract No. MOST 103-2221-E-006-177-. The authors would like to thank the Ministry of Science and Technology, Taiwan for their benign supports. The authors also would like to thank the anonymous referee for his/her valuable suggestions.

References

[1] **C. C. Lee, I. E. Liao, M. S. Hwang.** An efficient authentication protocol for mobile communication. *Telecommunication Systems*, 2011, Vol. 46, No. 1, 31–44.

[2] **C. C. Lee, M. S. Hwang, W. P. Yang.** Extension of authentication protocol for GSM. *IEE Proceedings-Communications*, 2003, Vol. 150, No. 2, 91-95.

[3] **T. Hwang, P. Gope.** Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time Secrets. *Wireless Personal Communications*, 2014, Vol. 77, No. 1, 197-224.

[4] **P. Gope, T. Hwang.** Enhanced secure mutual authentication, and key agreement scheme preserving user anonymity in global mobile networks. *Wireless Personal Communications*, 2015, Vol. 82, No. 4, 2231-2245.

[5] **W. B. Lee, C. K. Yeh.** A new delegation-based authentication protocol for use in portable communication systems. *IEEE Transactions on Wireless Communications*, 2005, Vol. 4, No. 1, 57-64. http://dx.doi.org/10.1109/TWC.2004.840220.

[6] **T. F. Lee, S. H. Chang, T. Hwang, S. K. Chong.** Enhanced delegation-based authentication protocol

for PCSs. *IEEE Transactions on Wireless Communications*, 2009, Vol. 8, No. 5, 2166-2171. http://dx.doi.org/10.1109/TWC.2009.070032.

[7] **T.-Y Youn, J. Lim**. Improved delegation-based authentication protocol for secure roaming service with unlinkability. *IEEE Communications Letters*, 2011, Vol. 14, No. 9, 791-793.

[8] **R.-C Wang, W.-S Juang, C. L. Lei.** A privacy and delegation-enhanced user authentication protocol for portable communication systems. *International Journal of AdHoc and Ubiquitous Computing*, 2011, Vol. 6, No. 3, 183-190.

[9] **C. C. Lee, R. X. Chang, T. Y. Chen, L. A. Chen**. An improved delegation-based authentication protocol for PCSs. *Information Technology and Control*, 2012, Vol. 41, No. 3, 258-267.

[10] **C. H. Wang, C. Y. Lin.** An efficient delegation-based roaming payment, protocol against denial of service attacks. In: *Proc. 2011 International Conference on Electronics, Communications and Control*, 2011, pp. 4136–4140.

[11] **J. L. Tsai, N. W. Lo, T. C. Wu.** Secure delegation-based authentication protocol for wireless roaming service. *IEEE Communications Letters*, 2012, Vol. 16, No. 7, 1100-1102.

[12] **A. Herzberg, H. Krawczyk, G. Tsudik.** On travelling incognito. *IEEE Workshop on Mobile Computing Systems and Applications*, 1994, pp. 205-211.

[13] **P. Gope, T. Hwang.** Lightweight and Energy Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks. *IEEE Systems Journal*, 2015 DOI: 10.1109/JSYST.2015.2416396.

[14] **P. Gope, T. Hwang**. Untraceable Sensor Movement in Distributed IoT Infrastructure. *IEEE Sensors Journal*, Vol. 15, No. 9, pp. 5340–5348, 2015, DOI: 10.1109/JSEN.2015.2441113.

[15] **P. Gope, T. Hwang.** A Realistic Lightweight Authentication Protocol Preserving Strong Anonymity for Securing RFID System. *Computers & Security*, 2015, DOI: 10.1016/j.cose.2015.05.004.

[16] **W. Diffie, P. C. van Oorshot, M. J. Wiener.** Authentication and Authenticated Key Exchanges. *Designs, Codes and Cryptography*, V.2, Kluwer Academic Publishers, 1992, pp. 107-125.

[17] **P. Kocher, J. Jaffe, B. Jun.** Differential power analysis. In: *Proc. CRYPTO'99*, 1999, LNCS 1666, pp. 388-397, Springer-Verlag.

Received February, 2015.