One-Time Secret for Fast Communal Verification and Nested Key Swap in Mobile Communications

Y.V.Sricharan[1] **B.Purushotham**[2]
[1] 2nd Year M.Tech, CREC, Tirupati
[2] Professor of Department of CSE, CREC, Tirupati

ABSTRACT

Verification is one of the security mechanisms which plays a quite important role in the entire mobile network system and acts as the first defence against Attackers. tailored for mobile communication environments through maintaining inner and outer synchronously changeable common secrets respectively. Every mobile user can be rapidly verified by visited location register (VLR) and home location register (HLR), respectively, in the proposed scheme. Not only does the proposed solution achieve communal verified, but it also greatly reduces the computation and communication cost of the mobile users as compared to the existing verification schemes.

Key words: Information security, Communal Verification, One time secrets.

1. INTRODUCTION

We make deep research on the performance of secure communal verification schemes and come up with an efficient solution to further simplify and speed up the verification processes through synchronously changeable secrets, which form a nested structure (containing an outer one-time secret and an inner one), shared by each mobile user and the system. The outer one-time secret is a temporal common key of the user and the HLR for initial verification or verification when the user roams around the service area of a new VLR. The inner one-time secret is shared by the user and some VLR for communal verification between the user and the same VLR. Compared to Hwang and Chang's scheme of, the proposed scheme greatly reduces the computation cost required for each mobile user by nearly 33%. Furthermore, the proposed scheme is formally demonstrated as being immune to both the replay attack and the impersonating attack.

Among all security mechanisms in the GSM-based systems, verification schemes are key techniques to ensure the correctness of the identities of all communication entities before they are about to perform other communication activities. These schemes form robust defenses to withstand the replay attack and the impersonating attack in the GSM system. It is efficient in case of communication cost and computation cost.

In the GSM system two verification actions must be performed, i.e., the communal verification between a VLR and the HLR and the communal verification between the system (VLR and HLR) and each user. In order to guarantee the quality of mobile communication, the verification mechanisms we adopt should be as efficient as possible. Each VLR and the HLR are both located in the interior wired network of the GSM system, so they can verification each other through the timestamp-based verification mechanism without suffering from the problem of clock synchronization. Since the clocks of each VLR and the HLR can be easily synchronized and the time consumed by transmitting a message between them is stable, we can make use of the timestamp-based solution to build up the communal verified protocol between each VLR and the HLR.

On the other hand, it is difficult to synchronize the clocks of the system (VLRs and the HLR) and all mobile users. Hence, we cannot utilize the timestamp-based solution to construct the verification protocol between the system and every mobile user even though the solution is the most efficient one among the three verification mechanisms. Owing to the assumption of the mechanism based on one-time secrets, it cannot form the verification protocol for the initial verification between the system and each mobile user. Thus, we adopt the nonce-based mechanism to establish the verification protocol for the initial verification between the system and every user.

Most of the current mobile communication services are based on the Global System for Mobile Communications (GSM) architecture, and some novel applications based on the third generation (3G) of mobile communication systems have also been deployed. However, the messages transmitted in wireless communication networks are exposed in the air, so malicious parties in wireless environments have more opportunities than those in wire-line environments to eavesdrop or intercept these transmitted messages. It will seriously threaten the security of wireless communication systems if no protection mechanism is considered. Although some security aspects of current mobile communication systems have been concerned, there still exist security problems in some GSM-based systems-for example, the impersonating attack works because of the lack of communal verification in the GSM system. Communal verification and other related security issues have been considered in the GSM-based verification protocols proposed in the literature, but their performance should be improved as much as possible to further meet the low-computation requirement for mobile users and guarantee the quality of the communication services.

2.MATERIALS AND METHODS

2.1 One-Time Secret Mechanism

Consider a sequence of mutual communal verification processes based on our proposed hybrid mechanism between mobile user i and the system (VLR and the HLR). In the initial verification , the user and the system verification each other by performing a nonce-based verification protocol, and then they negotiate an initial value of a one-time secret. Thus, they make use of the one-time secret, called the outer one-time secret, to complete the following verification processes.

In fact, the cost of the verification can be further reduced again if the user does not leave the service area of the current VLR. In this case, the user performs an initial communal verification protocol with the VLR only, and they set an initial value of another one-time secret, called the inner one-time secret, shared by them.

They can perform the following verification actions via the inner one-time secret until the user leaves the service area of the VLR. Once the user enters the service area of another VLR, the outer one-time secret will be resumed to serve as the key parameter for the next round of verification between the user and the system. In the proposed idea, mobile user i shares the outer one-time secret with the HLR and shares the inner one-time secret with the current VLR. This is referred to as the nested one-time secret mechanism, which is illustrated in Figure 2.1.

All of the mobile users pay much attention to the performance issue due to the limited computation capabilities of their mobile devices. Among the verification schemes for mobile communication proposed in the literatures [7], [9], [10], [14]-[20], Hwang and Chang’s scheme [10] is the most efficient one. According to different situations, we properly utilize three different verification mechanisms i.e., timestamps, one-time secrets, and nonces in the proposed verification scheme for mobile communication such that it possesses better performance than Hwang and Chang’s scheme.

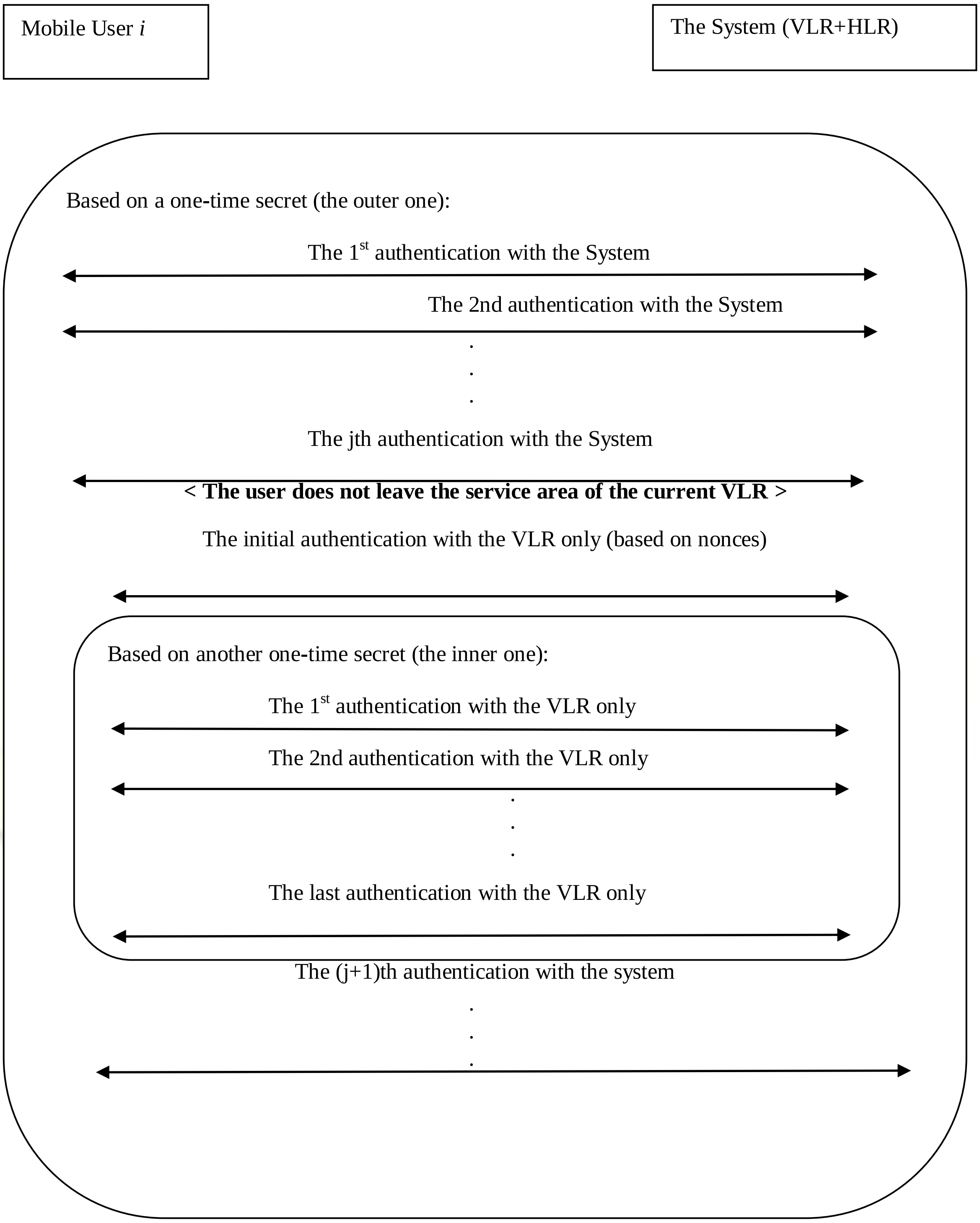
Mobile User *i*
The System (VLR+HLR)
Based on a one-time secret (the outer one):
The 1st authentication with the System
The 2nd authentication with the System
The jth authentication with the System
< **The user does not leave the service area of the current VLR** >
The initial authentication with the VLR only (based on nonces)
Based on another one-time secret (the inner one):
The 1st authentication with the VLR only
The 2nd authentication with the VLR only
The last authentication with the VLR only
The (j+1)th authentication with the system

Fig 2.1: The proposed nested one-time secret mechanism

2.2 Procedure and Description

A fast communal verification and key exchange scheme for mobile communications. Our scheme consists of two parts (modules) and each of the two parts contains two protocols (sub modules). The first part of the scheme is designed for communal verification between a mobile user and the system (a VLR and the HLR) where it includes two protocols:

A) An initial verification protocol for communal verification and the initialization or reinitialization of the outer one-time secret; and

B) An verification protocol based on the outer one-time secret for the ***j***th verification after the most recent performance of the initial verification protocol between the user and the system where j is a positive integer.

The second part of the scheme is tailored for communal verification between a mobile user and a VLR when the user does not leave the service area of the VLR. Similarly, the second part contains two protocols:

C) An initial verification protocol for communal verification and the initialization or reinitialization of the inner one-time secret; and

D) An verification protocol based on the inner one-time secret for the ***k***th verification after the most recent performance of the initial verification protocol between the user and the VLR where k is a positive integer.

2.3 Secure Hash Algorithm (SHA)

NIST published four additional hash functions in the SHA family, named after their digest lengths (in bits): SHA-224, SHA-256, SHA-384, and SHA-512. The algorithms are collectively known as SHA-2. SHA-256 and SHA-512 are novel hash functions computed with 32- and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are simply truncated versions of the first two, computed with different initial values.

SHA 256 Functions

SHA-256 uses six logical functions, where each function operates on 32-bit words, which are represented as x, y, and z. The result of each function is a new 32-bit word.

SHA-256 Constants

SHA-256 uses a sequence of sixty-four constant 32-bit words, K0, K1, K2 …….K63 powered 256. These words represent the first thirty -two bits of the fractional parts of the cube roots of the first sixty four prime numbers.

Preprocessing

Preprocessing shall take place before hash computation begins. This preprocessing consists of three steps: padding the message, M, parsing the padded message into message blocks, and setting the initial hash value, $H^{(0)}$.

Padding the Message

The message, M, shall be padded before hash computation begins. The purpose of this padding is to ensure that the padded message is a multiple of 512 or 1024 bits, depending on the algorithm.

Suppose that the length of the message, M, is l bits. Append the bit "1" to the end of the message, followed by k zero bits, where k is the smallest, non-negative solution to the equation l+1+ k= 448 mod 512. Then append the 64-bit block that is equal to the number l expressed using a binary representation. For example, the (8-bit ASCII) message "abc" has length 8 x 3 = 24, so the message is padded with a one bit, then 448 - (24 +1) = 423 zero bits, and then the message length, to become the 512-bit padded message. The length of the padded message should now be a multiple of 512 bits.

Parsing the Padded Message

After a message has been padded, it must be parsed into N, m-bit blocks before the hash computation can begin.

For SHA-256, the padded message is parsed into N 512-bit blocks, M (1), M (2), up to M(N). Since the 512 bits of the input block may be expressed as sixteen 32-bit words, the first 32 bits of message block i are denoted M(1of power of i to M , the next 32 bits are), M(2),…, M(N).

SHA-256 may be used to hash a message, M, having a length of l bits, where $0<=l<=2^{64}$. The algorithm uses 1) a message schedule of sixty - four 32-bit words, 2) eight working variables of 32 bits each, and 3) a hash value of eight 32-bit words. The final result of SHA-256 is a 256-bit message digest.

Some security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although SHA-2 bears some similarity to the SHA-1 algorithm, these attacks have not been successfully extended to SHA-2. SHA-256 is used to authenticate Debian Linux software packages and in the DKIM message signing standard

3.CONCLUSION

We have proposed a secure communal verification and key swap scheme for mobile communications based on a novel mechanism, i.e., nested one-time secrets. The proposed scheme can withstand the replay attack and the impersonating attack on mobile communications and speed up verification. The proposed scheme reduces the communication and computation cost, also provides the security.

4.REFERENCE

[1] B. Mallinder, “An overview of the GSM system,” in *Proc. 3rd Nordic Seminar Digital Land Mobile Radio Commun.*, Copenhagen, Denmark, 1998, pp. 12–15.

[2] A. Aziz and W. Diffie, “Privacy and authentication for wireless local area networks,” *IEEE Personal Commun.*, vol. 1, no. 1, pp. 24–31, 1993.

[3] M. S. Hwang, Y. L. Tang, and C. C. Lee, “An efficient authentication protocol for GSM networks,” in *Proc. AFCEA/IEEE Euro-Comm*,2000, pp. 326–329.

[4] S. Suzuki and K. Nakada, “An authentication technique based on distributed security management for the global mobility network,” *IEEE J. Sel. Areas Commun.*, vol. 15, no. 8, pp. 1608–1617, Oct. 1997.

[5] C. H. Lee, M. S. Hwang, and W. P. Yang, “Enhanced privacy and authentication for the global system for mobile communications,” *Wireless Netw.*, vol. 5, no. 4, pp. 231–243, 1999.

[6] L. Buttyan, C. Gbaguidi, S. Staamann, and U.Wilhelm, “Extensions to an authentication technique proposed for the global mobility network,” *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 373–376, Mar., 2000.

[7] K. F. Hwang and C. C. Chang, “A self-encryption mechanism for authentication of roaming and teleconference services,” *IEEE Trans. Wireless Commun.*, vol. 2, no. 2, pp. 400–407, Mar. 2003.

[8] C. C. Lee, M. S. Hwang, and W. P. Yang, “Extension of authentication protocol for GSM,” *IEE Proc., Commun.*, vol. 150, no. 2, pp. 91–95, 2003

.

[9] L. Harn and W. J. Hsin, “On the security of wireless network access with enhancements,” in *Proc. ACM Workshop Wireless Security*, 2003, pp. 88–95.

[10] A. Peinado, “Privacy and authentication protocol providing anonymous channels in GSM,” *Comput. Commun.*, vol. 27, no. 17, pp. 1709–1715, 2004.

[11] C. C. Chang, J. S. Lee, and Y. F. Chang, “Efficient authentication protocol of GSM,” *Comput. Commun.*, vol. 28, no. 8, pp. 921–928, 2005.

[12] C. Tang and D. O.Wu, “An efficient mobile authentication scheme for wireless networks,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1408–1416, Apr. 2008.

[13] M. Al-Fayoumi, S. Nashwan, S. Yousef, and A. R. Alzoubaidi, “A newhybrid approach of symmetric/asymmetric authentication protocol for future mobile networks,” in *Proc. Wireless Mobile Comput., Netw. Commun.*, 2007, pp. 29–29.

[14] V. Kalaichelvi and R. M. Chandrasekaran, “Secure authentication protocol for mobile,” *Proc. Comput., Commun. Netw.*, pp. 1–4, 2008.

[15] K. P. Kumar, G. Shailaja, A. Kavitha, and A. Saxena, “Mutual authentication and key agreement for GSM,” in *Proc. ICMB*, 2006, p. 25.