A GROUP KEY MANAGEMENT APPROACH FOR MULTICAST CRYPTOSYSTEMS

[1] M .V.VIJAYA SARADHI, [2] BH.RAVI KRISHNA

[1]Assoc.Prof & HOD, Department of Computer Science & Engineering (CSE), ASTRA

[2]Asst. Prof., Department of Basic Sciences & Humanities, VIGNAN-VITS

Email: meduri_vsd@yahoo.co.in, ravikrishnabh@gmail.com

ABSTRACT

The security in the multicast communication in the large groups is the major obstacles for effectively controlling access to the transmitting data. The IP Multicast itself does not provide any specific mechanisms to control the intruders in the group communication. Group key management is mainly addresses upon the trust model developed by Group Key Management Protocol (GKMP). There are several group key management protocols that are proposed, this paper will however elaborate mainly on Group key management which has a sound scalability when compared with other central key management systems. This paper emphases protocol which provides a scope for the dynamic group operations like join the group, leave the group, merge without the need of central mechanisms. An important component for protecting group secrecy is re-keying. With the combination of strong public and private key algorithms this would become a better serve to the multicast security.

Key words: *Group Key Management, Scalability, Secure Multicast; Re-Keying.*

1. INTRODUCTION

1.1 Unicast - Broadcast Multicast

The multicast group can be identified with the class D IP address so that the members can enter or leave the group with the management of Internet group management protocol. The trusted model gives a scope between the entities in a multicast security system. For secure group communication in the multicast network, a group key shared by all group members is required. This group key should be updated when there are membership changes in the group, such as when a new member joins or a current member leaves. Along with these considerations, we take the help relatively prime numbers and their enhancements that play a vital role in the construction of keys that enhances the strength for the security.

Multicast cryptosystems are preferably for sending the messages to a specific group of members in the multicast group. Unicast is for one recipient to transfer the message and 'Broadcast' is to send the message to all the members in the network. Multicast applications have a vital role in enlarging and inflating of the Internet. The Internet has experienced explosive growth in last two decades. The number of the Internet users, hosts and networks triples approximately every two years. Also Internet traffic is doubling every three months partly because of the increased users, but also because of the introduction of new multicast applications in the real world such as video conferencing, games, atm applications etc.. broad casting such as www, multimedia conference and e-commerce, VOD (Video on Demand), Internet broadcasting and video conferencing require a flexible multicasting capability. Multicast is a relatively new form of communications where a single packet is transmitted to more than one receivers. The Internet does not manage the multicast group membership tightly. A multicast message is sent from a source to a group of destination hosts. A source sends a packet to a multicast group specifying as the multicast group address. The packet is automatically duplicated at intermediate routers and any hosts that joined the group can receive a copy of the packet. Because a host can receive transmitted data of any multicast groups, secure communications is more important in multicasting than in unicasting.

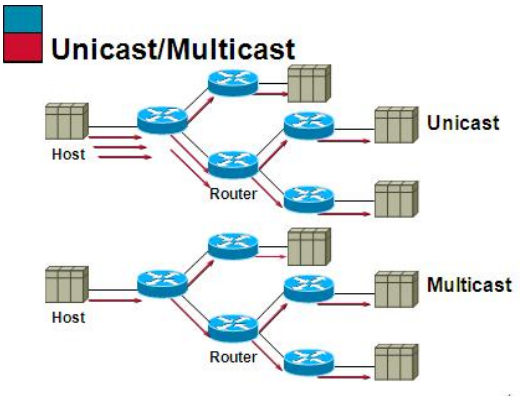

Figure 1.1: Unicast/Multicast Communication through routers

Another important feature of multicasting is its support for data casting applications. Instead of using a set of point-to-point connections between the participating nodes, multicasting can be used for distribution of the multimedia data to the receivers.

1.2 Multicast – Addressing

IPv4 multicast addresses are defined by the leading address bits of 1110, originating from the class D network design of the early Internet when this group of addresses was designated as Class D. The classless Inter-Domain Routing (CIDR) prefix of this group is 224.0.0.0/4. The group includes the addresses from 224.0.0.0 to 239.255.255.255. Address assignments from within this range are specified in an Internet Engineering Task Force (IETF) [3], Best Current Practice document, BCP 51, also known as RFC 3171.

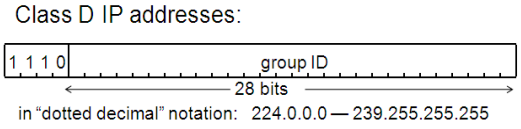

Figure 1.2: Class D IPAddress

The address block 224.0.0.0/24 (224.0.0.0 to 224.0.0.255) is designated for multicasting on the local local area network only. For example, the Routing Information Protocol (RIPv2) uses 224.0.0.9, Open Shortest Path First (OSPF) uses 224.0.0.5, and Zeroconf m DNS uses 224.0.0.251..

The notion of group is essential to the concept of multicasting.. In IP multicasting, multicast groups have an ID called multicast group ID. The format of class D IP addresses is shown in Figure 1.2.

2. ISSUES ON SECURE MULTICAST

The special Characteristics of a secure system includes: Confidentiality, Integrity, Authentication, Access control , Non-repudiation

2.1 Key Management

The key management for multicast requires quite a lot more traffic compared to the key management for unicast. First, the common group key should be distributed to each group member and all the senders. If the traffic should also be authenticated, each sender has to distribute their authentication key to all of the group members.

Some multicast routing systems don't require that there is a group owner or a group originator (core router), so the key management scheme presented above won't work. A simple solution is to use a semi-permanent group key, which is used to generate temporary group keys used to encrypt traffic or authenticate messages.

2.2 N-Way Cryptosystems

Symmetric cryptosystems use the same key for both encryption and decryption. Asymmetric cryptosystems use two separate keys; a message encrypted with one key can only be decrypted with another. Usually one of these keys is called public, another private, meaning that anyone can encrypt a message with the public key but only the party knowing the private key can find out the plaintext.

Some asymmetric cryptosystems, e.g., RSA, work also in another way. A message encrypted with the private key can be decrypted only with the public key. In essence, the RSA is a 2-way cryptosystem. An ideal encryption system for multicast or for any multi-party communications would have n keys, one for each participant. Such a system could be called an n-way cryptosystem.

3. GROUP KEY MANAGEMENT PROTOCOL

This document describes an architecture for the management of cryptographic keys for multicast communications. We identify theroles and

responsibilities of communications system elements inaccomplishing multicast key management, define security andfunctional requirements of each, and provide a detailed introduction to the Group Key Management Protocol (GKMP) [1][2] which provides theability to create and distribute keys within arbitrary-sized groups without the intervention of a global/centralized key manager. The GKMP combines techniques developed for creation of pairwise keys with techniques used to distribute keys from a KDC (i.e., symmetric encryption of keys) to distribute symmetric key to a group of hosts.

A multicast encryption scheme $M_E = (K_{gen}, \Gamma, E, D)$ consists of the following set of algorithms[4]:

1. K_{gen}: a probabilistic polynomial-time (in k) Key Generation algorithm which takes as inputs a security parameter 1^{α}, a threshold τ, the number of (initial) group members n, and generates global information , the encryption key π and the master secret key η.

2. Γ: a probabilistic Registration algorithm to compute the secret initialization data for a new user subscribing to the system. Γ receives as input the master key η and a new index i associated with the user; it returns the user's secret key η_i.

3. Encryption E: a probabilistic polynomial-time algorithm that, on inputs π, the encryption key, and a string $s \in \{0, 1\}^{\alpha}$, and a set $\acute{\Gamma}$ of revoked users (with $|\Gamma| \leq \alpha$) and their keys, produces as output $\psi \in \{0, 1\}^{*}$ called the ciphertext1.

4. Decryption D: a deterministic polynomial-time algorithm can be described such that $\forall m \in \{0, 1\}^{\alpha}, \forall i \in U \setminus \Gamma, D(\eta i, E(\pi, \{(j, \eta^{i}) | j \in \acute{\Gamma}, s)) = s$ (1).

3.1 Multicast Routing Protocols

In the previous section, we reviewed some algorithms that can potentially be used in multicast routing protocols. Similar to unicast routing protocols (such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) protocol), there should be multicast routing protocols such that multicast routers can determine where to forward multicast messages. In this section, we discuss existing multicast protocols and see how these protocols use some of the algorithms discussed in the previous section for exchanging the multicast routing information. We first review three routing protocols (Distance Vector Multicast Routing Protocol (DVMRP), Multicast Extensions to OSPF (MOSPF) protocol, and Protocol Independent Multicast – Dense Mode (PIM-DM) protocol) which are more efficient in situations where multicast group members are densely distributed over the network. Then, we discuss the Protocol Independent Multicast – Sparse Mode (PIM-SM) protocol which performs better when group members are sparsely distributed.

3.2 The Internet Group Management Protocol (IGMP)

The IGMP [7] is used by IP hosts to report their multicast group memberships to any immediately-neighboring multicast routers. This memo describes only the use of IGMP between hosts and routers to determine group membership. All IGMP messages of concern to hosts have the following format:

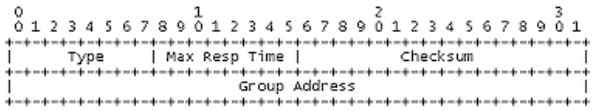

Figure 3.1 IGMP – IP Address

Routers that are members of multicast groups are expected to behave as hosts as well as routers, and may even respond to their own queries. IGMP may also be used between routers, but such use is not specified here. Like GMP is a integral part of IP. It is required to be implemented by all hosts wishing to receive IP multicasts.

3.3 Multicast Key Management Architectures

It includes: Group Key Creation,Group Key Distribution, Group Rekey, Group controller, Group receiver, Group Key Deletion.

It is desirable to be able to delete group members for either administrative purposes or security reasons. Administrative deletion is the deletion of a trusted group member. It is possible to confirm the deletion of trusted group members. Security relevant deletion is the deletion of an untrusted member [12]. It assumes that the member is ignore all deletion commands.

Administrative delete Administrative deletion removes the group keys from trusted group members. This deletion consists of two messages the first sends a command to the group encrypted in the groups TEK. The command essentially says: acknowledge receipt and then delete group keys. This command is signed by the group controller to prevent unauthorized deletions. The acknowledgment message is also encrypted under the group TEK and is sent to acknowledge receipt of the command. We could acknowledge accomplishment of the command if the net is willing to accept the burden of creating pairwise keys between the exiting group members and the group controller.

3.5 The Progressive Group Key Management Protocol

The Local Key Hierarchy (LKH) protocols, They reduces the re-key messages and encryption operations from $O(n)$ to $O(\log n)$ when compared to the Group Key Management Protocol (GKMP) and Secure Lock, where n is the number of group members.In our proposal, The Proposed the progressive group key management protocol (PGKMP) is based on The Chinese Remainder Theorem and a hierarchical graph in which each node contains a key and a modulus.

3.5.1 The Hierarchical Graph:

In the new protocol, the keys and moduli are constructed as a tree and maintained by the key node [5]. The tree graph is similar to the tree graph in the LKH protocol but each node of the tree in the new protocol is assigned two values: a key and a modulus. Figure 3.2 depicts the key and modulus graph, where *TEK* is a traffic encryption key, *kij* is a key encryption key, and *mij* is a modulus.

3.5.2 Moduli Maintenance:

The key server needs to store $2\log 2n$ moduli and each member needs to store $\log 2n$ moduli but they do not need to keep the moduli secret. The sibling nodes in the tree graph are assigned with two different moduli (i.e., $mi1$ and $mi2$ where i is the depth of the tree) and the nodes in the different level of the tree are assigned with the different moduli but each a pair of siblings at the same tree depth are assigned with the same two moduli under the different parents.

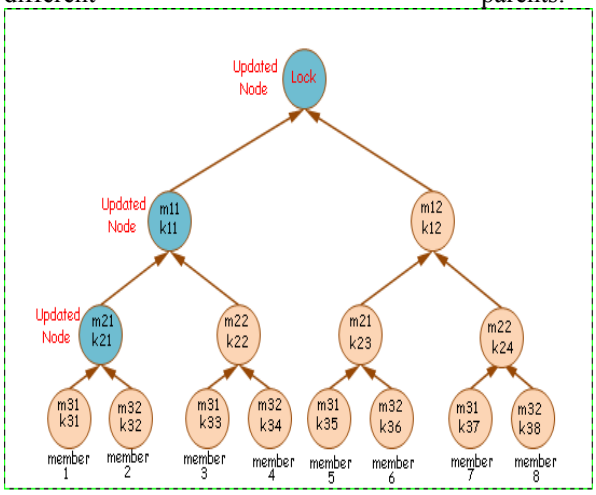

Figure3.2: A Tree Graph containing Key and Modulus

For instance, in Figure 3.2, for a path from $u1$ to the root, the moduli on the path include $m11$, $m21$, and $m31$, and the moduli on its direct children include $m12$, $m22$, and $m32$.

3.5.3 Key Maintenance:

The key server needs to store $2n$-1 keys, i.e., *TEK* and $kij(1 \le i \le \log 2n,\ 1 \le j \le 2i)$ where i is the depth of the node in the tree and j is the ordinal number of the node in the ith depth of the tree, and each member needs to store $\log 2n+1$ keys. The key server shares the keys with each member on the path from its leaf to the root.

4. SECURITY

When routing is to be done in a Multicast, there isn't just the problem with the routing itself. A message doesn't just have to get to the recipient in a fast and accurate way, a recipient as well as the sender has to know that the message isn't tampered with, altered or read by unauthorized persons. There are numerous threats to a Multicast network and they all apply for a Multicast. Actually, they are even harder to solve and control.

In multicast network basic functions like packet forwarding, routing and network management are done by all nodes instead of dedicated ones. Instead of using dedicated nodes for the execution of critical network functions you have to find other ways to solve this, because the nodes of a mobile multicast network can't be

trusted in this way.The requirements are: confidentiality, integrity, authentication and non-repudiation.

4.1 Solutions on security issues:

All the above security mechanisms must be implemented in any multicast networks so as to ensure the security of the transmissions along that network. Thus whenever considering any security issues with respect to a network, we always need to ensure that the above mentioned for security goals have been put into effect and none (most) of them are flawed.

Using authentication techniques during all routing phases exclude attackers and unauthorized nodes from participating in the routing by using digital signatures or some public key infrastructure (PKI). This can be done by cryptography techniques such as key system.

5. CONCLUSIONS & FUTURE SCOPE

Multicast routing protocols provide resilience against collaborating malicious nodes. PGKMP is a complete multipath protocol, in the sense that it provides the maximum security in the network when compared to the existing protocols like LKH etc. The security of PGKMP [11] is mainly based on neighborhood authentication of the nodes, as well as on security associations, while the use of public key cryptography is minimized. The PGKMP protocol can be integrated on top of existing on-demand routing protocols such as LKH. A key reason for this good performance is the fact that PGKMP operates entirely on-demand with no periodic activity of any kind required within the network. PGKMP finds disjoint paths only, so the route discovery cost will be less as compared to LKH where all possible paths exist and a key server has to be maintained. Also due to the double encryption scheme provided to the protocol, the network is more secured.

There is a scope to further decrease the overheads and increase more security with this Protocol (PGKMP) and a positive hope for the enhancement of this protocol.

REFERENCES:

[1]. Fenner, W.: Internet group management protocol, version 2. RFC-2236 (1997).

[2]. Harney, H., Muckenhirn, C.: Group key management protocol (gkmp) architecture. IETFRequest for Comments, RFC 2094 (1997).

[3]. Wallner, D., Harder, E., Agee, R.: Key management for multicast: Issues and architectures. IETF Request For Comments, RFC 2627 (1999)

[4]. Yitao Duan and John Canny: How to Construct Multicast Cryptosystems Provably Secure Against Adaptive Chosen Cipher text Attack, Computer Science Division, University of California, Berkeley, Berkeley, CA 94720, USA

[5]. Wong, C.K., Gouda, M., Lam, S.S.: Secure group communications using key graphs. IEEE/ACM Trans. Netw. **8** (2000) 16–30

[6]. Canetti, R., Garay, J., Itkis, G., Micciancio, D., Naor, M., Pinkas, B.: Multicast security: A taxonomy and some efficient constructions. In: INFOCOMM'99. (1999).

[7]. Chang, I., Engel, R., Kandlur, D., Pendarakis, D., Saha, D.: Key managementfor secure internet multicast using boolean function minimization
techniques. In: Proceedings IEEE Infocomm'99. Volume 2. (1999) 689–698.

[8]. Wong, C.K., Lam, S.S.: Keystone: A group key management service. In: International Conference on Telecommunications, ICT 2000. (2000).

[9]. Li, X.S., Yang, Y.R., Gouda, M.G., Lam, S.S.: Batch rekeying for secure group communications. In: Proceedings of the tenth international World Wide Web conference on World Wide Web, Orlando, FL USA (2001) 525–534.

[10]. Setia, S., Koussih, S., Jajodia, S., Harder, E.: Kronos: A scalable group re-keying approach for secure multicast. In: IEEE Symposium on Security and Privacy. (2000) 215–228

[11]. Ronggong Song. "A Scalable Group Key Management Protocol", IEEE Communications Letters, 07/2008

[12]. Yang, Y.R., Li, X.S., Zhang, X.B., Lam, S.S.: Reliable group rekeying: a performance

analysis. In: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications, ACM Press (2001) 27–38

[13]. Liu, D., Ning, P., Sun, K.: Efficient self-healing group key distribution with revocation capability. In: Proceedings of the 10th ACM conference on Computer and communication security, ACM Press , (2003) 231–240

[14]. H. Harney and C. Muckenhirn, "Group Key Management Protocol (GKMP) architecture," RFC 2093, July 1997.

AUHOR BIOGRAPHY:

M.V.Vijaya Saradhi

M.Vijaya Saradhi is Currently Associated Professor in the Department of Computer Science and Engineering at Aurora's Scientific,Technological and Research Academy, Hyderabad,India ,where he teaches Several Courses in the area of Computer Science. He is Currently Pursuing the PhD degree in Computer Science at Osmania University,Hyderabad, India.His main research interests are Software Metrics,Distributed Systems, Object-Oriented Modeling, Data Mining,Design Patterns,Object-Oriented Design Measurements and Empirical Software Engineering.He is a life member of various professional bodies like MIETE,MCSI,MIE,MISTE.

Ravi Krishna B

Ravi Krishna B received his Master's Degree in mathematics from Andhra University, presently working as an Asst. Professor in the Department of Basic Sciences & Humanities for Vignan Institute of Technology & Science, Hyderabad, India.His area of interests are Network security, Neural Networks.