An Improvement of Mobile Users Authentication in the Integration Environments*

Min-Shiang Hwang, Cheng-Chi Lee and Wei-Pang Yang

Abstract This paper shows that Tzeng and Tzeng’s protocol has a drawback that the protocol can be easily crashed by an evil VLR attack. Therefore, we propose a slight modification to their protocol to improve their shortcoming. As a result, our protocol does not only enhance the security of Tzeng and Tzeng’s protocol but also improves the efficiency.

Keywords Authentication, Certificate-based, Mobile Communication, Security

1. Introduction

Generally speaking, there are two kinds of key-based cryptosystem algorithms: symmetric and asymmetric. The two cryptosystems lead to different research strategies, especially in mobile communication systems. Some symmetric cryptosystems in mobile communication systems [8–10] have been proposed for authenticating mobile users in GSM, IS-41, and DECT. Since symmetric cryptosystems were first used, the power consumption and computational cost of handsets have both been reduced in these systems. However, these systems only offer one-way authentication. On the other hand, as for asymmetric cryptosystems, some protocols [4, 11] have been proposed with quite some advantages including achieving two-way authentication as well as being equipped with the mechanism of detecting clone. However, the major disadvantage of these protocols is higher computational cost.

To combine both the advantages of symmetric and asymmetric cryptosystems, some hybrid schemes [1–3, 5, 7, 12, 13, 15] have also been proposed. These schemes have succeeded in enhancing the security level and reducing the computational cost at the same time. However, there are still some shortcomings in their schemes. In Beller et. al.’s scheme [1], in order to authenticate mobile users, they have decided to send secret information via the network, which is very dangerous because an evil network operator may clone the user. Similar problems have also occurred in Park’s scheme [12]. In Carlsen [3] and Tatebayashi’s [13] schemes, a trust center has been additionally added to the system to distribute a session key for mobile users. In Yi et. al.’s scheme [15], they have proposed an efficient computation method with less storage requirement in the mobile device. This scheme is, however, insecure [6].

Recently, Tzeng and Tzeng [14] have proposed a hybrid scheme of efficient authentication protocol for the third-generation mobile communication system. Their protocol has both enhanced the security and improved the performance of the second-generation mobile communication system. Their protocol can satisfy some security requirements as follows: key exchange, mutual authentication, location privacy, anonymity, avoidance of clone, perfect forward secrecy, minimized long-distance real-time signaling, and minimized bilateral pre-arrangements between service providers and network operators. Furthermore, their protocol can verify mobile users for international roaming.

However, this Tzeng-Tzeng protocol has a drawback that the protocol can be easily crashed by an evil VLR (Visitor Location Register) attack. An evil VLR can impersonate MS (Mobile Station) to access services for the use in the repeated authentication protocol in the Tzeng-Tzeng protocol because he/she can obtain the Ticket and session key of MS for the use in another VLR. The reason is that if an evil VLR knows another legal VLR is providing services to an MS, the evil VLR can intercept the transmitted messages and forward his/her forged messages to the MS. The MS would believe that he/she is communicating with a perfectly normal VLR because the VLR has a legal certificate issued by HLR (Home Location Register). However, the MS would reply his/her messages (such as temporal secret key and session key). Once the evil VLR receives the MS’s messages, he/she can replay it to another legal VLR and then impersonate the MS to communication with another legal VLR in the repeated authentication protocol in the Tzeng-Tzeng protocol. In this paper, we shall point out this shortcoming more clearly later. Then, we shall propose a slight modification of the Tzeng-Tzeng protocol to improve the performance. Our protocol can not only enhance the se-


M.-S. Hwang, Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.; Fax: 886-4-23742337
E-mail: mshwang@cyut.edu.tw
C.-C. Lee, W.-P. Yang, Department of Computer and Information Science, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu 300, Taiwan, R.O.C.; E-mail: cclee@cis.nctu.edu.tw, wpyang@cis.nctu.edu.tw
Correspondence to M.-S. Hwang.

* This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-005.
curity of the Tzeng-Tzeng protocol but also improve their protocol’s efficiency.

The content of this paper is organized as follows: in the next section, we shall review Tzeng-Tzeng protocol. In Section 3, we shall analyze Tzeng-Tzeng protocol to show its weakness. Then, our improved protocol will be introduced in Section 4 and analyzed in Section 5. Finally, we shall conclude this paper with Section 6.

2. Review of the Tzeng-Tzeng protocol

Tzeng and Tzeng proposed an authentication protocol in the integration environments [14]. Technically, their protocol can be divided into two sub-protocols: the certificate-based authentication protocol and the repeated authentication protocol. The certificate-based authentication protocol is responsible for the registration procedure, handshake procedure, and the procedure for international roaming. The repeated authentication protocol is responsible for authorizing the requested services by the MS always staying at the same VLR. In this section, we only briefly review the certificate-based authentication protocol. In Table 1, we list the abbreviations and notations used in their protocol. The statement \( A \to B : \text{messages} \) denotes that the messages are transmitted from \( A \) to \( B \).

Table 1. The abbreviations and notations.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>VLR</td>
<td>Visitor Location Register</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile Station</td>
</tr>
<tr>
<td>TID/TMSI</td>
<td>Temporary mobile subscriber’s unique identity/Temporary Mobile Subscriber Identity</td>
</tr>
<tr>
<td>IDx</td>
<td>Identity of the entity ( x )</td>
</tr>
<tr>
<td>Ri</td>
<td>Random number</td>
</tr>
<tr>
<td>KA</td>
<td>Public key of the entity ( A )</td>
</tr>
<tr>
<td>KA/KA</td>
<td>Private key of the entity ( A )</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Issue date of the certificate or ticket</td>
</tr>
<tr>
<td>L</td>
<td>Live time of the certificate or ticket</td>
</tr>
<tr>
<td>CertA</td>
<td>Entity ( A )’s certificate ( (IDA, KA, DateA, LA, (IDA, KA, DateA, LA)_KRMS) )</td>
</tr>
<tr>
<td>KVLR</td>
<td>The key of generating message authentication code of VLR</td>
</tr>
<tr>
<td>Ks</td>
<td>A temporal secret key</td>
</tr>
<tr>
<td>⊕</td>
<td>XOR operation</td>
</tr>
</tbody>
</table>

The Certificate-based Authentication protocol:

When each entity is to be authenticated by others in the mobile network, the certificate-based method is used. HLR issues the certificate \( \text{Cert}_{MS} \) and \( \text{Cert}_{VLR} \) to MSs and VLRs. MS stores \( \text{Cert}_{MS}, KR_{MS} \), and \( \text{Cert}_{VLR} \) in their memory or SIM cards, and VLR stores the \( \text{Cert}_{VLR}, K_{VLR} \), and \( \text{Cert}_{HLR} \) in their memory. \( K_{VLR} \) means the secret key of VLR. The protocol is described in the following steps:

1. \( VLR \to MS: \text{Cert}_{VLR}, R_1 \)
   To authenticate MS, VLR generates \( R_1 \) and then sends his/her \( \text{Cert}_{VLR} \) and \( R_1 \) to MS.

2. \( MS \to VLR: (K_s, KU_{VLR}, (\text{Cert}_{MS} || (R_1 || R_2)\_KR_{MS}))_K_s \)
   Upon receiving \( \text{Cert}_{VLR} \) and \( R_1 \) from VLR, MS verifies whether \( \text{Cert}_{VLR} \) is a legitimate certificate using the public key of HLR. MS then generates an \( R_2 \) and a temporal secret key \( K_s \) and stores \( R_1, R_2, \) and \( \text{Cert}_{VLR} \) in his/her memory or SIM card. MS encrypts \( K_s \) using \( KU_{VLR} \) and sends it along with \( (\text{Cert}_{MS} || (R_1 || R_2)\_KR_{MS})_K_s \) to VLR. Upon receiving these messages, VLR decrypts \( K_s \) using \( KR_{VLR} \) and then uses \( K_s \) to decrypt \( \text{Cert}_{MS} \) and \( (R_1 || R_2)\_KR_{MS} \). VLR can obtain \( KU_{MS} \) from \( \text{Cert}_{MS} \) to decrypt \( R_1 \) and \( R_2 \). VLR then verifies whether \( R_1 \) is the same as the one previously sent. If it is correct, VLR computes the session key \( R_1 \oplus R_2 \) and stores it.

3. \( VLR \to MS: (\text{Ticket} || (R_1 || R_2)\_KR_{VLR})_K_s \)
   VLR can authenticate \( \text{Cert}_{MS} \) using the public key of HLR. After verifying MS, VLR generates a TID and a Ticket to MS, where the Ticket is a MAC (Message Authentication Code). The MAC is derived from \((\text{TID}, Date, L)\_KVLR\). Then VLR sends (Ticket || (R1 || R2)KR_{VLR})_K_s to MS.

After receiving these messages, MS decrypts Ticket and \((R_1 || R_2)\_KR_{VLR} \) using \( K_s \). MS can recover \((R_1 || R_2)\) using the public key of VLR and check whether it is correct. If it is, then the session key \( R_1 \oplus R_2 \) is computed. Finally, MS stores the Ticket and session key for the use in the repeated authentication protocol [14].

3. Cryptanalysis of the Tzeng-Tzeng protocol

In this section, we shall show that the Tzeng-Tzeng authentication protocol is not robust enough against the attack from an evil VLR. An evil VLR can impersonate an MS to request services in another VLR in the Tzeng-Tzeng repeated authentication protocol. Once the evil VLR obtains the Ticket and session key pair of an MS, he/she can impersonate this MS to access services for the use in the repeated authentication protocol in another VLR. In order to obtain the Ticket and session key pair of an MS, an evil VLR can intercept and modify messages during the communication sessions between the MS and another VLR. The detailed steps of this attack are shown in Figure 1 and as follows:

1. Assume that VLR’ is an attacker. To forge MS communicating with VLR, VLR’ can intercept \( \text{Cert}_{VLR} \) and \( R_1 \) when VLR sends them to MS and then modify them to \( \text{Cert}_{VLR} \) and \( R_1 \). Then VLR’ sends \( \text{Cert}_{VLR} \) and \( R_1 \) to MS.

2. After receiving \( \text{Cert}_{VLR} \) and \( R_1 \) from VLR’, MS believes that he/she is communicating with a legitimate VLR when making a call. MS follows the usual proced-
5. Upon receiving these messages from VLR, "denotes that the messages are transmitted from the secret key of VLR.

In our modified protocol, we can overcome the attack using his/her private key. Thus, VLR re-encrypts $K_s$ using the public key of VLR and sends the encrypted message and $(Cert_MS || (R_1 || R_2)_{K_{HR}})_{K_s}$ to VLR.

4. After receiving these messages from VLR, VLR follows the usual procedure in the Tzeng-Tzeng protocol. VLR can verify whether $Cert_MS$ is a legitimate MS. If it is correct in this case, yes, VLR believes that he/she is communicating with a legitimate MS. MS produces a Ticket and computes a session key to store them. VLR sends $(Ticket || (R_1 || R_2)_{K_{HR}})_{K_s}$ to MS.

5. VLR’ can intercept these messages and decrypt them because he/she has the key $K_s$. Finally, VLR’ has $Ticket$ and $session key$ for later use in the Tzeng-Tzeng repeated authentication protocol until the $Ticket$ is out of date.

4. Our improved protocol

In our modified protocol, we can overcome the attack from an evil VLR. Since the Ticket and session key of MS can be in no way obtained, an attacker cannot impersonate MS to communicate with VLR any longer in our modified Tzeng-Tzeng repeated authentication protocol.

As in the original Tzeng-Tzeng protocol, HLR distributes a certificate and a private key to each entity. For example, MS has $Cert_{MS}$, $KR_{MS}$, and $Cert_{HLR}$, and VLR has $Cert_{HLR}$, $KR_{HLR}$, and $Cert_{VLR}$, where $KR_{HLR}$ means the secret key of VLR. Here, we also use the same abbreviations and notations in Table 1. The statement “$A \to B$ : messages” denotes that the messages are transmitted from $A$ to $B$.

In our improved protocol, we propose some slight modification to the certificate-based authentication part of the Tzeng-Tzeng protocol. The other parts of the Tzeng-Tzeng protocol, such as the repeated authentication protocol and the authentication protocol for international roaming, stay the same as they are. The steps of our improved protocol are shown in Figure 2 and as follows:

1. $VL'R \to MS : Cert_{VLR}. (K_s)_{KU_{MS}}$

To authenticate MS, VLR generates a temporal secret key $K_s$ and then sends $Cert_{VLR}$ and $(K_s)_{KU_{MS}}$ to MS.

2. $MS \to VL'R : R. (Cert_MS || (R || K_s)_{KR_{HLR}})_{K_s}$

Upon receiving $Cert_{VLR}$ and $(K_s)_{KU_{MS}}$ from VLR, MS verifies whether $Cert_{VLR}$ is a legitimate certificate using the public key of HLR. MS decrypts $K_s$ using his/her private key. MS then generates an $R$ and stores $K_s$, $R$, and $Cert_{VLR}$ in his/her memory or SIM card. MS sends $R$ and $(Cert_MS || (R || K_s)_{KR_{HLR}})_{K_s}$ to VLR.

Upon receiving these messages, VLR decrypts $Cert_{MS}$ and $(R || K_s)_{KR_{HLR}}$ using the key $K_s$. VLR can obtain $KU_{MS}$ from $Cert_{MS}$ to decrypt $R$ and $K_s$. VLR then verifies whether $K_s$ is the same as the one previously sent and verifies whether $R$ remains the same too. If and only if both are yeses, VLR computes the session key $R \oplus K_s$ and stores it.

Note that no one can forge $R$ even if $R$ is in plaintext. If an attacker wants to forge it, he/she has to know $K_s$ and $KR_{HLR}$ to compute $(Cert_MS || (R || K_s)_{KR_{HLR}})_{K_s}$. In an asymmetric cryptosystem, the private key $KR_{HLR}$ is only known to MS. Therefore, no one can forge $R$.

3. $VL'R \to MS : (Ticket || (R || K_s)_{KR_{VLR}})_{K_s}$

VLR can authenticate the $Cert_{VLR}$ using the public key of HLR. After verifying the MS, VLR generates a $TID$ and a Ticket for the MS, where the Ticket is a MAC. The MAC is computed from $(TID, Date, L)_{VLR}$. Then VLR sends $(Ticket || (R || K_s)_{KR_{VLR}})_{K_s}$ to MS.

After receiving this message, MS decrypts $Ticket$ and $(R || K_s)_{KR_{VLR}}$ using $K_s$. MS can recover $(R || K_s)$ using the public key of VLR and check whether it is correct. If it is, then VLR computes the session key $R \oplus K_s$. Finally, MS stores the $Ticket$ and session key for later use in the repeated authentication protocol [14].

5. Analysis

Our protocol is a slight modification of the Tzeng-Tzeng protocol [14]. The security and efficiency of the Tzeng-
Tzeng protocol have already been discussed and demonstrated in [14]. In this session, we shall only discuss the difference between their protocol and ours.

Security analysis:

Our protocol can overcome the attack from an evil VLR that the Tzeng-Tzeng protocol falls for. In the Tzeng-Tzeng protocol, an attacker can intercept and modify the messages between MS and VLR and then impersonate MS to fool VLR. However, this attack will surely be detected by our VLR. The reason for that is only MS and VLR know the temporal secret key $K_s$. Since $K_s$ is not known to any others, an attacker cannot obtain Ticket and $(R \parallel K_s)$ of MS. Therefore, there will be no way to fool VLR in the repeated authentication protocol.

Efficiency:

In Table 2, we can see that our protocol is more efficient than the original Tzeng-Tzeng protocol. In our protocol, one unit of computation time is reduced because MS does not generate a $K_s$. Therefore, the computation cost is low, and the power consumption of MS is of course reduced in our protocol. Here, $T(\cdot)$ stands for the computation time. For example, $T($Symmetric$)$ and $T($Asymmetric$)$ indicate respectively the computation time the symmetric cryptosystem spends and that the asymmetric cryptosystem spends; $T(K_s)$, $T($TID$)$, $T($Ticket$)$, and $T($Random$)$ indicate respectively the computation time for the generation of $K_s$, TID, Ticket, and random numbers ($R_1$, $R_2$, $R$); and $T($XOR$)$ indicates the computation time the XOR operation spends. We divide $T($Asymmetric$)$ into two processes, signing $S$ and verifying $V$, which use private key and public key respectively. $T($Asymmetric$ – S)$ and $T($Asymmetric$ – V$) indicate respectively the computing time the asymmetric cryptosystem spending on signing process and the computing time the verifying process takes. In general, the verifying process is mostly faster than the signing process in an asymmetric cryptosystem. That is to say, in terms of the computations in the asymmetric cryptosystem in VLR, our protocol is more efficient than the Tzeng-Tzeng protocol, and in terms of the computations in the computing asymmetric cryptosystem in MS, the Tzeng-Tzeng protocol is more efficient than of our protocol. Overall, Our protocol is more secure and efficient than that of the Tzeng-Tzeng protocol.

6. Conclusions

In this paper, we have pointed out that the Tzeng-Tzeng protocol is not strong enough against the attack from an evil VLR and thus is not a secure protocol. Therefore, we have proposed an improvement of the Tzeng-Tzeng protocol which is a slight modification. The proposed protocol does not only achieve their original security requirements but also enhances the security by withstanding the attack from an evil VLR. In addition, the efficiency of our protocol is even higher than that of the original Tzeng-Tzeng protocol.

Acknowledgement

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-005.

References

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field “Electronic Engineer” in 1988. He also passed the National Telecommunication Special Examination in field “Information Engineering”, qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

Wei-Pang Yang was born on May 17, 1950 in Hualien, Taiwan, Republic of China. He received the B.S. degree in mathematics from National Taiwan Normal University in 1974, and the M.S. and Ph.D. degrees from the National Chiao Tung University in 1979 and 1984, respectively, both in computer engineering. Since August 1979, he has been on the faculty of the Department of Computer Science and Information Engineering at National Chiao Tung University, Hsinchu, Taiwan. In the academic year 1985-1986, he was awarded the National Postdoctoral Research Fellowship and was a visiting scholar at Harvard University. From 1986 to 1987, he was the Director of the Computer Center of National Chiao Tung University. In August 1988, he joined the Department of Computer and Information Science at National Chiao Tung University, and acted as the Head of the Department for one year. Then he went to IBM Almaden Research Center in San Jose, California for another one year as visiting scientist. From 1990 to 1992, he was the Head of the Department of Computer and Information Science again. His research interests include database theory, database security, object-oriented database, image database, and Chinese database retrieval systems.

Dr. Yang is a senior member of IEEE, and a member of ACM. He was the winner of the 1988, and 1992 AceR Long Term Award for Outstanding M.S. Thesis Supervision, 1993 AceR Long Term Award for Outstanding Ph. D. Dissertation Supervision, and the winner of 1990 Outstanding Paper Award of the Computer Society of the Republic of China. He also obtained the Outstanding Research Award of National Science Council of the Republic of China.