ONE TIME SECRET KEY MECHANISM FOR MOBILE COMMUNICATION

Vasu.R[1] and Dr.Sunitha Abburu[2]

[1]Adhiyamaan College of Engineering, Department of Computer Application, Hosur
vasu.shriram2@gmail.com
[2]Professor and Director, Adhiyamaan College of Engineering, Department of Computer Application, Hosur.
ausunithaa@yahoo.co.in

ABSTRACT

Mobile communication is playing a vital role in the current technical world and becoming more popular and prevalent across the world everyday at one end and many security problems are arising at the other end. To overcome these security problems many security mechanisms for mobile communications have been introduced in the literature. Among these mechanisms, authentication plays a quite important role in the entire mobile network system and acts as the first defense against attackers since it ensures the correctness of the identities of distributed communication entities before they engage in any other communication activity. In this paper, we propose a novel authentication mechanism, called the nested one-time secret mechanism, efficient for mobile communication environment which mainly focus on the security issues of mobile communication and also overcome the problem of high computational and communication cost with good result in reducing the cost of computational and communication cost from the existing system, the cost reduction is possible by reducing the usage of the memory for key generation in the proposed scheme and the experimental result of the proposed scheme is also been showed in this paper.

KEYWORDS

Visitor Locator Registry (VLR), Home Locator Registry (HLR), Third Generation (3G), Wireless LAN (WLAN), Authentication and Key Agreement (AKA).

1. INTRODUCTION

Rapid development of wireless networks are gradually changing the way we live, and security such as authentication of mobile stations is a serious concern for many emerging application. However, there is no trusted authentication server available to mobile users out of its home network. How to achieve mutual authentication between a mobile user and a visited location register [VLR] in wireless networks is an important security issue.

The goal of this paper is dual. First, we provide a comprehensive discussion of security problems and current technologies in 3G and WLAN systems. Second, we provide introductory discussions about the security problems in mobile communication also implementing the proposed scheme that generates the secured key for each transaction between users, which ensure high security.

The proposed scheme maintains security against attacks by unauthorized users. The encryption and decryption of messages over mobile communication can be handled by one time secret key mechanism and the secret key is useful to impersonate the user. In this paper, we propose a one–time secret key user authentication protocol for mobile communication which brings various flexibilities to the system. With the proposed protocol, users can access their accounts using a

generated secret key without being dependent on their password alone. This enables users to communicate between the different users through the Visitor Located Registry.

The rest of this paper is organized as follows. Section 2 gives the literature survey. Section 3 reviews the issues of wireless security which helps to improvise for the implementation of proposed scheme. Section 4 implements the one time secret key mechanism. Section 5 gives the experimental result which shows the performance of proposed scheme. Finally we conclude with conclusion in Section 6.

2. LITERATURE SURVEY

Many mobile authentication schemes have been proposed in recent years for the key exchange. In 2008, Tang and Wu et al, [1] proposed a delegation-based authentication protocol for use in mobile station authentication. It uses an elliptic-curve-cryptosystem based trust delegation (allocation) mechanism to generate a delegation (allocation) pass code for mobile station authentication, and it can effectively defend all known attacks to mobile networks including the denial-of-service attack. Moreover, the mobile station only needs to receive one message and send one message to authenticate itself to a visitor's location register, and the scheme only requires a single elliptic-curve scalar point multiplication on a mobile device. Therefore, this scheme enjoys both computation efficiency and communication efficiency as compared to known mobile authentication schemes but suffers from the replication attack. Under this kind of attack, our proposed one time secret key mechanism address the issue by generating a key for communication between a mobile user and the legal service provider(VLR).

The existing methods faces various challenges, one among them is fixed password approach. In this approach unauthorized users can misuse and steal the authenticated user identity. A hacker can break the password trying many possible guesses offline. If such a weak secret key is used as a security mechanism, providing mobile communication security becomes challenge to the service provider. Strong password protocols were proposed to solve this problem by Qiyan et al, [2] proposes a novel signature model – Time Valid One-Time Signature (TV-OTS) – to boost the efficiency of regular one-time signature schemes. Based on the TV-OTS model an efficient multicast authentication scheme "TV-HORS" combines one-way hash chains with TV-OTS to avoid frequent public key distribution. It provides fast signing/verification and buffering-free data processing, which make it one of the fastest multicast authentication schemes to date in terms of end-to-end computational latency. TV-HORS is tolerance to packet loss and strong robustness against malicious attacks. The only drawback is its relatively large key size. Ammayappan et al, [3] propose an improvement to the GSM authentication protocol, based on Elliptic Curve Cryptography, that offers enhanced security provides mutual authentication, requires less storage and avoids replay attack. The proposed approach requires less memory size for key generation.

In 2003, Hwang and Chang's et al, [4] scheme proposed a mutual authentication and key exchange protocols and Yixin et al, [5] proposes a authentication protocol for teleconference services that includes identity anonymity (secrecy), one-time *PID* (pseudonym identity) renewal and location intractability. It is shown that the security has been significantly enhanced, while the computation complexity is similar to the existing one appeared in the literature. The computation requirement for mobile device is quite low. Maria et al, [6] focuses on the design of key management (KM) for the environment of Mobile Ad Hoc Networks (MANETs). KM ensures communication security among nodes and the capability of their cooperation as a secure group. It consists of key generation, user authentication and key distribution services. KM address key distribution, group key generation, entity authentication by emphasizing that the entity authentication should be designed with key distribution algorithms and vice versa. An

entity authentication scheme based on the Merle Tree algorithm, applied on a key generation protocol to produce an efficient, scalable and secure KM scheme.

Lamport et al, [7] method of user password authentication, is secure even if an intruder can read the system's data, and can tamper with or eavesdrop on the communication between the user and the system. The method assumes a secure one-way encryption function and can be implemented with a microcomputer in the user's terminal. James et al, [8] defined first description of security model for authenticated key exchange protocols with predicate-based authentication. Predicate-based key exchange is defined in terms of non-interactive algorithms so that it is independent of any networking layer for message delivery. The method does not specify how the user determines what predicates to use or to which session an incoming message belongs but a key-exchange protocol should be substrate-neutral. Traditional symmetric cryptography [9] is based on the sender and receiver of a message knowing and using the same secret key. The sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message. However the main problem in this scheme is in getting the sender and receiver to agree on the secret key without anyone else getting to know it. Our approach requires an initial password to use the secret key so it does not lead to any known attacks by the unauthorized users. In [10] new authentication schemes for third generation mobile radio systems is been discussed. These new requirements are motivated by the expected upcoming of many new network operators and service providers. Thus, an explicit mutual authentication of the user and the network operator is required. Mutual authentication of users and network operators can be achieved either by symmetric or asymmetrical authentication schemes.

In fact, it is difficult to satisfy the above assumption in current mobile communication environments. In this paper, we discuss the performance of secure mutual authentication schemes and come up with an efficient solution to further simplify and speed up the authentication processes. This is achieved 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 authentication or authentication 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 mutual authentication between the user and the same VLR. Compared to the existing schemes, the proposed scheme greatly reduces the computation cost required for each mobile user at efficient rate. The cost reduction in the proposed scheme is based on the less usage of memory for generating the random strings, encryption and decryption of the key, unlike the memory usage in existing system is high it leads to increase in computational cost. In addition, the proposed scheme is formally demonstrated as being protected to both the replay attack and the impersonating attack.

3. WIRELESS SECURITY IN MOBILE COMMUNICATION

The various issues of wireless security and techniques are discussed in this section which describes about the secure authentication in mobile communication.

3.1 Techniques for privacy and authentication in personal communication systems

Describes progress in the development of authentication and key agreement (AKA) processes for personal communication systems (PCS).A conceptual framework is first established, this is a three-part general model that characterizes all AKA techniques. Then three proposed AKA methods are compared using novel authentication model. These methods are the secret key method of GSM, the secret key method of United States Digital Cellular (IS-54, IS-95), and a public key/secret key method. Finally, a summary is presented that indicates the AKA method of preference for some proposed PCS air interfaces that are under development by standards bodies.

3.2 Privacy and authentication for wireless local area networks

Wireless networks are being driven by network access to mobiles or nomadic computing devices. Although the need for wireless access to a network is evident, new problems are inherent in the wireless medium itself. Specifically, the wireless medium introduces new opportunities for eavesdropping on wireless data communications. Anyone with an appropriate wireless receiver can eavesdrop, and this kind of eavesdropping is virtually undetectable. Furthermore, since the wireless medium cannot be contained by the usual physical constraints of walls and doors, active intrusions through the wireless medium are also made easier. In order to prevent this unauthorized access to the network, Burrows (1990) present the design of a secure communication protocol that provides for both the privacy of wireless data communications and the authenticity of communicating parties. The placement of the protocol in the overall protocol stack and issues relevant to wireless links and mobile computing devices are discussed. They also present proof of the security of the protocol using the logic of authentication formalism developed by Burrows.

3.3 An efficient authentication protocol for GSM networks

Today, the Global System for Mobile Communications (GSM) is widely recognized as the modern mobile network architecture. A large portion of GSM network traffic is a produced by constant signaling between mobile stations and the base stations. In order to reduce the network traffic, various security protocols have been proposed.

3.4 An authentication technique based on distributed security management for the global mobility network

This paper proposes an authentication technique for use in the global mobility network (GLOMONET), which provides a personal communication user with global roaming service. This technique is based on new distributed security management, where authentication management in roaming-service provision is conducted only by the roamed network (the visited network). The original security manager (OSM) administrates the original authentication key (OAK) acquired when a user makes contracts with the home network, while the temporary security manager (TSM) is generated for a roamer in the visited network in order to provide roaming services. The TSM generates and administrates the temporary authentication key (TAK) for a roamer, which key is confidential to the OSM, releases the TAK administration when a roamer moves to other networks, and then disappears.

The proposed authentication technique consists of two phases. In the roaming-service-setup phase, triggered by the user's location registration request, authentication control to set up the roaming-service environment is negotiated by the TSM in the visited network, the OSM, and the roamer. In the roaming-service-provision phase, triggered by the user's service request, authentication control to provide the roaming service is negotiated (using the TAK acquired by the roamer in the first phase) only by the visited network and the roamer. This authentication control using the TAK provides a unified authentication procedure with a single logic to both subscribers and roamers. In addition, the security management of the whole GLOMONET is reinforced and the security responsibility is made clear by allocating the subscriber's/roamer's security administration to only the TSM.

3.5 Wireless Network Security and Interworking

A variety of wireless technologies have been standardized and commercialized, but no single technology is considered the best because of different coverage and bandwidth limitations. Thus, interworking between heterogeneous wireless networks is extremely important for

ubiquitous and high-performance wireless communications. Security in interworking is a major challenge due to the vastly different security architectures used within each network.

4. ONE TIME SECRET KEY MECHANISM

We propose a fast mutual authentication and key exchange scheme for mobile communications. Our scheme consists of two parts and each of the two parts contains two protocols.

The first part of the scheme is designed for mutual authentication between a mobile user and the system (a VLR and the HLR) where it includes two protocols:

1) An initial authentication protocol for mutual authentication and the initialization of the outer one-time secret.
2) An authentication protocol based on the outer one-time secret for the jth authentication after the most recent performance of the initial authentication protocol in this section between the user and the system where is a positive integer second part of the scheme is modified for mutual authentication between a mobile user and a VLR when the user does not leave the service area of the VLR.

The second part contains two protocols:
1) An initial authentication protocol for mutual authentication and the initialization of the inner one-time secret.
2) An authentication protocol based on the inner one-time secret for the kth authentication after the most recent performance of the initial authentication protocol between the user and the VLR where a positive integer.

4.1 The Initial Authentication Protocol for Mobile User and the System

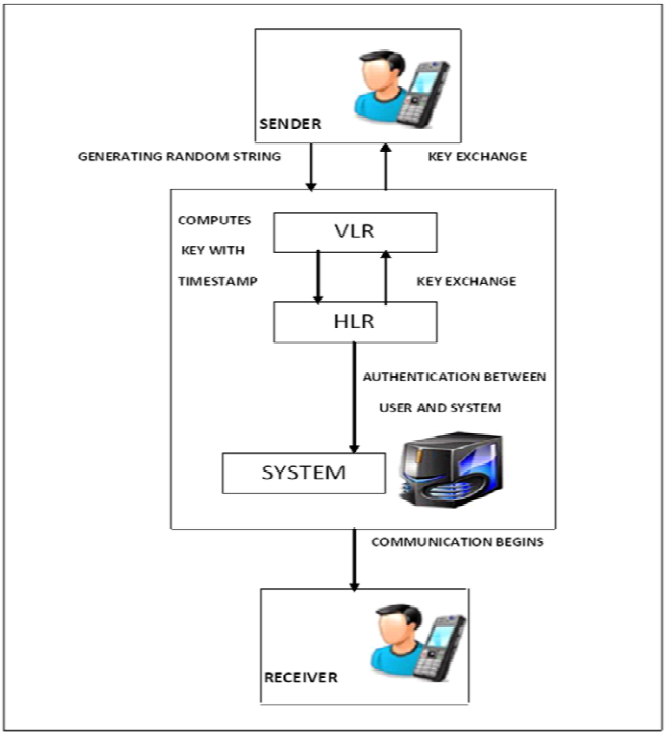

Figure 1 System Architecture.

Figure 1 shows the system architecture for one time search key mechanism. The user must perform the initial authentication protocol for authentication and initializing the outer one-time secret if one of the following two conditions occurs:

1) Requests to be authenticated by the system at the first time.

2) The protocol of the initial authentication is not successfully finished.

The details of the initial authentication protocol are described as follows:

Step (1): Randomly generates a string, and then forms key and sends to VLR.

Step (2): After receiving the key by VLR, VLR computes it again with time stamp and sends to the HLR.

Step (3): The HLR decrypts and checks if the key is not expired. If true, the HLR decrypts to obtain and randomly chooses three strings and re computes and then sends to VLR, where is the timestamp made by the HLR, the HLR sets and stores.

Step (4): VLR decrypts to obtain the key and checks if key is not expired based on the time stamp of HLR. If true, it will be sent to user.

Step (5): User decrypts and checks if identical to the one is produced in step1. If it is true, then it will be sent to VLR. In addition, sets and stores.

Step (6): Verifies whether security key identical to the one it obtained in step 4 or not. If true, then the system (and the HLR) have mutually authenticated each other and synchronized.

i.e., the initial value of the outer one-time secret is successful. Otherwise, the authentication fails, and HLR will be discarded. The string is used as a common secret key for mutual authentication between and in the next authentication activity if the user still stays in the service area of then.

4.2 The jth Authentication Protocol for Mobile User and the System

User performs the protocol based on the outer one-time secret for authentication up to the user visits a new VLR and the most recent authentication between the user and the system was successfully completed. The jth mutual authentication protocol for the user and the system after the successful execution of the protocol in this section is described below, where j is a positive integer. The initial value of j is reset to 1 whenever the previous round of authentication was successfully completed through performing the protocol of this section.

Step (0): The jth authentication process begins.

Step (1): User randomly generates two strings for example x and y the two strings are computes. Then, sends to VLR which is the current VLR visited by user.

Step (2): After receiving the randomly generated key the VLR computes the key along with the timestamp and sends to the HLR, where is the timestamp made by VLR.

Step (3): The HLR decrypts and checks if is not expired. The HLR decrypts to obtain the two strings x and y and then HLR retrieves according to where the timestamp made by HLR. HLR deletes and stores.

Step (4): VLR decrypts and then checks and sends to user.

Step (5): User checks if identical to the one is produced in **Step** (1). If it is true and the system have mutually authenticated each other successfully deletes and stores, i.e., the new value of the outer one-time secret. Besides, and take as the session key for secure communication in this session. The string is used as a common secret key for mutual authentication between and in the next authentication activity if still stays in the service area of then.

Step (6): The jth authentication process ends. If wants to perform the above protocol for the next round of mutual authentication between the system and user, user again want to set j=j+1 and goes to **Step** (0).

4.3 The Initial Authentication Protocol for User and the Current VLR

User performs the protocol for mutual authentication with the current VLR and initializes an inner one-time secret for roaming services with the VLR when one of the following two conditions occurs:

1) The most recent authentication is successfully finished by performing the protocol of this section and user should stay in same service area of the current VLR.

2) The protocol of this section is not successfully finished, and does not leave the service area of the current VLR. The details of the initial authentication protocol for user and the current VLR are described as follows.

Step (1): Randomly generates a string she/he computes and sends to VLR.

Step (2): VLR decrypts by using the common secret key to get. It randomly chooses two strings and then computes and sends to HLR.

Step (3): After decrypting obtains the key and she/he checks if is equal to the one produced in step 1. If the key is true, then it will be sent to VLR.

Step (4): VLR gets and checks if the key is equal to the one that it has chosen. If true, authentication is successfully made between each other and shares an initial common one-time secret along with a session key successfully.

4.4 The kth Authentication Protocol for User and the Current VLR

User performs the protocol based on the inner one-time secret for mutual authentication as long as does not leave the service area of the current VLR and the most recent authentication was successfully finished via the protocol of this section. The kth mutual authentication protocol for the user and the current VLR after successful execution of the protocol in this section is described below. The initial value is reset to 1 whenever the most recent authentication was successfully completed through performing the protocol this section.

Step (0): The kth authentication process begins.

Step (1): Randomly chooses a string and computes and then sends to VLR.

Step (2): After decrypting gets and it checks if is equal to VLR timestamp. If it is true, sends to and then deletes and stores.

Step (3): HLR gets and checks if it is equal to the one produced in step1. If true, and authenticate each other and share a session key successfully deletes and stores.

Step (4): The kth authentication process ends. If user wants to perform the next round of authentication process, she/he sets k=k+1 and goes to **Step** (0).

Finally, the proposed scheme integrated into a complete and fast authentication scheme for mobile communication.

5. EXPERIMENTAL RESULT

Mobile subscriber MS is to be authenticated to the HLR via the VLR, using his/her password. KHLR is the public key of the HLR known to all parties, and K VLR is the symmetric encryption key shared between the VLR and HLR.

The main difference between the proposed protocol and the current GSM authentication protocol regarding the protocol performance is the use of the public key operations. In the novel authentication mechanism, called the one-time secret key mechanism, the cost of encryption is about 30-33 times less than the cost of existing systems. The current protocol is designed with this fact in mind to minimize the communication and computational cost which does nested one public key operation.

	Existed System	Proposed Scheme	Difference
For Each User			
Generating Random Strings	1280 b	512 b	768 b
Hashing Process	0	256 b	256 b
Encryption & Decryption	256 b	256 b	0
Communication Cost	1536 b	1024 b	Reduced by 512 b
For Entire Protocol			
Generating Random Strings	512 b	256 b	256 b
Hashing Process	0	512 b	512 b
Encryption & Decryption	3960 b	3568 b	392 b
Computational Cost	4472 b	4336 b	Reduced by 136 b

Table.1 Comparisons of Existed System and Proposed Solution Based on Memory Usage.

In the table 1, the usage of the memory for various purposes such as generating random strings, hashing process, encryption and decryption is compared between the existing system and proposed scheme, which describes that the existing system using more memory size for the key exchange process, it leads to high computational and communication cost where as in proposed scheme usage of the memory is minimized and the communication and computational cost reduced. Thus, the proposed scheme is more secure in authentication process and also at very efficient cost.

6. CONCLUSION

We have proposed a secure mutual authentication and key exchange scheme for mobile communications based on a novel mechanism, i.e., nested one-time secrets. The proposed scheme is strong user authentication protocol for GSM that permits users to access their accounts remembering only a password without being limited to their SIM card. The proposed scheme reduces the communication and computation cost, also security scheme is very efficient.

An improved one time secret key based key exchange protocol which is secure to undetectable password attacks is proposed. The proposed protocol is achieving better performance efficiency by requiring less numbers of random elements. The above theoretical and experimental results show that the proposed protocol is secure, efficient and practical.

REFERENCES

[1] Tang and D. O.Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE Transactions on Wireless Communications, Volume 7, Issue 4, April 2008 pp. 1408 - 1416.

[2] Qiyan Wang, Khurana, H, Ying Huang, Nahrstedt, K, "Time Valid One-Time Signature for Time-Critical Multicast Data Authentication", IEEE-Infocom, April 2009, pp 19-25.

[3] Ammayappan, K. Saxena, A. Negi A, "Mutual Authentication and Key Agreement based on Elliptic Curve Cryptography for GSM" , International Conference on Advanced Computing and Communications (ADCOM), 20-23 Dec 2006 , pp 183 - 186.

[4] K. F. Hwang, C. C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," IEEE Transactions Wireless Communications, vol. 2, no. 2, Mar. 2003, pp. 400–407.

[5] Yixin Jiang and Chuang Lin, Minghui Shi and Xuemin (Sherman) Shen, A Self-Encryption Authentication Protocol with Identity Anonymity for Teleconference Services" IEEE Globecom 2005

[6] Maria Striki, John S. Baras, "Towards Integrating Key Distribution with Entity Authentication for Efficient, Scalable and Secure Group Communication in MANETs", IEEE International Conference on Communications, Vol.7, Inst. for Syst. Res., Maryland Univ., College Park, MD, USA, 20-24 June 2004, pp 4377 – 4381.

[7] L. Lamport, "Password Authentication with Insecure Communication", *Communications of the ACM*, 24(11), November 1981, pp 770-772.

[8] James, Birkett, Stebila, Douglas, "Predicate-Based Key Exchange", *Information Security and Privacy: Proceedings of the 15th Australasian Conference, ACISP 2010*, Springer, Macquarie Graduate School of Management, Sydney.

[9] Atul Chaturvedi, Shyam Sundar, "A Secure Key Agreement Protocol Using Braid Groups Department of Mathematics", Internationnal Journal of Advanced Networking and Applications (IJANA), Volume: 01, Issue 05, 2010, Pages: 327-330.

[10] Stefan Piitz, Roland Schmitz, Friedrich Tonsing, "Authentication Schemes for Third Generation Mobile Radio Systems", The Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Boston, MA , USA, vol.1, 8-11 Sep 1998, , pp 126 – 130.