SECURITY WEAKNESSES ON A MUTUAL AUTHENTICATION AND KEY AGREEMENT SCHEME IN GLOBAL MOBILE NETWORKS

Prosanta Gope[1] and Tzonelih Hwang[2]

[1]National Cheng Kung University, Tainan, Taiwan, R.O.C
prosanta.nitdgp@gmail.com
[2]National Cheng Kung University, Tainan, Taiwan, R.O.C
hwangtl@ismail.csie.ncku.edu.tw

ABSTRACT

User mobility is a feature that raises many issues related to security. One of them is the disclosure of a mobile user's real identity during the authentication process, or the other procedures specific to global mobile networks (GLOMONET). Such disclosure allows an unauthorized third-party to track the mobile user's movements and current whereabouts. In this article, we address some problems of mutual authentication and key agreement with user anonymity for GLOMONET. Recently, Qi et al. proposed such scheme, which is claimed to be a slight modification of He et al.'s protocol based on smart card. However, we reveal that both the schemes still suffer from certain weaknesses which have been overlooked previously and thus they cannot achieve desired security.

KEYWORDS

Authentication, Anonymity, Roaming, Privacy, Untraceability, Smart card, Global mobile network.

1. INTRODUCTION

Global mobile network (GLOMONET) is a useful networking environment which permits a mobile user to access the services provided by the home agent (HA) in a foreign network (FA). For securing the communication conducted over GLOMONETs, it is important to provide a way for authenticating mobile users in an anonymous manner. Besides, in the design of an efficient authentication scheme for roaming services in GLOMONET, mutual authentication must be supported to prevent any illegal use of resources and to ensure that mobile users are connected to the trusted network. In order to do so, the authentication scheme should have ability to resist various kinds of attacks or any forgery attempts. For accomplishing these goals, many authentication and key agreement schemes have been proposed with anonymity for roaming services in global mobile networks [1-7]. Particularly, in 2004, Zhu et al. proposed a wireless security protocol based on smart card and featuring user anonymity [1]. Unfortunately, Lee and Hwang [2] pointed out in 2006 that Zhu and Ma's protocol's [1] does not achieve mutual authentication and is also subjected to the forgery attack.

Sundarapandian et al. (Eds) : CCSEIT, DMDB, ICBB, MoWiN, AIAP - 2014
pp. 01–07, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4801

Lee et al. also proposed a slightly modified version of Zhu et al's protocol so as to remedy the identified shortcomings. However, in [3], it was shown that the Zhu et al.'s scheme and Lee and et al.'s scheme fails to provide user anonymity, and Wu, Lee and Tsaur proposed an enhanced scheme by providing an effective remedy. Independently, in [4], Chang et al. showed that Lee et al.'s scheme cannot provide user anonymity under the forgery attack and also proposed an enhanced authentication scheme. Unfortunately, Youn et al. found that the scheme of [4] fails to achieve user anonymity under four attack strategies [5]. Thereafter, He et al. proposed an improved scheme [6] based on the concept of pseudonym. However, the scheme is considered to be economically impractical because of the extraction of parameters from the private space of the smart card. Besides, recently, Qi et al. [7] pointed out some other drawbacks of the He et al. scheme and they proposed an improved authentication protocol for GLOMONET environment. However, in this article, we show that both the schemes [6-7] have some serious weaknesses which have been overlooked.

The remainder of this article is organized as follows. Section 2 reviews the protocol of [7] and 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.

Table 1. Notation and Abbreviations.

Notation	Description
MS	Mobile station/User
FA	Foreign agent
HA	Home agent
ID_M	Identity of a mobile user
ID_f	Identity of a foreign agent
ID_h	Identity of a home agent
PSW_M	Password of the mobile user
$h(.)$	One-way hash function
$\oplus$	Exclusive-OR operation
P	Concatenation operation

2. REVIEW OF QI ET AL.'S SCHEME

Qi et al. scheme [7], which is claimed to be a slight modification of, but a security enhancement on He et al.'s scheme [6], consists of three phases. In Phase I, the home agent (HA) security issues a smart card to a mobile user MS. In Phase II, mutual authentication between MS and a foreign agent (FA) is performed under the supervision of the home agent (HA). After the successful authentication, a legitimate MS can access the wireless service from the FA, and establish a session key between them. In Phase III, MS can renew his/her password. It is assumed that each foreign agent FA shares a long-term secret key K_{fh} with home agent HA.

2.1 Assumption on Quadratic Residue

Conceive, p and q two large primes, from that we calculate $n = p*q$. Now, if $y = x^2 \bmod n$ has a solution, in other words, there exists a square root for y, then y is a quadratic residue of mod n. Therefore, we can represent the set of all quadratic residue numbers in [1, n-1] by QR_n. Based on the quadratic residue assumption, which states that for any $y \in QR_n$, it is difficult to figure out the value of x without having any prior knowledge of p and q because of the difficulty of factoring n[8] into two prime factors which is indeed a difficult task.

2.2 Phase I: Registration Phase

When a mobile user wants to register at the home agent HA, the user has to submit a request to the home agent, and then home agent will issue a smart card with the related information to the user. In this regard, MS at first submits his/her claimed identity ID_M to HA in via a secure channel. After receiving the request from MS, the home agent HA generates a secret random number x and computes $K_{ms} = h(ID_M\ \mathrm{P}x)$ and then the system (HA) generates two large primes p and q and computes n = p*q. Finally, HA personalized a smart card with h (.), K_{ms}, and n , and issues it to MS via a secure channel and then stores ID_M , and K_{ms} for further communication. Hereafter, MS computes $K_{ms}^{*} = h(ID_M\ \mathrm{P}x) \oplus h(ID_M\ \mathrm{P}PSW_M)$ and replaces K_{ms}^{*} with and holds h (.), K_{ms}^{*}, and n for further communication.

2.3 Phase II: Login and Authentication Phase

Once enrolled by HA, when MS visits a foreign network managed by the FA, he/she needs to authenticate himself/herself to FA in order to show that he/she is a legitimate subscriber of his/her home network managed by HA. In this phase FA authenticates MS under the assistance of HA, and issues a session key SK. The steps of this phase are outlined in Fig. 1 and explained as follows.

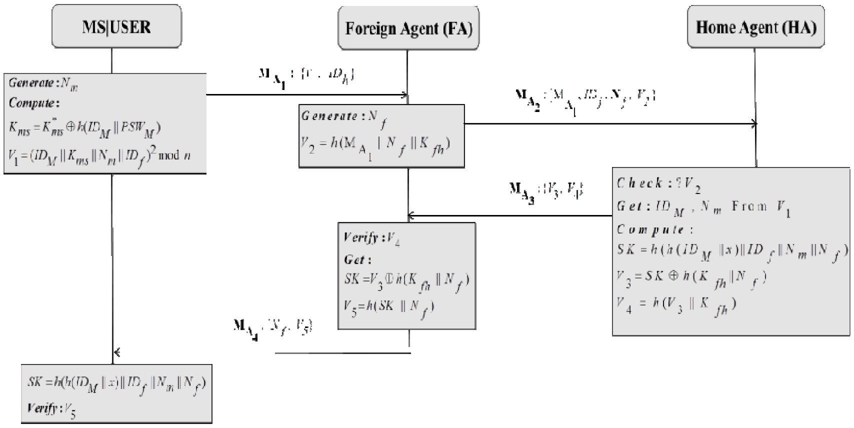
MS|USER
Foreign Agent (FA)
Home Agent (HA)
Generate : N_m
Compute :
$K_{ms} = K_{ms}^{*} \oplus h(ID_M \| PSW_M)$
$V_1 = (ID_M \| K_{ms} \| N_m \| ID_f)^2 \bmod n$
$M_{A_1} : \{V_1, ID_h\}$
Generate : N_f
$V_2 = h(M_{A_1} \| N_f \| K_{fh})$
$M_{A_2} : \{M_{A_1}, ID_f, N_f, V_2\}$
Check : ? V_2
Get : ID_M , N_m From V_1
Compute :
$SK = h(h(ID_M \| x) \| ID_f \| N_m \| N_f)$
$V_3 = SK \oplus h(K_{fh} \| N_f)$
$V_4 = h(V_3 \| K_{fh})$
$M_{A_3} : \{V_3, V_4\}$
Verify : V_4
Get :
$SK = V_3 \oplus h(K_{fh} \| N_f)$
$V_5 = h(SK \| N_f)$
$M_{A_4} : \{N_f, V_5\}$
$SK = h(h(ID_M \| x) \| ID_f \| N_m \| N_f)$
Verify : V_5

Figure.1 Login and Authentication Phase of Qi et al.'s Scheme

Step 1 M_{A_1} : MS → FA: $\{V_1,\ ID_h\}$.

MS submits his/her identity ID_M and password PSW_M to the smart card and computes $K_{ms} = K_{ms}^{*} \oplus h(ID_M\ \mathrm{P}PSW_M)$. Hereafter, MS generates a random number N_m and derives $V_1 = (ID_M\ \mathrm{P}K_{ms}\ \mathrm{P}N_m\ \mathrm{P}ID_f)^2 \bmod n$. Finally, MS sends the login message M_{A_1} to FA.

Step 2 M_{A_2} : FA → HA:$\{M_{A_1}, ID_f, N_f, V_2\}$.

After receiving the login message $\mathrm{M}_{\mathrm{A}_1}$, FA generates a random number N_f and computes $V_2 = h(\mathrm{M}_{\mathrm{A}_1} \mathrm{P} N_f \mathrm{P} K_{fh})$. Hereafter, it requests the HA by sending it's claimed identity ID_f, the nonce N_f ,V_2 , in addition to those of MS.

Step 3 $\mathrm{M}_{\mathrm{A}_3} : \mathrm{HA} \rightarrow \mathrm{FA} : \{V_3,\ V_4\ \}.$

Upon receiving the request from FA, the home agent HA checks ID_f and then computes and verifies whether V_2 is equal to $h(\mathrm{M}_{\mathrm{A}_1} \mathrm{P} N_f \mathrm{P} K_{fh})$ or not. After successful verification, HA solves V_1 by using the Chinese Remainder Theorem [8-10] with p and q and get ID_M, K_{ms}, N_m, and ID_f . Thereafter, HA computes $h(ID_M \mathrm{P} x)$ and verifies with the received K_{ms} . If the verification is successful then HA considers the MS as a legitimate mobile subscriber. Hereafter, HA computes $SK = h(h(ID_M \mathrm{P} x) \mathrm{P} ID_f \mathrm{P} N_m \mathrm{P} N_f),$, $V_3 = SK \oplus h(K_{fh} \mathrm{P} N_f)$, $V_4 = h(V_3 \mathrm{P} K_{fh})$ where SK denotes the session key between MS and FA. Finally, HA forms $\mathrm{M}_{\mathrm{A}_3}$ and sends it to FA.

Step 4 $\mathrm{M}_{\mathrm{A}_4} : \mathrm{FA} \rightarrow \mathrm{MS} : \{N_f,\ V_5\}.$

Upon receiving $\mathrm{M}_{\mathrm{A}_3}$, FA checks whether V_4 is equal to $h(V_3 \mathrm{P} K_{fh})$ or not. After successful verification, FA computes $SK = V_3 \oplus h(K_{fh} \ \mathrm{P}\ N_f)$, $V_5 = h(SK\ \mathrm{P}\ N_f)$ and sends $\mathrm{M}_{\mathrm{A}_4}$ to MS. After receiving $\mathrm{M}_{\mathrm{A}_4}$ from FA, MS at first computes $SK = V_3 \oplus h(K_{fh} \ \mathrm{P}\ N_f)$ and then verifies V_5 is equal to $h(SK\ \mathrm{P}\ N_f)$ or not. If it is true, then MS establishes a *SK* with FA; otherwise authentication fails.

2.4 Phase III: Password Renewal Phase

In this scheme, a mobile user can freely change his/her password on the smart card without the help of the home agent HA. Now, when mobile user MS with a smart card wants to change the password of the smart card, MS makes a request to the smart card, and then inputs the old password PSW_M and the new password PSW_M to the smart card. Then the smart card recovers $K_{ms} = K^{*}_{ms} \oplus h(ID_M\ \mathrm{P} PSW_M)$ and derives $K^{**}_{ms} = K^{*}_{ms} \oplus h(ID_M\ \mathrm{P} PSW^{*}_M)$ .Finally, stores the K^{**}_{ms} in place of K^{*}_{ms} .

3. Security Weaknesses in Qi et al.'s Protocol

During the cryptanalysis of the He et al.'s scheme, Qi et al. shown that the He et al's scheme is highly insecure because of the several attacks like "mobile tracking and identity guessing attack", "offline guessing attack" etc. In this regard, the adversary needs to perform some exhaustive guess operations and through which he/she needs to figure out one unknown parameter from a relation, where other parameters in the relation are publicly known (unencrypted data). Unfortunately, while designing their improved scheme [7], like He et al., Qi et al. also overlooked that issue in some cases. As a consequence of that Qi et al.'s improved scheme still has several serious deficiencies (shown below).

3.1 Revealing of long-term Secret Key and Session Key

Consider an adversary $\mathcal{A}$ has control over the communicating messages transmitted over open networks. Precisely, the adversary $\mathcal{A}$ has the capability to intercept the messages flowing through the mobile network. Now, in the login and authentication phase of the Qi et al.'s scheme, after the successful verification of the mobile user, as well as the foreign network when, the home agent HA sends the response message $\mathrm{M}_{\mathrm{A}_3}$ to FA. We assume that the adversary has intercepted that message. Therefore, $\mathcal{A}$ receives both V_3, V_4, where $V_4 = h(V_3 \; \mathrm{P} K_{fh})$. In this relation, only K_{fh} is unknown to the adversary $\mathcal{A}$. Therefore, by executing an exhaustive search operation, he/she can easily figure out the long-term shared secret key K_{fh}, which is indeed a serious concern. As, this will not only affect that particular mobile subscriber, at the same time it also compromises the security of other mobile users who received their smart card from that particular home agent and willing to roam over through the area covered by that particular foreign agent whose secret key K_{fh} has been compromised. In this case, after acquiring that secret key, the adversary can perform any kind of forgery attempt and even can share this secret key with a dishonest foreign agent who can exploit it with its superior capabilities and that may even annoy the mobile subscriber with billing problem. Now, we consider that the adversary $\mathcal{A}$ eavesdrops the communication between MS and FA, in other words, the adversary has intercepted the response message $\mathrm{M}_{\mathrm{A}_4}$, which is sent by the foreign agent FA to MS. In this regard, using the parameters N_f, V_5 , where $V_5 = h(SK \;\; \mathrm{P} \; N_f)$ and executing the exhaustive search operation, the adversary can easily get the session key SK every time, which is also a serious apprehension. The similar problems can also be profound in the login and authentication phase of the He et al.'s scheme.

.

3.2 Vulnerable to Known Session Key Attack

It is obvious that known session key attack is a serious threat against any session key establishing schemes. A protocol is called secure against known session key attacks if a revealed session key does not influence on the security of other session keys. In other words, if past session keys are compromised, it should not allow an adversary to compromise future session key or any even any other session keys earlier than that one. In this way, a protocol can also compromise its backward and forward secrecy. Where, by backward secrecy, we mean that a compromise of any session key should not compromise any earlier key. While forward secrecy implies that a compromise of the current session key should not compromise any future key. However, unfortunately, the Qi et al.'s scheme cannot ensure the security against known session key attack. If a session key established between MS and FA is revealed to an adversary, then the adversary may target the relation $SK = V_3 \oplus h(K_{fh} \;\; \mathrm{P} \; N_f)$, where the parameters V_3 and N_f are public. Therefore, by executing the exhaustive search operation, the adversary $\mathcal{A}$ can figure out K_{fh}. Now, by using that the adversary can easily acquire all the past and future session keys. Accordingly, Qi et al.'s scheme cannot insure any forward and backward secrecy. Moreover, this problem also persists in the login and authentication phase of the He et al.'s scheme.

3.3 Unsuccessful Key-Agreement

In the login and authentication phase of [7], after acquiring the secret key K_{fh} by executing an exhaustive search operation presented in Sect. 3.1 and 3.2, if the adversary $\mathcal{A}$ eavesdrops the message $\mathrm{M}_{\mathrm{A}_3}$ and then attempts to modify V_3 to $V_3^{'}$, and using that, alters V_4 to $V_4^{'}$ and then sends $\{V_3^{'},\ V_4^{'}\}$ to the foreign agent. However, unfortunately, the foreign agent cannot comprehend that alternation. Because, when the foreign agent verifies the relation $h(V_3^{'}\ \mathrm{P}\, K_{fh})$ with $V_4^{'}$, it seems to be perfect for the system (FA). In this way, an attacker can resist a legitimate foreign agent FA to produce the valid session key and eventually that makes the key-agreement unsuccessful. In fact, the similar problem can also be profound in [6].

3.4 Logical Error during Renewal of Password

Apart from the aforesaid serious security issues, the improved scheme proposed by Qi et al. also encompasses one logical mistake during the execution of the password renewal phase. After retrieving the original K_{ms} through $K_{ms} = K_{ms}^{*} \oplus h(ID_M\ \mathrm{P}\, PSW_M)$, the smart card updates the K_{ms}^{**} with the relation $K_{ms}^{**} = K_{ms}^{*} \oplus h(ID_M\ \mathrm{P}\, PSW_M^{*})$. Where K_{ms}^{*} denotes the previously updated key. In this way, MS forgets the original K_{ms} which was given by the home agent HA during registration. . As a consequence of that, after the execution of the password renewal phase, if MS wants to acquire roaming services in that case during authentication the home agent cannot match the K_{ms} with the relation $h(ID_M\ \mathrm{P}\, x)$. This will surely compel both the MS and HA to execute the registration phase once again, which is not desired at all.

4. CONCLUSION

Recently, Qi et al. proposed a authentication and key agreement protocol featuring user anonymity. In this article, we have demonstrated certain deficiencies found in Qi et al.'s proposed authentication scheme. Where, we have found that the scheme presented by Qi. et al. is vulnerable to known session key attack, forgery attacks etc. Nevertheless, the proposed scheme has also committed some logical errors during the password renewal phase.

ACKNOWLEDGEMENTS

This work is financially supported by the National Science Council of Republic of China (Taiwan), under Contract No. NSC MOST 103-2221-E-006 -177 -. The authors would like to thank the National Science Council of Republic of China for their benign supports

REFERENCES

[1] Zhu, J. & Ma, J. (2004). A new authentication scheme with anonymity for wireless environments, IEEE Transactions on Consumer Electronics, 50(1) 230-234.

[2] Lee,C., Hwang, M. S., & Liao, I. E. (2006). Security enhancement on a new authentication scheme with anonymity for wireless environment, IEEE Transactions on Industrial Electronics, 53(5), 1683-1687.

[3] Wu, C. Lee, W. B. & Tsaur, W. J. (2008). A secure authentication scheme with anonymity for wireless communications, IEEE Communication Letters, 12(10), 722-723.

[4] Cheng, C.C. Lee, C.Y. & Chiu, Y.C. (2009) Enhance authentication scheme with anonymity for roaming service in global mobility networks, Computer Communications, 32, 611-618.

[5] Youn, T. Y., Park, T. H., & Lim. (2009). Weaknesses in an anonymous authentication scheme for roaming service in global mobile networks, IEEE Communication Letters, 13(7), 471-473.

[6] He, D., Ma, M., Chen, C., and Bu J. (2011). Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks, Wireless Personal Communications, 61, 465-476.

[7] Jiang Q., Ma, J., Li, G., Yang, L. (2013), An enhanced authentication scheme with privacy preservation for roaming services in global mobility networks, Wireless Personal Communications, 68, 1477-1491.

[8] Rosen, K. (1988). Elementary number theory and its applications, Addision Wesley.

[9] Stalling, W. (2000). Cryptography and network security principles and practice, Prentice Hall.

[10] Trappe, W., and Washington, C., L. (2006). Introduction to cryptography with coding theory, Prentice Hall.

[11] Chang, C., Lee, J. & Chang, Y. (2005). Efficient authentication protocols of GSM. Computer Communications, 28 (8), 921-928.

[12] C.C Lo, Y.J.Chen.(1997). Secure communication mechanisms for GSM networks. In Proceedings of the IEEE transactions on Consumer Electronics 45, 1074-1080.

[13] T-F Lee, C. C Chang and T. Hwang, Private Authentication Techniques for the Global Mobility Network, ' Wireless Personal Communications, Vol 35, No 4, Jan 2005, pp. 329-336

[14] Hwang, T. Gope, P. Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time Secrets, Wireless Personal Communications, DOI. 10.1007/s11277-013-1501-5, 2013

[15] TS 33.102: Security architecture, version 4.2.0, released 4. Third Generation Partnership Project-Technical Specification Group, 2001.

[16] TR 33.902: Formal analysis of the 3G authentication protocol. Third Generation Partnership Project-Authentication and Key Agreement (AKA), 2000.

AUTHOR BIOGRAPHIES

Prosanta Gope received his M.Tech degree in Computer Science and Engineering from National Institute of Technology (NIT), Durgapur, India, in 2009. Currently he has been pursuing his PhD degree in Computer Science and Information Engineering, National Cheng Kung University (NCKU), Tainan, Taiwan. His research interests include authentication, authenticated encryption, security in mobile communication and cloud computing.

Tzonelih Hwang received the M.S. and Ph.D. degrees in Computer Science from the University of Southwestern Louisiana, USA, in 1988. He is currently a Distinguished Professor in the department of Computer Science and Information Engineering, National Cheng Kung University (NCKU), Tainan, Taiwan. Dr. Hwang has actively participated in several research activities including as a research scientist at the Center for Advanced Computer Studies, University of Southwestern Louisiana, USA. He is also associated as a vigorous member of the editorial board of some reputable international journals. He has published more than 250 technical papers and holds four patents. His research interests include network and information security, access control systems, error control codes, security in mobile communication and quantum cryptography.