Further Improvement on A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments*

Chun-Ta Li† Min-Shiang Hwang‡ Yen-Ping Chu§

Department of Management Information Systems‡
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Email: mshwang@nchu.edu.tw
Fax: 886-4-22857173

Department of Computer Science and Engineering†
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.

Department of Computer Science and Information Engineering§
Tunghai University
181 Section 3, Taichung Harbor Road, Taichung, Taiwan 407, R.O.C.

October 31, 2012

*This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grants NSC 95-2218-E-001-001, and NSC95-2218-E-011-015.

‡Responsible for correspondence: Prof. Min-Shiang Hwang

Further Improvement on A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments

Abstract

Privacy and authentication are very important concepts and service levels to anonymous communications and data confidentiality. Recently, Ren et al. proposed an authentication and access control scheme for preserving privacy in PCEs (Pervasive Computing Environments). However, in this paper, it is demonstrated that the so-called secure, privacy preserving authentication and access control scheme proposed by Ren et al. is vulnerable to service abuse attacks and, as a result, illegitimate users can freely access the service through the service provider without any worries and this flaw would lead to a serious accounting problem with their scheme. Therefore, we proposed a security improvement to their scheme to neutralize this weakness and an efficiency improvement to enhance the performance of their scheme in the user operational phase. More importantly, a new improved proposal for a scheme can still allow the mobile user to anonymously interact with the service provider in a PCE is demonstrated.

Keywords: Access control; Authentication; Privacy; Pervasive Computing Environment; Security

1 Introduction

In today's pervasive computing environments (PCEs), people are increasingly surrounded by interconnected personal devices and the ancillary abundant services that are pervasive, and affect their lives in multifarious aspects, from the personal to the home, offices, commuting, schools, public places and so on. On the other hand, in such open networking environments, privacy and security are important issues and it becomes necessary to provide secure communications over insecure communication channels [2, 4, 9, 10], especially in privacy-essential and confidential environments.

Recently, Ren et al. proposed an authentication and access control scheme for preserving privacy in pervasive computing environments [7], the scheme integrates the concept of blind signatures [3] and hash chain cryptographic techniques [6, 8] while providing such advantages as anonymous, non-linkability, establishing session-keys establishment, and mutual authentication between a mobile user and a service provider. Their scheme has a great impact upon the related area in PCEs and it is the first attempt to provide a secure communications model with mutual authentication, key establishment protocol, and privacy preserving access control to differentiated services in pervasive computing environments. Moreover, the performance of their scheme is extremely efficient than [5] in terms of communication loads, computation loads, and storage loads. However, we find that Ren et al. scheme is vulnerable to the abusive attacks because of not authenticating the credentials and anyone can fabricate an invalid credential with a valid certificate to access the service without limits, which terms are even not available to a valid mobile user whose access can be denied. The above-mentioned weakness of Ren et al. scheme will be explained in Section 3. Inevitably, as a result there would be a serious accounting problem with their scheme and this paper further proposes an improvement to neutralize this security flaw. In addition, this paper will offer a minor revision of their scheme to enhance the efficiency of procedures involved, which can be practically applied within the PCEs.

The rest of this paper is organized as follows. Ren et al. scheme will be reviewed in Section 2. The weaknesses of their scheme are introduced in Section 3. In Section 4, an improvement is proposed to repair the security flaw. Conclusions are presented in Section 5.

Table 1: Notations

U, S, P	A mobile user, service provider, and a service access point.
SID	A service type identifier.
(PK_i, SK_i)	A public key and private key of entity i.
M_i	The receipt of the service access for a user i to register himself as a legal user of destined service that S provides.
$H(.)$	A collision-free and public one-way hash function.
$K_{i,j}$	The shared secret key between entities i and j.
r_i	A nonce, which entity i generates.
$CertI$	A certificate of entity I.
$H^j(m)$	A hash chain, which hash message m j times, $j \leq n$, with length n.
$H_{K_{i,j}}(m)$	A Message Authentication Code (MAC), which is the message digest of message m with key $K_{i,j}$.
$E_K[.]$	The symmetric encryption function with key K.
$D_K[.]$	The symmetric decryption function with key K.
$E_{PK_i}\{.\}$	The asymmetric encryption function with entity i's PK_i.
$D_{SK_i}\{.\}$	The asymmetric decryption function with entity i's SK_i.

2 Review of Ren et al. Scheme

In this section, we briefly review Ren et al. scheme. The security flaw of their scheme is introduced in next section. Some notations used in [7] and this paper are defined in Table 1. Their scheme consists of two protocols, namely: user authorization protocol and user operational protocol. In addition, there are three types of participants in it, namely: mobile users, services, and back-end service providers, respectively. The detailed steps of the two protocols are briefly described in the following subsections.

2.1 User Authorization Protocol

The user authorization protocol consists of two phases, namely: credential generation phase and credential authorization phase, respectively. In credential generation, a mobile user U first generates two nonces r_{u_1} and r_{u_2} and signs its own ID with nonce r_{u_2} by computing $A = E_{SK_U}\{U, r_{u_2}\}$. Then, U computes the value $C^0 = H(r_{u_2}, U, A)$ and the credential chain $C^n = H^n(C^0)$, with length n. Finally, U blinds C^n as $B = E_{PK_{SID}}\{r_{u_1}\} * C^n$ and sends $(U, B, CertU, SID)$ to the service provider S for credential authorization.

In the credential authorization stage, S first verifies the validity of $CertU$, and if it holds, S signs B by computing $C = E_{SK_{SID}}\{B\} = r_{u_1} * E_{SK_{SID}}\{C^n\}$ and sends C to U. If an attacker who eavesdrops on the blinded credential and signature C in transit, he/she still cannot use C to obtain some service from S because it is protected by the blind factor r_{u_1}. Then, U unblinds r_{u_1} by computing $D = C/r_{u_1} = E_{SK_{SID}}\{C^n\}$ and checks the authenticity of D by verifying whether $C^n = D_{PK_{SID}}\{D\}$ holds or not. If it holds, U obtains an authorized credential C^n and its signature D.

2.2 User Operational Protocol

When a mobile user U wants to anonymously access the service from the service provider S through a service access point P, U first generates a nonce r_{u_3} and sends an access request $E = (SID, E_{PK_S}\{r_{u_3}, C^n, D\})$ to P. Then, P forwards E to S through a secret tunnel. Noted that a previously established secure tunnel exists between P and S. Upon receiving the access request message, S can use its private key SK_S to decrypt $E_{PK_S}\{r_{u_3}, C^n, D\}$ by computing $D_{SK_S}\{E_{PK_S}\{r_{u_3}, C^n, D\}\}$ and verify whether $C^n = D_{PK_{SID}}\{D\}$ holds or not. If it holds, S stores C^n in its data base, and sends an access acknowledgement (r_{u_3}, C^n) to P through a secure tunnel; otherwise, it is dropped and stopped.

Upon receiving an acknowledgement of access (r_{u_3}, C^n) from S, P generates a nonce r_{p_1}, computes $K_{UP} = H(C^n, r_{p_1}, r_{u_3}, 0)$, and sends an acknowledgement of access $(r_{p_1}, E_{K_{UP}}[r_{u_3}, P])$ to U. Then, U computes $K'_{UP} = H(C^n, r_{p_1}, r_{u_3}, 0)$ and reveals (r_{u_3}, P) by computing $D_{K'_{UP}}[E_{K_{UP}}[r_{u_3}, P]]$. In addition, U computes $F = K_{UP}"[m_0]$ and sends $(r_{p_1}, r_{u_3}, F, H_{K'_{UP}}(F))$ to P, where $K_{UP}" = H(C^n, r_{p_1}, r_{u_3}, 1)$. Finally, P verifies $H_{K'_{UP}}(F)$ by using K_{UP}, if it holds, P is convinced that a fresh session key exists as $K_{UP}* = K_{UP}"$ where U and P can compute $K_{UP}*$ to reveal m_0 by computing $D_{K_{UP}*}[F]$, where

$K_{UP}* = H(C^n, r_{p_1}, r_{u_3}, 1)$.

3 The Weaknesses of Ren et al. Scheme

In this section, we highlight two weaknesses of Ren et al. scheme. The details of the two weaknesses are described in the following subsections.

3.1 Abusive Attacks on Ren et al. Scheme

In these attacks, an attacker C can fabricate a false but valid user U identity and impersonate U to request an authorized credential from the service provider S. Moreover, even a valid user U can deny that he/she has not requested the service and the service provider cannot prove such information to on trusted evidence and hence there is no way to prevent such a service abuse problem. The detailed steps of the cryptanalysis of Ren et al. scheme are described as follows.

Step 1: In the credential generation phase of the user authorization protocol, an attacker C randomly generates two nonces r_{a_1} and r_{a_2} and carelessly computes the fake credential by computing $C'^0 = H(r_{a_2}, U', A')$, where U' is some valid user's identity and $A' = E_{PK_{U'}}\{U', r_{a_2}\}$. It should be noted that in Ren et al. protocol, they claimed that the signature contained was in C^0 and this provides a non-repudiation property. However, in fact, there is no way to know whether a user uses their private key to sign the C^0 due to it being protected by a nonce r_{a_2} and thus an attacker or anyone could maliciously generate a fake credential C'^0. Thereafter, C computes the credential chain $C'^n = H^n(C'^0)$ and $B' = E_{PK_{SID}}\{r_{a_1}\} * C'^n$.

Step 2: In the credential authorization phase of the user authorization protocol, the service provider only checks the validity of a certificate $CertU'$. Thus, an attacker C or a dishonest user can send any valid certificate $CertU'$ with U', B', SID to the service provider to request an authorized credential for entry. Once the $CertU'$ is valid, S will sign B' and send C' back to the malicious user, where $C' = E_{SK_{SID}}\{B'\} = r_{a_1} * E_{SK_{SID}}\{C'^n\}$.

Step 3: Upon receiving C' from S, the attacker can compute $D' = C'/r_{a_1} = E_{SK_{SID}}\{C'^n\}$ and obtain an authorized credential C'^n and its signature D'. Finally, the attacker can freely use C'^n and its signature D' to access the services without any problems and therefore abusive attacks cannot be prevented in Ren et al. scheme.

Although Ren et al. verify the correctness of the proposed user operational protocol based on the BAN logic [1], their scheme is vulnerable and can easily be cryptanalyzed due to the authentication is broken between $CertU'$'s identifier and the blinded credential chain in user authorization protocol. The authors do not use BAN logic to verify the correctness of the proposed user authorization protocol, thus their scheme is susceptible to the service abusive attack.

3.2 Low Efficiency in User Operational Protocol of Ren et al. Scheme

When a mobile user sends an access request through the user operational protocol, the service provider decrypts and verifies the authenticity of the authorized credential by computing $C^n = E_{PK_{SID}}\{D\}$. If aforesaid holds, the service provider must compare C^n with all the authorized credentials C_i^n stored in its DB, where $i = 1, 2, 3, \ldots, N$ and N is the number of authorized users in the DB. Suppose that S takes j milliseconds to compare a C^n with a C_i^n. Thus, it needs $j * N$ milliseconds to be executed to confirm that a request C^n is valid or not. In practice, if the number of N is a million users and there are k authorized users sending access requests to S simultaneously, S must take $k * j * N$ milliseconds to confirm them and maybe the request users need to wait a few minutes for a reply acknowledgements from S. However, Mobile user U | Service provider S

1. Compute $C^n = H^n(M_i, U, r_{u_2})$
   $B = E_{PK_{SID}}\{r_{u_1}\} * C^n$

2. Send $E_{PK_S}\{U, B, M_i, SID, RM\}$ $\longrightarrow$

3. Compute
   $D_{SK_S}\{E_{PK_S}\{U, B, M_i, SID, RM\}\}$
   Verify the validity of M_i and RM
   Sign B as $C = E_{SK_{SID}}\{B\}$
   Mark M_i non-fresh

$\xleftarrow{C}$

4. Compute
   $D = C/r_{u_1} = E_{SK_{SID}}\{C^n\}$
   Verify the validity of D

Figure 1: User authorization protocol of the improved scheme

in practice, it exhibits a low efficiency and in application it becomes infeasible for access users to wait for the respondent results for such long time in the user operational protocol of Ren et al. scheme. Therefore, we will propose an improved scheme to decrease the waiting time for access users and ensure a high rate of efficiency in the user operational protocol of their scheme.

4 The Improved Scheme

To overcome the above-mentioned problems in Section 3, we propose two improvements on Ren et al. scheme in the following subsection and the details of the improved scheme are described as follows.

4.1 Security Improvement

Considering the nature of abusive attacks as mentioned in Section 3.1, an attacker C only needs to compute $C'^n = H^n(C'^0)$ and $B' = E_{PK_{SID}}\{r_{a_1}\} * C'^n$

and provides $CertU'$ to convince S in Steps 1 and 2. The reason for this attack is because there is no binding between $CertU'$'s identifier and the blinded credential chain C'^n submitted for signing. This flaw fools the service provider into signing the credential B'. Thus, we used the receipt M_i to prevent above attacks in the improved scheme. For a receipt M_i, a mobile user U may demand to be paid for requesting the services from the service provider S and S will issue a unique receipt number M_i to the paid user U after U pays the money to S. Then, S will set up an "eligible paid users list" that records the information of the paid users and their corresponding receipts. The access user must keep M_i secret and he/she has only one chance to use M_i to ask the service provider to run the following steps to acquire the authorized credential in the user authorization protocol. The details of user authorization protocol of the improved scheme are briefly described as follows and shown in Figure 1.

Step 1: In this step, a mobile user U first generates two nonces r_{u_1} and r_{u_2}, then he/she computes the $C^n = H^n(M_i, U, r_{u_2})$, and blinds C^n as $B = E_{PK_{SID}}\{r_{u_1}\} * C^n$.

Step 2: Then, U computes $RM = E_{SK_U}\{U, B, M_i, SID\}$ and sends the value $E_{PK_S}\{U, B, M_i, SID, RM\}$ to the service provider S for credential authorization, where $E_{SK_U}\{*\}$ stands for signing $\{*\}$ with the private key of user U.

Step 3: After receiving the user U's authorization request, S decrypts it with his/her private key SK_S and further verifies the authenticity of M_i and RM by checking the eligible paid users list. If M_i is fresh and the signature is valid, it means that the authorization request is indeed generated by the rightful holder of the receipt M_i and the certificate $CertU$ having the identifier U. Then, S signs B as $C = E_{SK_{SID}}\{B\} = r_{u_1} * E_{SK_{SID}}\{C^n\}$ and marks M_i as a non-fresh value for the purpose of preventing the double-spending problem. Afterwards, S sends C to the user U.

Step 4: After receiving C, U unblinds C as D by computing $D = C/r_{u_1} = E_{SK_{SID}}\{C^n\}$. Thus, U can check the authenticity of D by verifying $C^n \stackrel{?}{=} D_{PK_{SID}}\{D\}$. If it holds, U obtains an authorized credential C^n and its signature D.

Evidently, as the above improved scheme shows, an attacker C does not have the valid receipt M_i and rightful signature RM for asking S to run the credential authorization protocol. Thus, C cannot get the valid C^n and its signature from S in the improved scheme. Moreover, each M_i is used exactly once and it is encrypted by S's public key PK_S and only S can decrypt it by using the corresponding private key SK_S during the process of transmission of the authorization request. After that, M_i would be marked as a non-fresh value and this leads thereto that an attacker C has no opportunity to use it repeatedly. Concerning the computational overhead, during the user authorization protocol of the improved scheme, M_i and S perform one additional asymmetric operation for $RM = E_{SK_U}\{U, B, M_i, SID\}$ and $D_{PK_U}\{RM\}$ per session. It is clear that the overhead of one asymmetric operation for each participant is negligible, especially in view of the level of security the improved scheme offers. Finally, we believe that abusive attacks can surely be prevented in our improved scheme.

4.2 Efficiency Improvement

Considering the nature of low efficiency on Ren et al. scheme as mentioned in Section 3.2, the service provider must compare C^n with all the authorized credentials C_i^n stored in its DB, where $i = 1, 2, 3, \cdots, N$ and N is the number of authorized users in the DB. Since all authorized credentials stored in DB are N, the time complexity of their scheme is thus O(N). It may become infeasible for access users to wait for the respondent results for a long time in the user operational protocol of their scheme. As a result, in the user operational protocol of the improved scheme, we used the temporary identity TID_i to enhance the efficiency of their scheme. Before sending the access request to access point P, U generates a temporary identity TID_i and sends $E = (SID, E_{PK_S}\{TID_i, r_{u_3}, C^n, D\})$ to P. Afterwards, S would record (TID_i, C^n) such in its DB if the access request is valid. Noted that TID_i is an index. When the mobile user U sends the access request to S the next time around, S accords TID_i to find the user's C^n for verification and thus it does not need to compare a C^n with all the authorized credentials C_i^n (where $i = 1, 2, 3, \ldots, N$ and N is the number of authorized users) stored in its DB during user operational protocol.

For the security of TID_i, this design still maintains anonymity because TID_i is a meaningless number and there is no binding between TID_i and user identifier. So, privacy is maintained in our proposed mechanism. On the other hand, our improved scheme accords TID_i to build an index table for retrieving so the service provider only needs to compare C^n once in every session if TID_i exists and there is no collision problem. In this term, the time complexity of the proposed scheme is O(1). Hence, the improved scheme is more efficient than Ren et al. scheme, which could greatly decrease waiting time for users and assist in wider deployments of the scheme.

5 Conclusions

We have shown that Ren et al. scheme is vulnerable to abusive attacks, and that an attacker can freely access the service through the service provider without any worries. The main contribution of our proposed improved scheme is that abusive attacks cannot succeed in it and we have done minor revisions to make the improved scheme more efficient than Ren et al. scheme.

References

[1] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, 1990.

[2] Johann Cas. Privacy in pervasive computing environments - a contradiction in terms? *IEEE Technology and Society Magazine*, 24(1):24–33, 2005.

[3] D. Chaum. Blind signature systems. In *Proceedings of advances in Crypto'83*, page 153, New York, USA, 1983.

[4] Munirul Haque and Sheikh Iqbal Ahamed. Security in pervasive computing: Current status and open issues. *International Journal of Network Security*, 3(3):203–214, 2006.

[5] Qi He, Dapeng Wu, and Pradeep Khosla. The quest for personal control over mobile location privacy. *IEEE Communications Magazine*, 42(5):130–136, 2004.

[6] Min-Shiang Hwang and Pei-Chen Sung. A study of micro-payment based on one-way hash chain. *International Journal of Network Security*, 2(2):81–90, 2006.

[7] Kui Ren, Wenjing Lou, Kwangjo Kim, and Robert Deng. A novel privacy preserving authentication and access control scheme for pervasive computing environments. *IEEE Transactions on Vehicular Technology*, 55(4):1373–1384, July 2006.

[8] Chwei-Shyong Tsai, Chih-Wei Lin, and Min-Shiang Hwang. A new strong-password authentication scheme using one-way hash functions. *International Journal of Computer and Systems Sciences*, 45(4):623–626, 2006.

[9] Johann van der Merwe, Dawoud Dawoud, and Stephen Mcdonald. A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Computing Surveys*, 39(1):1–45, 2007.

[10] Feng Zhu, Matt Mutka, and Lionel Ni. Facilitating secure ad hoc service discovery in public environments. *The Journal of Systems and Software*, 76(1):45–54, April 2005.