International Journal of Computer Science and Business Informatics

IJCSBI.ORG

A Lightweight Authentication Scheme for Mobile Cloud Computing

Mohammad Rasoul Momeni
Department of Computer Engineering,
Imam Reza International University of Mashhad, Iran

ABSTRACT

The ABI Research believes that the number of mobile cloud computing users is expected to grow from 42.8 million (1.1% of total mobile users) in 2008 to 998 million (19% of total mobile users) in 2014. The security risks have become a hurdle in the rapid adaptability of the mobile cloud computing technology. Significant efforts have been devoted in research organizations and academia to securing the mobile cloud computing technology. In this paper we proposed a lightweight authentication protocol for mobile cloud environment. Our proposed protocol has many advantages such as: supporting user anonymity, local authentication and also resistance against related attacks such as replay attack, stolen verifier attack, modification attack, server spoofing attack and so on.

Keywords

mobile cloud computing, security risks, lightweight authentication, local authentication.

1. Introduction

Due to inherent challenges of wireless communications such as insecure nature and problems related to heterogeneity, security and privacy issues are too complex in mobile cloud computing. And also due to energy constraints in mobile devices, mobile users need to lightweight security mechanisms. As a security factor, authentication methods are grouped to four classes. 1. what you are? (e.g. fingerprint), 2. what you have? (e.g. smart cards), 3. what you know? (e.g. passwords) and 4. what you do? or implicit authentication. Authentication is the most important factor to protect systems against attacks. Especially in wireless mobile communications, authentication methods should be lightweight, also computation and communication costs should be little. Firstly lamport in 1981 proposed an authentication scheme over an open channel [1]. Chang and Wu proposed smart cards for remote user authentication protocols [2]. Then many two factor authentication protocols have been proposed [3-7]. Chow et al proposed an authentication framework for mobile cloud users [8]. Their proposed authentication scheme was implicit authentication. Schwab and li proposed an entity authentication scheme for mobile cloud environment [9]. They used fuzzy password authentication in their scheme. Hoon and Euiin also proposed an authentication scheme using

profiling technique in mobile cloud computing [10]. The rest of the paper is organized as follows: in Section 2, we propose our scheme. Section 3 and 4 describe the security and performance analysis respectively. And finally section 5 concludes the paper. The notations to be used in this paper are in Table 1.

Table 1. Notations

Symbol	Description
X	a high entropy secret random number
$H()$	a collision-free one-way hash function
SP_{MU}	service permissions of mobile network
$Cert_{MU}$	An authentication certificate
$IMSI$	International mobile subscriber identity
$TMSI$	Temporary mobile subscriber identity
LAS	Local authentication server
SK	A session key
$\|\|$	Concatenation operator
MAC_{LAS}	MAC address of local authentication server
r_1 and r_2	Two random numbers

2. Proposed authentication Protocol

In this section our protocol is presented. The time for remote authentication protocol is long, especially in the wireless mobile communications. Hence this protocol provides local authentication. In this protocol mobile user is authenticated in his/her mobile network, hence this mechanism provides low latency and saves bandwidth. In the end of authentication phase mobile user receives a $Cert_{MU}$ from mobile service provider that presents it to the cloud service provider. Note that mobile service

provider and cloud service provider are fully trusted together. Proposed protocol consists of registration phase and mutual authentication with session key agreement phase that are described below.

2.1 Registration phase

In this phase mobile user performs registration phase via secure channel as follows. Note that registration phase is done only once when mobile user wants to join the mobile network.

1) The mobile user submits his/her *IMSI* as identity and some personal secret information to the server.

2) Now the server checks this *ID* and if already exists in server database rejects it, Mobile user must prepares unique *ID*. It is clear to see that in this step identity management is provided. Now server can compute authentication key $AK = H(X \| IMSI)$ which X is a high entropy secret random number and $H()$ is a collision-free one-way hash function.

3) The server returns AK and SP_{MU} to the mobile user, which SP_{MU} is service permissions of mobile network allocated to the mobile user by server.

2.2 Mutual authentication with session key agreement

After registration whenever mobile user wants to use mobile network services, he/she must be authenticated. Hence he/she sends a login request message to the server and then server verifies the authenticity of the login request message as follows.

1) The mobile user generates a random number r_1 and message $R_1 = (SP_{MU} \| r_1)$, then encrypts R_1 by the AK. He/she sends $M_1 = (TMSI, E_{AK}(R_1), H(TMSI, MAC_{LAS}, E_{AK}(R_1))$ to LAS. For protecting user anonymity instead of using $IMSI$, $TMSI$ is used.

2) After receiving M_1, the server computes $H^*(TMSI, MAC_{LAS}, E_{AK}(R_1))$, then checks $H = H^*$ for detecting modification attack. If H is not equal to H^* and $TMSI$ is not valid, LAS aborts the current session. Hence denial of service can be eliminated. Then decrypts the R_1 and obtains the SP_{MU} and r_1. Now LAS generates r_2, $Cert_{MU}$ and message $R_2 = (Cert_{MU} \| r_1 \| r_2)$, also it generates $SK = H(TMSI \| r_1 \| r_2)$ and sends $M_2 = (MAC_{LAS}, E_{AK}(R_2), H(MAC_{LAS}, TMSI, E_{AK}(R_2))$.

3) After receiving M_2, mobile user computes $H^*(MAC_{LAS}, TMSI, E_{AK}(R_2))$ then checks $H = H^*$ for detecting modification attack. If H is not equal to H^* mobile user

aborts the current session, Hence denial of service can be eliminated. Then decrypts the R_2 and obtains the $Cert_{MU}$, r_1 and r_2. Also it checks random number r_1 to avoid replay attacks. Mobile user generates $SK = H\ (TMSI \parallel r_1 \parallel r_2)$, hereafter both sides use SK for encrypting the messages instead of AK. Note that AK and SK are valid only for this session.

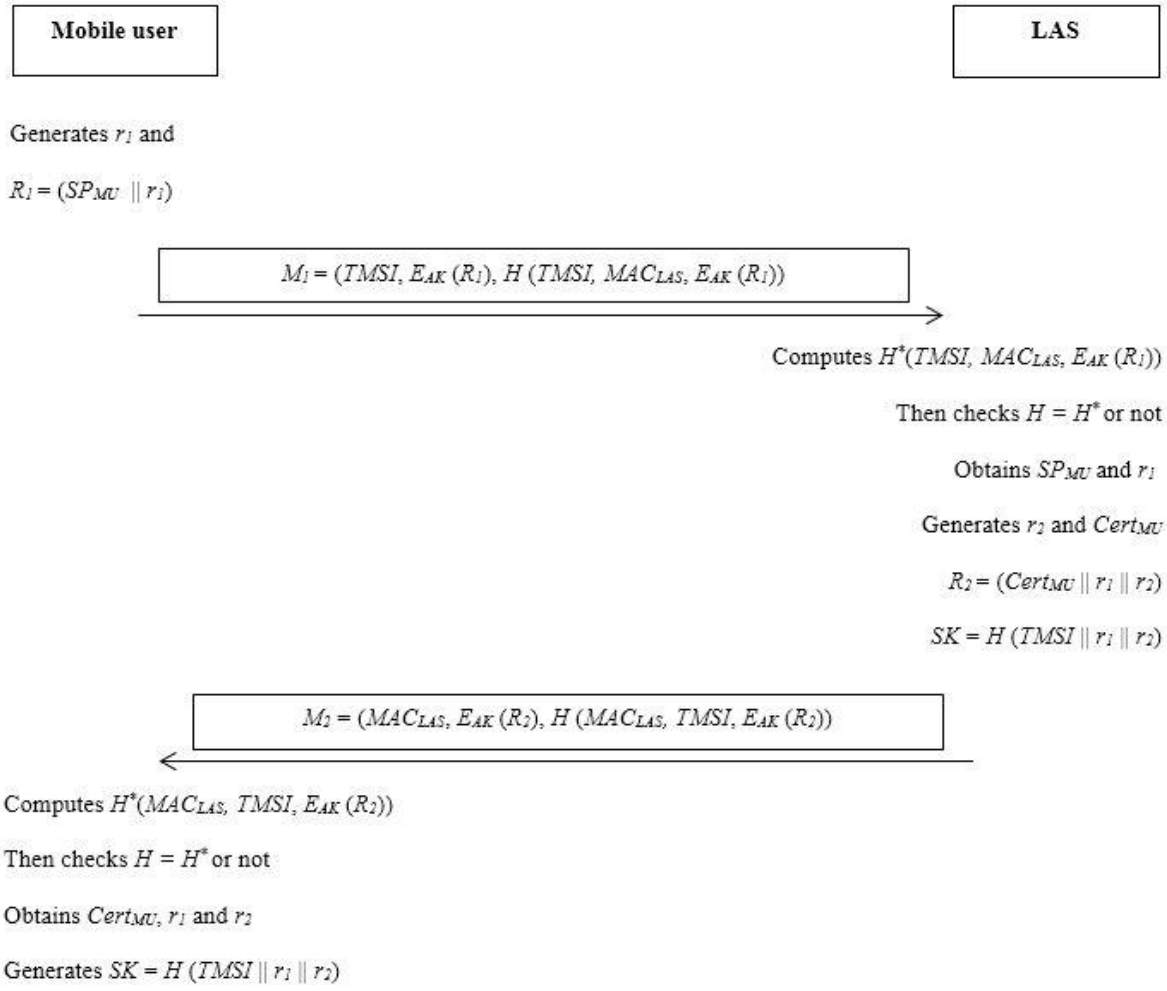

Figure 1. Proposed scheme

2.3 Authentication key change phase

When an authentication key is leaked, mobile user needs to a new authentication key. In order to get new authentication key mobile user submits his/her *IMSI* as identity, old authentication key and some personal secret information through the secure channel to LAS. After checking the validity of mobile user, LAS selects a new

random number X^* and generates the new authentication key $AK^* = H(X^* \| IMSI)$. Now LAS sends AK^* to mobile user through the secure channel.

3. Security analysis

In this section security features of our proposed protocol is presented and we demonstrate proposed protocol can withstand against related security attacks.

3.1 No clock synchronization problem: many proposed authentication protocols use timestamps to avoid replay attacks but timestamp mechanism is difficult and expensive in wireless mobile communications [11] and distributed networks [12,13,14]. Our proposed protocol is nonce-based and does not have clock synchronization problem.

3.2 Session key agreement: in our proposed protocol a session key is generated which uses random numbers like r_1 and r_2. This session key provides secure communications over open channel by encrypting the exchanged messages.

3.3 Modification attack resistance: to avoid modification attacks in our proposed protocol, collision-free one-way hash function is used. If an adversary sends a modified message, recipient can easily detect it by checking the hash values.

3.4 Replay attack resistance: our proposed protocol includes random numbers to avoid replay attacks. Guessing the value of random numbers is very hard for attackers because they are refreshed in each session and authentication time.

3.5 Authentication key change phase: When an authentication key is leaked, mobile user needs to a new authentication key. Our proposed protocol supports Authentication key change phase. As mentioned after checking the validity of mobile user, LAS selects a new random number X^* and generates the new authentication key $AK^* = H(X^* \| IMSI)$. Now LAS sends AK^* to mobile user through the secure channel.

3.6 Stolen verifier attack resistance: our proposed protocol is robust against stolen verifier attack because server does not keep any secret table or any pre-shared secret key. Hence adversary cannot gain any valuable information from this attack.

3.7 Server spoofing attack resistance: our proposed protocol provides mutual authentication for both participants. Mobile user authenticates the LAS and also LAS can authenticate the mobile user. Hence sever spoofing attack is ineffective.

3.8 Local authentication: as mentioned proposed scheme implements local authentication. Local authentication has two big advantages: it saves bandwidth and

removes latency.

3.9 User anonymity: user anonymity means protecting real identity of user against public, no server [15]. Our proposed scheme satisfies user anonymity, because in the registration phase *IMSI* (real identity of user) transmits through secure channel. In the authentication phase instead of *IMSI*, *TMSI* transmits to LAS.

3.10 Parallel session attack resistance: both two identities of mobile user and LAS exist in the hash functions of exchanged messages M_1 and M_2. This mechanism prevents parallel session attack and our proposed scheme is robust against parallel session attack.

3.11 Known plaintext attack resistance: the attacker does not know $AK = H(X \| IMSI)$, because *IMSI* transmits through secure channel in the registration phase and in the authentication phase *TMSI* transmits to LAS instead of *IMSI*. Also *X* is a high entropy secret random number that attacker cannot access it. Hence our proposed protocol is robust against Known plaintext attack.

4. Performance analysis

In this section we evaluate the performance of our proposed protocol. Note that a good authentication scheme for mobile cloud computing must be lightweight. In order to be lightweight we used symmetric encryption, since it has very low computation cost. Our proposed scheme analysis is shown in Table *2*.

Table 2. Computation cost of our scheme

Computation cost	Mobile user	Local authentication server
Registration phase	-	$1C_H$
Authentication phase	$3C_H + C_R + 2C_{SYM}$	$3C_H + C_R + 2C_{SYM}$

Also computation cost of LMAM [16] is shown in Table 3.

Table 3. Computation cost of LMAM [16].

Computation cost	Mobile user	Local authentication server
Registration phase	-	$1C_H$
Authentication phase	$3C_H + C_R + 3C_{SYM}$	$5C_H + C_R + 3C_{SYM}$

Comparing the two tables, it is clear to see our proposed scheme is more efficient than LMAM. Respectively C_H, C_R and C_{SYM} are hash functions cost, random numbers cost and also symmetric encryptions cost.

5. Conclusion

In this paper we proposed a lightweight authentication protocol for mobile cloud computing. The time for remote authentication protocol is long, especially in the wireless mobile communications. Hence this protocol provides local authentication. In this protocol mobile user is authenticated in his/her mobile network, hence this mechanism provides low latency and saves bandwidth. Also our proposed protocol satisfies user anonymity, mutual authentication and so on. In terms of resistance against related attacks, our proposed protocol is robust against replay attack, stolen verifier attack, modification attack, server spoofing attack and so on. It is important to note that, proposed protocol is according to real communication scenarios.

References

[1] L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981) 770–772.
[2] C. Chang, T. Wu, Remote password authentication with smart cards, IEE Proceedings-Computers and Digital Techniques 138 (3) (1991) 165–168.
[3] J. Shen, C. Lin, M. Hwang, A modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 49 (2) (2003) 414–416.
[4] I. Liao, C. Lee, M. Hwang, A password authentication scheme over insecure networks, Journal of Computer and System Sciences 72 (4) (2006) 727–740.
[5] C. Lee, M. Hwang, I. Liao, Security enhancement on a new authentication scheme with anonymity for wireless environments, IEEE Transactions on Industrial Electronics 53 (5) (2006) 1683–1687.
[6] J. Xu, W. Zhu, D. Feng, An improved smart card based password authentication scheme with provable security, Computer Standards & Interfaces 31 (4) (2009) 723–728.

[7] K. Yeh, C. Su, N. Lo, Y. Li, Y. Hung, Two robust remote user authentication protocols using smart cards, Journal of Systems and Software 83 (12) (2010) 2556–2565.
[8] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, "Authentication in the clouds: a framework and its application to mobile users," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW), pp. 1 - 6, 2010.
[9] David Schwab, Li Yang, Entity Authentication in a Mobile-Cloud Environment, CSIIRW '12, Oct 30 - Nov 01 2012, Oak Ridge, TN, USA ACM 978-1-4503-1687-3/12/10.
[10] Hoon jeong, Euiin choi, user authentication using profiling in mobile cloud computing, AASRI Procedia 2 (2012) 262 – 267, Doi: 10.1016/j.aasri.2012.09.044.
[11] A. Giridhar, P. Kumar, Distributed clock synchronization over wireless networks: algorithms and analysis, in: Proceedings of the 45th IEEE Conference on Decision and Control, IEEE, 2006, pp. 4915–4920.
[12] D. Mills, Internet time synchronization: the network time protocol, IEEE Transactions on Communications 39 (10) (1991) 1393–1482.
[13] J. Han, D. Jeong, A practical implementation of IEEE 1588–2008 transparent clock for distributed measurement and control systems, IEEE Transactions on Instrumentation and Measurement 59 (2) (2010) 433–439.
[14] R. Baldoni, A. Corsaro, L. Querzoni, S. Scipioni, S. Piergiovanni, Coupling-based internal clock synchronization for large-scale dynamic distributed systems, IEEE Transactions on Parallel and Distributed Systems 21 (5) (2010) 607–619.
[15] D. Wanga, Chun-guang, Cryptanalysis of a remote user authentication scheme for mobile client–server environment based on ECC, Information Fusion 14 (2013) 498–503.
[16] D. He, M. Ma, Y. Zhang, C. Chen, J. Bu, A strong user authentication scheme with smart cards for wireless communications. Computer Communications, 34 (2011) 367–374.

This paper may be cited as:

Momeni, M. R., 2014. A Lightweight Authentication Scheme for Mobile Cloud Computing. *International Journal of Computer Science and Business Informatics, Vol. 14, No. 2, pp. 153-160.*