Source Specific Centralized Secure Multicast Scheme based on IPSec

Safdar Hussain Shaheen
Riphah International University
Islamabad, Pakistan
safdarhussainshaheen@yahoo.com

Muhammad Yousaf
Riphah International University
Islamabad, Pakistan
muhammad.yousaf@riu.edu.pk

***Abstract*—Group-oriented applications require multicast communication for distributing information among the group members efficiently. The deployment of such kind of applications in strategic and military grade organizations needs the secure group-oriented mechanism. The key concerns involved in secure multicast communication are "forward and backward security", "source/recipient identification and authentication", "key revocation" and "secure rekeying". This paper proposes a source specific centralized secure multicast scheme based on IPSec infrastructure by addressing these security challenges. The key management, in proposed secure multicast scheme, has been carried out using the Group Internet Key Exchange (G-IKE v2) version 2 protocol.**

Keyword—Authentication; Group Key Management; IKEv2; IPSec; Multicast;

I. INTRODUCTION

By default internet (IP network) [1] provides an infrastructure for unicast transmission in which originator sends his data to only one receiver. It is more suitable and the major source of transaction or communication worldwide. However, the cost of this technique is proportional to the number of receivers in case of data transmission to a group of receivers. The environment in which the transmission of information from one sender to multiple receivers is required, multicast communication [2] is the most suitable option. It allows the transmission of information from one sender to a group of recipients in a single send operation. For example: video and audio conferencing; distance learning from the centralized location; multi-media streaming etc. In strategic and military grade organizations, group-oriented services are unavoidable for sending information to all of its centers. Furthermore, the mandatory requirement in such kind of organizations is the security of data traffic. Therefore, the deployment of secure multicasting is indispensable in such kind of organizations. The key security issues which need to be addressed for secure multicast deployment are Confidentiality, Integrity and Authenticity (CIA) of data, "forward and backward security", "source/recipient identification and authentication", "key revocation", "secure rekeying process" and negotiation and establishment of group key securely. The one of the way to achieve security services like CIA is IPSec [3] in encapsulated security payload (ESP) [4] and authentication header (AH) [5] states. By default, the built-in security mechanisms in the IPSec are used to protect unicast communication. Since security requirements for multicast and pairwise communication are disparate. Therefore, use of IPsec in standard form for securing multicast communication is an emerging research paradigm. The group key and other necessary parameters for secure group communication can be accomplished by using Group Internet Key Exchange (G-IKE v2) protocol [9]. Aforementioned challenges are also addressed in the proposed scheme. More concisely, this paper presents an efficient and flexible Source Specific Centralized Secure Multicast (SSCSM) Scheme based on standard IPSec. It assures the forward and backward security for group members who join or leave the multicast group. On key revocation, it facilitates the group members with a fresh group key. Furthermore, our scheme addresses authentication of data, originator, and group members. This scheme is applicable in both transport and tunnel mode for multicast communication.

The rest of the paper is organized as follows: section II gives a brief literature review whereas section III elucidates topology, components of SSCSM scheme together with their functionalities. The framework and operations are described in section IV. The limitations of SSCSM are presented in section V. Finally the concluding remarks and future directions are provided in section VI.

II. LITERATURE REVIEW

Numerous approaches are available in the literature for securing multicast communication. Ali et al. [6] presented a secure multicast scheme by modifying standard version of IPSec. Gross and gnjatic [7] provided an extension of multicast regarding security architecture for the Internet Protocol. Baugher et al. [8] discussed group key management about multicast security. For sharing common security policy and keying material among the group members, a scheme of the Group Domain of Interpretation (GDOI) has been introduced in by Weis et al. [11]. Furthermore, Aurisch and Karg [10] have developed a protocol called MIKE for key management for multicast communication. Aforementioned schemes need some improvements due to the following reasons: the schemes presented in [6,7] are not compatible to the standard IPSec.

978-1-4673-7914-4/15/$31.00 ©2015 IEEE

Some automatic or manual modifications seem to be required to make them compatible with standard IPSec configuration. Also for successful negotiation and common group key establishment, GDOI needs fifteen messages to exchange (nine in the main mode and six in aggressive mode). The scheme presented in this paper is compatible with standard IPSec. Also, it shares a common group key among group members in four messages instead of fifteen. This four rounds exchange enhances the efficiency of our proposed scheme. Furthermore, there is no need to modify IPSec infrastructure to use this scheme. It works well in both the transport as well as tunnel mode.

III. Source Specific Centralized Secure Multicast (SSCSM) Scheme

The proposed SSCSM scheme works in the one-to-many scenario. The key players of this scheme are the sender, receiver and Multicast Group Manager (MGM).

- Sender: It may be a member of a multicast group and liable to send messages to MGM.
- Receiver: This entity listens to a multicast IP address for receiving multicast messages.
- Multicast Group Manager (MGM): It plays a role of both registration authority and group controller. MGM is responsible for verification, authentication and authorization of group members. It also assigns a unique identification (UID) key to each group member during the registration process. The UID is calculated by taking the hash (SHA-256) of IP address of group member and master key (MK) of GM [13]. Furthermore, after registration it establishes a secure channel with group member by invoking G-IKE (v2) and then grants permission to legitimate group member to download keying material and group security policy. Moreover, MGM is liable for advertising multicast address (group), generating, distributing and updating the group key securely to the authentic members of SSCSM Scheme. Fig.1 indicates the players involved in this scheme.

A. Topology

The topology of our proposed secure scheme is illustrated in Fig. 2. Initially, MGM advertises IPv6 as a multicast group address. To receive secure multicast transmission, sender and group members (routers) request to MGM for enrollment. Group members are verified by MGM on the basis of their credentials. Then, G-IKE v2 is invoked between MGM and group members to establish a secure unicast channel. After registration, legitimate group members are allowed to download keying material and group security policy for SSCSM Scheme. For this purpose, the MGM's payload is used to transmit the security policy to authorized group members. Finally, it is configured in IPSec at kernel level for further secure communication. The sender sends multicast traffic to MGM. MGM verifies the identity of the sender and then forward sender's information to multicast group address IPv6 [14]. The members of the group, listening to multicast address (IPv6) may receive such traffic. This scheme can be deployed in to two modes namely; the tunnel mode and transport mode.

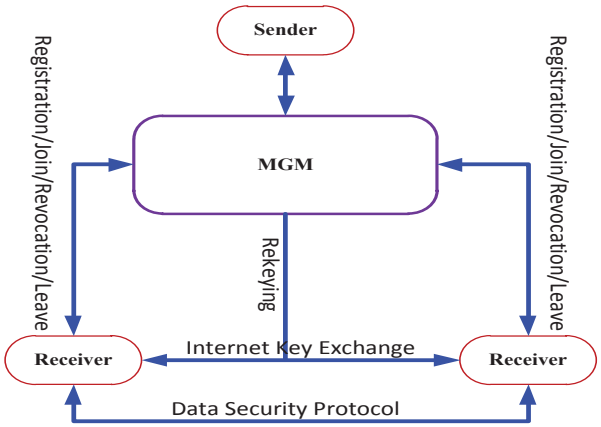

Fig. 1. Structure of the SSCSM Scheme

1) Tunnel Mode: In this mode IPSec is deployed in intermediate networking devices (routers) and MGM. These devices established virtual private network (VPN) [15] by using IPSec. VPN [16,17] provides confidentiality because the tunnels are encrypted. Sender and receivers are not IPSec enabled in this mode, because, only MGM and designated end routers are IPSec enabled. Therefore, the common group key is shared among these group members only. MGM encrypts traffic and forwards to the multicast address (IPv6). Designated routers which are listening multicast traffic decrypt the encrypted traffic on behalf of group members and distribute it to the respective members. The topology of tunnel mode is illustrated in Fig. 2.

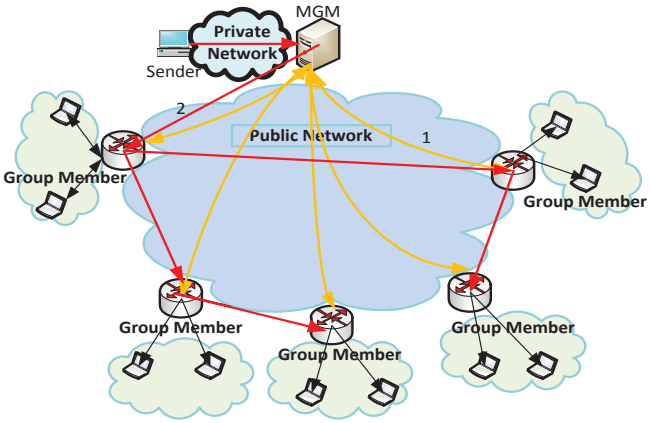

Fig. 2. Topology for proposed scheme in tunnel mode

In Fig. 2 yellow lines indicate unicast secure channel uses for downloading security policy and keying material. Whereas, red lines show the secure multicast traffic being

distributed to designated routers by MGM which have made a VPN tunnels using IPSec. Finally, the designated routers decrypt the confidential traffic and distribute it over to the respective receivers in plain form.

2) Transport Mode: This mode is used to provide end-to-end security. In this scenario, not only the intermediate routers but the sender and receivers are IPSec enabled as well. The sender encrypts the packet with common group key and forwards it to MGM. MGM validates the identity of the sender and then transmits a packet to the multicast address. When a packet enters into VPN tunnel, it is encrypted again and decrypted on reaching on end routers (designated routers). Then, the packet encrypted by source (sender) is distributed to respective group members (receivers). At last, the receiver obtains the normal packet after decryption. This process is depicted in Fig. 3(a).

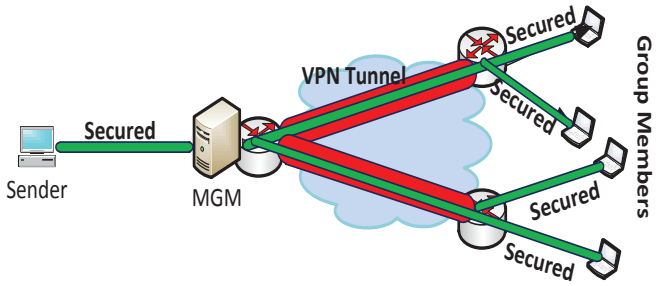

Fig. 3(a). End-to-end multicast security scenario with IPSec enabled routers

The End-to-end multicast security scenario without IPSec enabled routers is shown in Fig. 3(b). The difference between Fig. 3(a) and Fig. 3(b) is that the designated routers are IPSec enabled in the former but not in the later one. However, in both of these scenarios, traffic monitoring tools are not been able to determine what kind of packet is being transmitted.

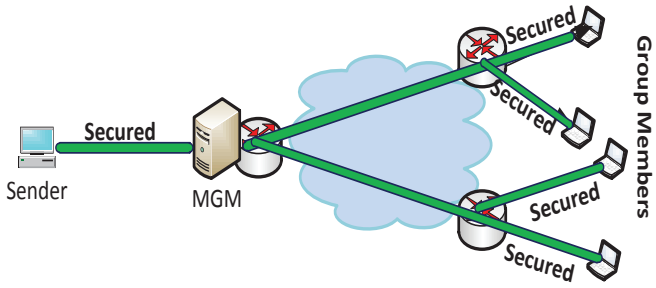

Fig. 3(b). End-to-end multicast security scenario without IPSec enabled routers

B. *Components and Functionality*

With respect to Fig. 4, the components of SSCSM Scheme and their functionalities are listed below.

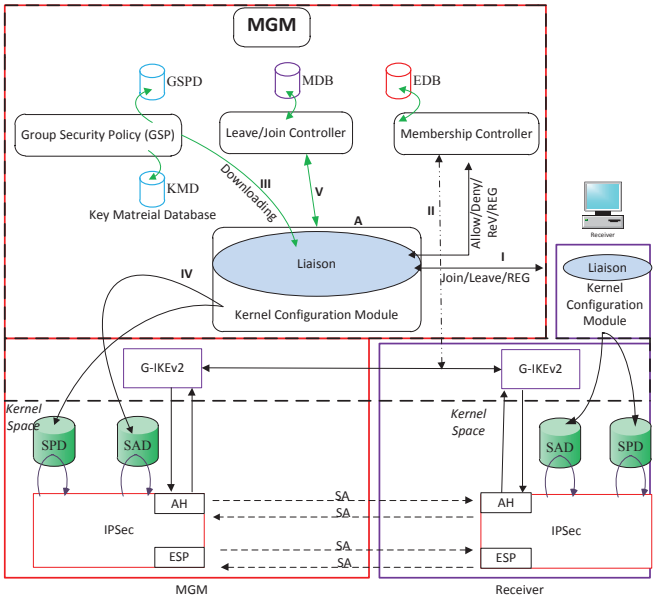

Fig. 4. Components of secure multicast scheme

The primary components of SSCSM Scheme are:

- Multicast Group Manager (MGM)
- Liaison
- Kernel Configuration Module (KCM)
- Membership Controller (MC)
- Leave/Join Controller (LC/JC)
- Group Security Policy (GSP)
- Group Internet Key Exchange (G-IKE)
- The Internet Protocol Security (IPSec)

Whereas the databases needed for storing records of SSCSM Scheme are

- EDB: Enrollment Database
- MDB: Member Database
- GSPD: Group Security Policy Database
- KMD: Keying material Database
- SPD: Security Policy Database
- SAD: Security Association Database

Above mentioned components are shown in Fig. 4. For simplicity, we have divided these components into two categories namely; MGM's components and Receiver's components. In Fig. 4 components enclosed in red boxes belong to MGM whereas purple boxes indicate receiver's components. It is notable that sender (originator) has components similar to the receiver. The functionalities of listed components are now illustrated in detail.

1) Components of Multicast Group Manager (MGM)

It is responsible for handling almost all kinds of queries regarding secure multicast communication. It is liable for maintaining the group security policy and keying material for the group. When a group member gets enrolled, it is

endorsed to download security policy and keying material. MGM also executes rekeying process whenever any group member leaves or joins the group. Anyone can enroll at any time and download group security policy and keying material. During joining process, the identity of the group member is verified. If it is valid group identity then MGM authorizes him to download new keying material. Using this keying material, group members calculate the group key and the authentication key for further secure group communication. The essential components of MGM are given below;

a) Liaison

It is a major component of MGM. It receives requests/queries from the receiver and replies it accordingly. It is deployed on MGM as well as on receiver systems. Liaisons on both ends communicate to send and receive multicast queries.

b) Kernel Configuration Module (KCM)

The main functionality of this module is to configure/reconfigure the Security Policy Database (SPD) and Security Association Database (SAD) of IPSec deployed on systems or devices after obtaining relevant information from Liaison module.

c) Membership Controller (MC)

This component is responsible for enrollment of members interested in receiving secure multicast traffic. At first step, it verifies client's credentials and assigns a unique identity based on its IP and MGM master key (MK). It is being illustrated in [13]. MC also performs the task of verification, authentication and authorization when any member joins the multicast group. The record of enrolled entities is stored in Enrollment Database (EDB).

d) Leave/Join Controller (L/JC)

When members join or leave the secure multicast group, L/JC save/delete its entry from Member Database (MDB). MGM send secure multicast traffic to the members only which exist in MDB.

e) Group Security Policy (GSP)

At start, MGM chooses a security policy for group members. This security policy is saved in SPDB. In SSCSM Scheme IPSec keeps same security policy for inbound and outbound states.

f) Group Internet Key Exchange (G-IKEv2)

This protocol is used to establish a secure channel between MGM and other IPSec enabled hosts. Basically, it employs the security features of IKEv2 for handling key management issues in SSCSM Scheme. In addition, it protects the negotiation process among the group. The two exchanges in G-IKEv2 that are essential for establishing a secure channel are IKE_SA_INIT and GSA_AUTH. Each exchange consists of request/response pairs. The first exchange negotiates cryptographic algorithms and nonces according to group policy and then applies a Diffie-Hellman key exchange protocol [12] between the member and MGM to establish a secure channel. The second exchange authenticates the previous messages, sends the identities, keying material and group security policy for further secure multicast communication. From these keying material group members devices the authentication key and the group key for further secure communication.

g) The Internet Protocol Security (IPSec)

IPSec is standardized by IETF (Internet Engineering Task Force) and provides Confidentiality and Authentication to the traffic regarding IPv4 as well as IPv6 [14]. It offers two protocols for authentication and confidentiality namely; AH and ESP. Authentication is obtained by using AH protocol whereas confidentiality is achieved through ESP. It supports two different modes of operations, the tunnel mode, and the transport mode. Transport mode offers end–to-end security whereas tunnel mode is used to build a virtual private network (VPN).

h) Databases in MGM

EDB: It is used to store the credentials of registered members.
MDB: This database is used to store the members who joined the multicast group.
GSPD: The group security policy is saved in this database.
KMD: Keying material is recorded in this database.
SPD: This is security policy database of IPSec and resided in kernel space. KCM updates this database for IPSec use in proposed secure scheme.
SAD: Group security parameters are saved in this database. It contains "source and destination address (multicast address of group)", " source and destination port", "security parameter index (SPI)", "security protocols (AH or ESP)", " cryptographic algorithms such as AES256, SHA256, ECC etc", "sequence number for avoiding replay attack" and "expiry period if required". SPI indicates Group security association (SA) having common group key and authentication key. The aforesaid components are demonstrated in Fig. 4.

2) Components of receiver

Receiver components include Liaison, KCM, and IPSEC. The functionality of these components is same as in the case of MGM. These components are also shown in Fig. 4.

IV. FRAMEWORK AND OPERATIONS

The framework and operations of SSCSM Scheme are divided into the following five phases. These phases are demonstrated in Fig. 5.

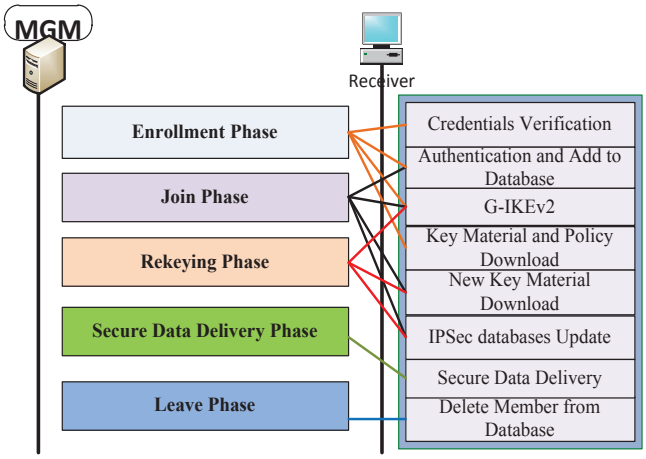

Fig. 5. Phases of proposed scheme and their operations

A. *Enrollment Phase*

In this phase, liaison module of receiver communicates to the liaison module of MGM and request for registration. Liaison module of MGM forwards his request to MC along with receiver's credentials. MC verifies receiver's credentials and grants permission, after checking the validity, to download keying material and group security policy. Then G-IKE v2 is invoked at both ends for negotiation and secure session establishment. Afterward, UID, Group address in the form of IPv6, group security policy, and key material are securely transmitted to client end through securely established channel. Finally, KCM configures the IPsec's policy database (PDB) and security association database (SAD) for confidentiality and integrity of multicast data.

B. *Join Phase*

In this phase hosts (receivers) who are interested in receiving multicast traffic sends a request to MGM to join the specified group. Liaison module of MGM forwards its request to MC. MC verifies the host against registered database. In the case of failure, liaison sends the pre-registration request message to host otherwise liaison save the client record in MDB. Then G-IKEv2 is invoked between host and MGM to establish a secure session. Finally, host downloads the new key material, deduces keys from this material and updates the IPSec configuration.

C. *Rekeying Phase*

Whenever any host (receiver) joins or leaves the secure multicast group. The new key material is generated by MGM and downloaded by every group members using the G-IKEv2 secure channel and then session key and a secret shared key for group communication are constructed. In this way forward and backward secrecy is maintained through the rekeying process.

D. *Secure Data Delivery Phase*

In this phase, secure data delivery is made by using IPSec. IPSec can be configured through KCM on all members and MGM. They have same security policy along with same the group and authentication keys, deduced from a common key material.

E. *Leave Phase*

Upon group leaving request from any member, Liaison module deletes its entry from MDB and then rekeying process is initiated for forward and backward security.

V. LIMITATIONS OF THE PROPOSED SCHEME

The present scheme has been proposed for a closed environment in which security is on top priority such as Command and Control (C&C) system of military grade organizations. It works efficiently for a small group having fewer numbers of participants. Since the group size is directly proportional to the computational complexity in this scheme. Therefore, the computational overhead is a bottleneck for a large group of participants. Furthermore, the centrally control characteristic of this scheme makes it vulnerable against a Single Point Failure (SPF). Since, SPF is an ultimate deficiency in centralized management schemes. Therefore, for simplicity we assume that backup server, disaster management, and recovery mechanisms are available in case of SPF in targeted closed environment.

VI. CONCLUSION AND FUTURE WORK

In this paper, a Source Specific Centralized Secure Multicast Scheme has been proposed using standard IPSec infrastructure. The establishment of a secure channel between MGM and group member has been made by using G-IKE v2. Then, a secure channel is used to transfer keying material and group security policy to group members. Group and authentication keys are deduced from keying material in this scheme. The verification of each group member (sender or receivers) may be accomplished any time by MGM using its master key (MK). Forward and backward security has been obtained by introducing secure rekeying process in this scheme. It works well in transport as well as tunnel modes. Kernel configuration module is liable to update IPSec databases such as SAD and SPD in this scheme. Records of member's registration and joining/leaving are maintained by Membership Controller and Join/Leave Controller in user space. The functionality of revocation has also been added in this scheme. This scheme can be implemented in the real time multicast environment for secure communication. It is efficient and scalable for small group working in the centralized environment. Despite all, it also provides message authentication due to its source specific and centralized control nature. This work can be extended to attain the scalability and efficiency for larger groups. The implementation, test bed results, and comparative analysis will be address in next studies.

ACKNOWLEDGMENT

I am privileged to thank Dr. Mobeen Akhtar Mir for her nice co-operation and effective guidance during the

accomplishment of this task. Special thanks to Dr. Muhammad Younas Majeed and Dr. Muddasar Jalil for their scholarly guidance and kind support during write up.

REFERENCES

[1] J. Postel, “Internet Protocol Handbook Table of Contents,” IETF RFC 774, October 1980.

[2] B. Quinn and K. Almeroth,"IP Multicast Applications: Challenges and Solutions," IETF RFC 3170, September 2001

[3] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," IETF RFC 4301, December 2005.

[4] Stephen Kent and Randall Atkinson,"IP Encapsulation Security Payload ESP," IETF RFC 2406, November1998.

[5] Stephen Kent and Randall Atkinson, "IP Authentication Header”, IETF RFC 2402,November 1998.

[6] Eman Ali, Tarek El-fouly and Ahmed Badr,"MESP: A Modified IPSec for secure multicast communication," 6th International Coference on ITS Teleconuiiic&ations Proceedings, 2006.

[7] G. Gross and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol," IETF RFC 5374, November 2008.

[8] M. Baugher, R. Canetti, L. Dondeti, F. Lindholm ,"Multicast Security (MSEC) Group Key Management Architecture ," RFC 4046, April 2005.

[9] S. Rowles,A. Yeung, Ed.P. Tran and Y. NirAl, "Group Key Management using IKEv2," MSEC Working Group draft-yeung-g-ikev2-04, March 11, 2012.

[10] T. Aurisch and C. Karg,"A daemon for multicast internet key exchange," In 28th Annual IEEE Conference on Local ComputerNetworks, 2003.

[11] B. Weis, B. Weis and T. Hardjono, "The Group Domain of Interpretation," IETF RFC 6407, 2011.

[12] Whitfield Diffie and Martin E. Hellman, "New directions in cryptography," IEEE Transactionson Information Theory, (22):644.654, 1976.

[13] S.H.shaheen, M.Yousaf, "Security Analysis of DTLS Structure and Its Application to Secure Multicast Communication," Frontiers of Information Technology (FIT), vol. 8(1), pp.165,169, 17-19, Dec. 2014.

[14] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," I*ETF RFC 2460*, Dec 1998.

[15] E. Rosen and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)," IETF RFC 4364, February 2006.

[16] Rekhter, Y., and E. Rosen."Extranet Multicast in BGP/IP MPLS VPNs." IETF Draft, 2014.

[17] Li, Zhenbin, and Hui Ni."Role-Based State Advertisement for Multicast in MPLS/BGP IP VPNs.," IETF Draft , October 18,2015.