Indian Journal of Science and Technology, Vol 8(15), DOI: 10.17485/ijst/2015/v8i15/72941, July 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Multi-factor User Authentication on Group Communication

Sunghyuck Hong*

Division of Information and Communication, Baekseok University, Korea; shong@bu.ac.kr

Abstract

Group communications are becoming popular by explosively increased Internet usage, and there are various group communications on Internet applications such as video conferences, on-line text chatting programs, online games and gambling. However, the conventional group key agreement protocols are only focused on how to minimize the computational overhead by concentrating on generating the common group key efficiently. As a result, the common group key is generated efficiently. However, a failure in user authentication permits unknown attackers to obtain valuable information during the group communication. This paper proposes a Media Access Control (MAC)-based authentication in the group key agreement in order to secure the user authentication process in group communications. Without a preliminary agreement, participants in a group communication cannot trust each other in the beginning of the group setup. Therefore, the group controller, who is randomly selected from the group members, needs a security deposit from all members in case an illegitimate user tries to join the group. The user MAC address proposed in this paper can act as a security deposit to provide a secure communication channel while preventing the MAC spoofing problem.

Keywords: Authentication, Component, Group Key Agreement, Group Member Identity, MAC Address

1. Introduction

Authentication in distributed computing networks is the process of verifying users, hosts, processes, which request and consume resources on behalf of associated users[1].

In the 1993 edition of The New Yorker, Peter Steiner published a cartoon that showed a dog explaining to another dog the major advantage of the Internet with the statement "on the internet, nobody knows you are a dog"[2]. At the beginning of communication, group members must agree to trust a minimum of one entity, such as a Trust Third Party, for communicating each other. A security hole starts from this precondition. No perfect secure system exists. Therefore, all systems can be hacked and there are no exceptions to this rule[3].

As mentioned above, conventional authentication methods are not adequate for dynamic peer groups in the beginning of communication. Thus a different authentication method is needed to achieve a secure user authentication in dynamic peer group communication. The main idea presented in this paper is to establish a physical location as user identity. A MAC (Media Access Control) address can make an adversary hard to break into the system. However, MAC spoofing is the biggest concern in a MAC-based authentication scheme. A Secure Address Resolution Protocol (SARP)[6] potentially can be used to prevent MAC spoofing; so MAC-based authentication can be a good solution to authenticate user identity at the beginning of group communication.

2. Authentication Problem

According to[13], there are three main methods of authentication. The first is password-based, the second is software-based and the last is hardware-based. Passwords and Personal Identification Numbers (PINs) are the most common examples of a "something you know" method of authentication for computer systems. If the user in the password-based authentication system simply types the password that matches with the password in the system, then the user authentication process is complete. The major advantages are simple to access the system, no

*Author for correspondence

additional cost for authentication, and no further effort being required to check identity. Most users tend to select a password that is easy to remember and related to personal information such as names and dates of birth. In addition, most users do not change passwords regularly, further decreasing user security.

Software-based key authentication is "something you have" such as a certificate which is issued by a Certificate Authority (CA) or a Trust Third Party (TTP). The software certificate provides a means of authenticating user identity. This approach can avoid password-based authentication problems. However, establishment costs are higher than the password-based authentication because a CA is required to issue certificates to the users.

Hardware-based key authentication uses a physical device such as a Smart Card to hold the user credentials, such as a private key or an encryption key. The user credentials are more secure since the information is stored on the Smart Card and not on the server. An adversary has a chance to steal the user credential only when the user uses the Smart Card. However, there are costs incurred to build a smart card security system and the Smart Card can be stolen and misplaced.

Each authentication method has advantages and disadvantages. The right one needs to be chosen for each individual situation. Password-based and software-based key authentication schemes are suitable for non-collaborative, centrally managed, one-to-many broadcast groups such as those encountered in Internet multicast. However, most group communications are peer to peer. Any member can be a sender or a receiver and there is no central controller like a server. Therefore, the dynamic group communication needs a different authentication method due to the characteristics of the group communication, thus, the MAC-based authentication is proposed as a different form of authentication. MAC-based user authentication does not depend on "something you have" nor on "something you know" but on the user's physical location in the network. In other words, the user's physical location is the user's identification.

Most of the Group Key Agreement (GKA) protocols do not have identity authentication because they assume that members know each other. Even though, group communications use the Secure Spread Library for communication privacy and message integrity[4]. Most authentication processes in group communication use a preliminary agreement and focus on the person who uses computers or network devices such as a mobile phone, videoconference, and a game console. The preliminary agreement, that can prevent a MIMA in the group communication is not supposed to be exposed to non-group members. However, there is the possibility of user identity being stolen by an adversary. No matter how secure the key confirmation being used is, or how good the preliminary agreement protocol is, an adversary, who knows the preliminary agreement, can successfully pass over the key integrity process that verifies the key that belongs to each communicating party. User authentication must verify user identification without a preliminary agreement since an adversary could have a chance to steal the preliminary agreement. Therefore, only the intended user must use the user identification.

In most GKA protocols the focus is on generating the Common Group Key (CGK) efficiently for encrypting and decrypting messages during the group communication. Each member contributes an equal share to the CGK by using modular exponentiation[5]. The N-party Diffie-Hellman (DH) key exchange, an extension of the DH key exchange, provides secure communication to group members. However, neither entity authentication nor key confirmation is provided in the DH key exchange scheme[6,17] and most GKA protocols have been using the DH key exchange scheme. In addition, there is no verification of group member identities. When group members assume to know each other's identity, the GKA protocol bypasses any authentication procedure and starts to generate the CGK and distributes the CGK to each member. The lack of an authentication mechanism jeopardizes integrity and confidentiality because if an unidentified user impersonates a member of the group and contributes to the group key, he then gains access to the CGK and will be able to decrypt messages that have been encrypted by the CGK. Therefore, the authentication process becomes an even more important process than generating CGK for a secure communication.

3. Group Key Management

Before a communication session begins each party must establish a secure communication channel. Unless the channel is secure, messages over the network will be in danger of being delivered to the right destination. Group key management is used for building a secure channel.

There are two types of schemes in the group key management. One is group key distribution and the other is

group key agreement. One of the members in the group is responsible for key distribution, so key distribution computes the group key and distributes it to each member in the group. This scheme is suitable for client-server environments like multicast. Each member has an equal opportunity for generating the group key. One of the group members takes the role of the group controller who collects all partial group keys and computes the CGK and then distributes it to each member. This scheme is suitable for peer-to-peer group communication[14-16].

In this context key distribution or key agreement is the cornerstone for a secure communication. CLIQUES[5] is an example of a GKA protocol developed for key agreement in dynamic groups. However, CLIQUES does not have entity authentication. The group key agreement itself has data source authentication, which means that all key agreement protocol messages are signed by the sender and verified by all other participants. In order to authenticate members in the group, CLIQUES uses Secure Spread entity authentication that is assumed to be performed when a member connects to the system and the Secure Spread uses Open SSL, an open source toolkit for cryptography. Open SSL provides the creation of the RSA cryptosystem, named after its inventors R. Rivest, A. Shamir, and L. Adleman, is the most widely used public-key cryptosystem[7,8], DH key parameters, creation of X.509 certificates, message digests, and data encryption and decryption. Authentication processes in Open SSL are based on X.509 certificate. The certificate-based authentication should have a Trusted Third Part that issues a certificate to members. However, dynamic peer group communication needs a different method of authentication because password-based and certificate-based (software-based key) authentication processes are not validated in the group membership authentication.

4. Multi-factor User Authentication

Security is priority number one since someone else could obtain a user's identity, then the trustworthy relationship in the group communications will be jeopardized.

A method for authenticating an individual's membership in a dynamic group without revealing the individual's identity is presented in[10]. Some members hesitate about revealing their identities due to the danger of being used by someone else. According to[11], identity theft now ranks as America's fastest-growing crime, claiming nearly 10 million victims in just the last 12 months and at a cost of more than $53 billion. Consequently, using an identity for authentication, which can be transferred to someone else, is not a perfect solution in group communication. Computer networking is facing the same problem as the real world. Sometimes, someone can use other's identification. This is a serious problem for user identification.

Figure 1 shows the overview of the MUA (Multi-factor User Authentication) protocol. Once a group is formed with Secure Spread Library, then randomly select one of the members as a group controller who will be responsible for obtaining each member's MAC address and distributing the Common Group Key (CGK) to group members.

The SARP protocol is assumed as being performed when group members exchange MAC addresses. Each member encrypts its MAC address with a group controllers' public key and sends its encrypted MAC address to the group controller. A group controller obtains the MAC addresses and decrypts the MAC address with his private key that is associated with the public key. Finally, the group controller distributes an exponentiation base 'g' to each member with the verifying members' MAC address. Each member M_i selects a random private number r_i and computes $M_i = g^{ri} \; mod \; p$. Table 1 shows the definitions in a group key generation tree. A binary tree is used for the key generation processes because if a tree is perfectly balanced, then the CGK computational overhead relatively as low as $O\ (log\ n)$.

Figure 2 shows an example of a key tree to generate the CGK in the MGDH protocol. If a parent node is $<l, v>$, then he has two children nodes, $<l+1, 2v>$ and $<l+1, 2v+1>$. Leaf nodes are member nodes. Every key $K<l,v>$ is computed as follows:

$$K<l,v> = g^{K<l+1,2v>\ K<l+1,2v+1>} \; mod \; p \qquad (1)$$

Equation (1) is computed with two exponents, which are the blind keys of nodes, $<l+1, 2v>$ and $<l+1, 2v+1>$. Each node in the tree performs computations as exemplified in Table 1, 2. The MGDH protocol adds a MAC-based authentication in the GDH[13]. The MAC address-based user authentication protocol is more secure than the conventional GDH, which lacks the user authentication processes.

In addition, the basic concept of MGDH is not that the user authentication is based on something the user had nor something the user knows, but on the user's physical location instead.

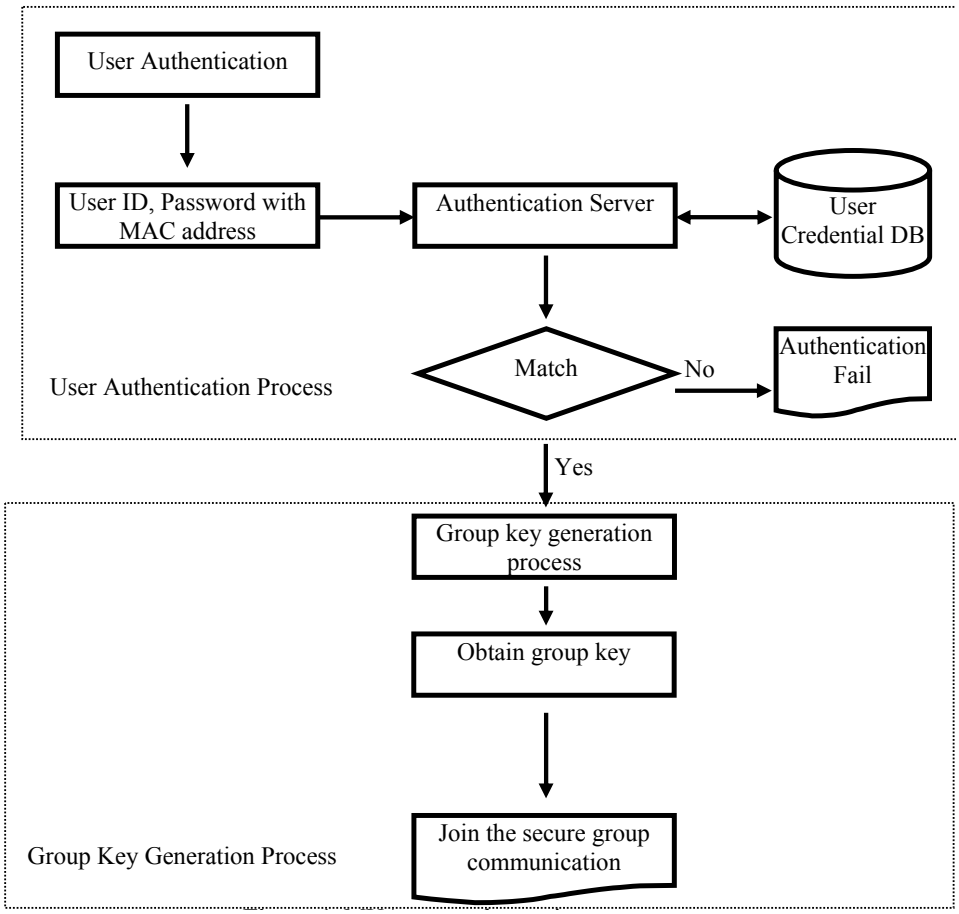

Figure 1. MUA protocol overview.

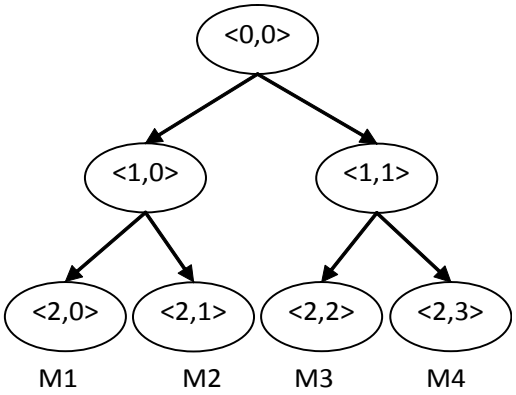

Figure 2. The notation of a group key generation tree.

Table 1. Notation

n	Maximum number of group members
$<l, v>$	v-th node at level l in the group key generation tree (where $0 \le v \le 2^l - 1$)
M_i	i-th group member; $i \in [1,n]$
Z_p^*	Integer set; $Z_p^* = \{1, 2, \ldots, p-1\}$
g	Exponentiation base; $g \in Z_p^*$
p	A large prime number; $p \in Z_p^*$
$K<l,v>$	Mi's session random key
$f(k)$	$g^k \bmod p$

4.1 MAC Spoofing

MAC spoofing is a serious threat in the MAC-based authentication. However, the use of SARP can prevent use of the MAC spoofing programs. The Address Resolution Protocol (ARP) is an essential function used by a sending wired Network Interface Card (NIC) to find the physical address of a destination NIC[9]. ARP is used for connecting another computer by ftp or telnet.

4.2 The Problem

The user in the network who needs to send the data will have the IP address of destination, but the sending NIC must use ARP to discover the corresponding physical address. The

Table 2. Key Calculation

Node	Computation
<0,0>	$g^{r1r2r3r4}$ mod p
<1,0>	g^{r1r2} mod p
<1,1>	g^{r3r4} mod p
<2,0>	g^{r1} mod p
<2,1>	g^{r2} mod p
<2,2>	g^{r3} mod p
<2,3>	g^{r4} mod p

address is obtained by broadcasting an ARP request packet that announces the IP address of the destination NIC. All stations hear the request and the station having the corresponding IP address will return an ARP response packet containing the MAC address and IP address. The sending station will then include this MAC address as the destination address in the packet being sent. The sending station also stores the corresponding IP address and MAC address mapping in a table for a period of time or until the station receives another ARP response from the station having that IP address. At this time, MAC spoofing can happen. For example, an adversary can fool a station by sending the MAC address from a malicious network device. A false ARP response, which includes the IP address of a legitimate network device and the MAC address of the rogue device, could cause all legitimate stations on the network to automatically update their ARP tables with the false mapping.

4.3 Solution

MAC addresses and IP addresses are not private; a malicious adversary who accessed the ARP table can make them available. Therefore, MAC spoofing is the biggest concern in a MAC-based authentication scheme. A Secure ARP (SARP)[12] can be potentially used to prevent MAC spoofing. SARP is an enhancement to ARP that provides a special secure tunnel between each client and router, which ignores any ARP responses not associated with the clients on the other end of the secure tunnels. Therefore, only legitimate ARP responses provide the basis for updating ARP tables. Only if SARP is installed on the client side of the stations, can the stations implement SARP to prevent MAC spoofing.

5. Conclusion

The major premise in this paper is that there is not a perfect system in the present and that no perfect system will exist in the future. Every security effort only makes it harder for adversaries to break into the system. Group communication needs a secure communication channel to prevent eavesdropping on messages. The group key agreement uses a SSL (Secure Spread Library) for secure communication. In spite of using SSL, there is nothing that inspires trust in the beginning of communication. Every group member must agree to trust one thing - a trusted third party - and then finally the trust relationship will grow and expand. In the meantime, if an adversary joins the group and pretended to be a legitimate group member at the beginning of the communication stage, there is no way to prevent this Early Bird Attack (EBA). This paper proposes the use of a Media Access Control (MAC) address as a security deposit in the beginning of communication stage and it contributes to secure the group member authentication while the MAC spoofing problem is avoided. Therefore, a potential adversary might hesitate to join the group if the originating physical location is revealed. As a result, the secure user authentication process in the group communication can be guaranteed as the MAC-based authentication is being used.

Checking the efficiency and performance of MGDH's protocol is currently under investigation.

6. Acknowledgment

This research is supported by 2015 Baekseok University research fund.

7. References

1. Linn J. Practical authentication for distributed computing. 11th IEEE Symposium on Research in Security and Privacy; 1990. p. 31–40.
2. Peter S. The New Yorker. 1993; 69(20):61.
3. Garms J, Somerfield D. Professional Java Security. Wrox Press; 2001.
4. Amir Y, Kim Y, Nita-Rotaru C, Schultz J, Stanyon J. Secure group communication using robust contributory key agreement. IEEE Transactions on Parallel and Distributed System. 2004; 15(5):468–80.
5. Michael S, Gene T, Michael W. CLIQUES: a new approach to group key agreement. 18th international conference on distributed computing systems; 1998. p. 380–7.
6. Gouda MG, Huang C-T. A secure address resolution protocol. Computer Networks. 2003; 41:57–71.

7. Menezes A, van Oorschot P, Vanstone S. Handbook of Applied Cryptography. CRC Press; 1996. p. 285.
8. Linn J. Practical authentication for distributed computing. Proceedings of 11th IEEE Symposium on Research in Security and Privacy; 1990. p. 31–40.
9. Kim Y, Adrian P, Gene T. Tree-based group key agreement. ACM Trans Inf Syst Secur. 2004; 7(1):60–96.
10. Pang S, Kim D, Bang S. Membership authentication in the dynamic group by face classification using SVM ensemble. Pattern Recognition Letters. 2003; 24(1–3):215–25.
11. Dwan B. Identity theft. Computer Fraud and Security. 2004; 4:14–7.
12. Steiner M, Tsudik G, Waidner M. Diffie-hellman key distribution extended to group communication. ACM Conference on Computer and Communication Security; 1996. p. 31–7.
13. Smith RE. Authentication from passwords to public keys. Addison Wesley; 2002.
14. Muthumayil K, Rajamani V, Manikandan S, Buvana M. A group key agreement protocol based on stability and power using Elliptic curve cryptography. 2011 International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT); 2011. p. 1051–6.
15. Kumar K, Nafeesa Begum J, Sumathy V. A novel approach towards cost effective region-based group key agreement protocol for secure group communication. International Journal of Computer Science and Information Security. 2010; 8(2):65–74.
16. Rajeswari PG, Thilagavathi K. An efficient authentication protocol based on elliptic curve cryptography for mobile networks. IJCSNS International Journal of Computer Science and Network Security. 2009; 9(2):176–85.
17. Kaabneh K, Al-Bdour H. Key exchange protocol in elliptic curve cryptography with no public point. American Journal of Applied Sciences. 2005; 2(8):1232–5.