ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

Validate Group Keys for SRTP: Combining Kerberos and Multimedia Internet Keying (MIKEY)

A.Kandapriya[1], S.Subash Prabhu[2]

PG Scholar, Department of CSE, P.S.R Rengasamy College of Engineering for Women, Tamilnadu, India[1]

Assistant Professor, Department of CSE, P.S.R Rengasamy College of Engineering for Women, Tamilnadu, India[2]

ABSTRACT: Authenticated transport of cryptographic keys for secure group-communication between Distributed system to avoid the security vulnerability and to find the authorized user to increase the availability for that implement the design called Multimedia Internet Keying (MIKEY) is a by RFC -3830 standardized key exchange protocol and Kerberos for authentication. They have multiple options for key exchange and low latency from MIKEY is mainly used for real-time multimedia application in conjunction with SRTP used and typically uses the three key exchange methods. Then employ protocol composition logic (PCL), a state-of-the-art approach for analyzing our design. The Group Key will be generated for a certain type of the group people and using that key that person can access that group information. The group key is used to add the person in the group to do transaction by using Public/Private key options for providing access to each message and it also avoids the unauthorized person to interrupt. We have implemented both designs starting with the publicly available reference achievement of Kerberos, and an open-source completion of MIKEY.

KEYWORDS: Cryptographic algorithm, Computer security, Authentication, SRTP

I. INTRODUCTION

Computer networking is the engineering discipline concerned with the communication between computer systems or devices. Computer network is any set of computer devices connected to each other with the ability to exchange data. Network Security involves the authorization of access to data in a network, which is controlled by the network administrator. Network Security protocols usually use encryption and decryption technology. Encryption and Decryption scrambles data sent and receive over network connections to hide information. The simple way of protecting a network resource is by assigning a unique name and a corresponding password. Enterprise and organization have computer files which are vital to their work. Like hood military and industries will have files is more important to the defense of the country. This makes sure that files are securely stored on a file server. Several threats and attacks are possible through network administrators, ip spoofing, Denial of service, so on. Eliminating all risk is not possible, but avoiding has chance through Kerberos and Multimedia Internet Keying.

Authentication is needed for communication so proving identity to someone is ought. Kerberos provides authentication in an enterprise and public safety setting through symmetric key encryption, key management, key transport protocol and key distribution center. Kerberos provide authentication under the condition of cryptographic which also provide the following requirement like secure, reliable, transparent, scalability. Kerberos has three main Characteristics such as Authentication, authorization, and accounting (AAA). These collective processes are considered important for effective network management and security. Mutual authentication is performed where the client and server proves their identity to each other. More difficult for guessing passwords and also hard to reuse the stolen authentication tickets.
Multimedia Internet Keying describes key management, which can be used for secure real time application (for peer to peer and group communication). Key management addresses the multimedia scenario, where SRTP defines RTP to provide encryption, integrity, replay protection and message authentication. The MIKEY protocol is planned to provide end-to-end security among users to support a communication. For this, it shares a session key, which is known as

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

Traffic Encryption Key (TEK), among the participants of a communication session. The MIKEY protocol might also authenticate the participants of the communication. MIKEY provides a lot of methods to share the session key and authenticate participant. The combination of these two protocols will give a more secure authentication system.
The rest of the paper is organized as follows: In Section II present the related work based on review of previous work. Section III discusses the proposed work which contents Kerberos and Multimedia Internet Keying Conclusion and Future Work is presented in section IV.

II. BACKGROUND AND REALTED WORK

In the networking literature, there are distinct works that propose Authentication Protocol .The following section deals with most representative work that is related to the proposed work.

Authentication Protocol
There are various techniques by which a message could be disseminated over the network. In the networking literature, there are several works that proposed to reduce the security problem at the registration level to provide more security and to increase the availability of key. The following literature review deals with the literature works related to this project
Using Encryption for Authentication in Large Networks of Computers [1].Use of Conventional encryption and public-key encryption to achieve authenticated communication in computer networks. Example protocol are management of authenticated mail, document integrity and signature verification, but it Does not focus on other security, such as traffic analysis, detecting of tampering and also minimize throughput . *A Survey of Key Management for Secure Group Communication [2]*. A Survey for secure group communication applications can use IP multicast to transmit data to all n group members where researchers have followed three main classes: Group Key Management Protocol, which try to minimize the necessity of KDC, group member and computational power between client and server. Decentralized architecture: The executive of large group by dividing into small group which is reducing the problem of controlling the work in a single place and provide more scalable. Distributed Key Management protocols provide same responsibility to all members. An analysis prepared it clear there is no unique solution. Centralized key management schemes are simple to implement, they are likely to require an overhead on a single entity. Distributed Key management not for scalable Where the greatest solution for a particular application may not be most excellent for another, so it is vital to understand other requirement of application before selecting a security solution. *Protocol Composition Logic [4]*.Proving security properties of network protocol are inflexible problem which are executed multiple protocols simultaneously and attack can access information from one session to defects the security of another. Symmetric key and public key cryptography are used. A secrecy property asserts some data that is used in the protocol is not exposed to others. If protocol generates a fresh value, called a nonce, and sends it in an encrypted message under normal status .The nonce remains secret with that only agents have the decryption key can acquire the nonce we also developed PCL, which is a high level logic standard for security protocol which also support compositional analysis about security protocols. The public-key infrastructures are used instead of the shared secret key. So the modular nature of the secrecy and authentication proofs is hard to prove. *A Composition Logic for Proving Security Properties of the Protocol [5]*. Proving security properties of the protocol by composition of logic which contains axioms and inference rules for proof of correctness which follows the sequence of action in the protocol. We present logic for proving security properties of protocols that logic uses five predicates: Sent Decrypts, Honest, Source, and Knows. The logic presented in this work includes modal operators naming sequences of actions from a procedure calculus. This logic provides a technique for attaching assertions to protocol actions, in a way of resembling dynamic logic for sequential imperative programs applying Floyd–Hoare style annotations Assertions are associated with an action which grip in any protocol executions. The semantic of our logic is based on the set of traces of the protocol execution. This approach lets as proven properties of protocol that hold in all runs without any explicit reasoning about the possible action of an intruder. Where authentication property fails and the identity of the responder cannot correct. *Internet Key Exchange [9]*. The IPSec goals to provide application apparent end to end security of the internet protocol for security a property which depends on the key exchange protocol known as Internet Key Exchange (IKE). Formal analysis of IKE version is IKEV1 and IKEV2 where IPSec implement by setting up for each communication so called as security association which provide three main security properties for consequently transmitted messages. Establishing a session key in

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

IPSec is an involved process with a large amount of options to choose such as sub-protocols, cryptographic methods and option field. According to IKE, it provides "Mutual authentication between two parties and also provide IKE security organization". Where IKEV2 show less limitation than IKEV1. In phase1 only weak authentication is achieved, phase2 not assured for reflecting attacks. Future works are identity protection and toughness against denial-of-service attack. Which also has no identity protection and may exchange some security parameters with peers they are authenticated. *Group Key Management in Multicast Security [3]*. In multicast security, key management for securing group communication is an important area that needs to be addressed which requires multiple security association (SA) such as GCKS, GSA. Multiple SA that is not only used for protecting data traffic also for registration and rekeying. *Multicast Security (MSEC) [6]*. The use of multicast has the lack of security. The indication of group management is proposing in internet engineering task force and multicast security workgroup. Group key management is assembling upon group key management protocol (GKMP). This is also protecting group secrecy known as rekeying. When the group being compromised due to leaving a member of a group and joining the group or access the key by an unauthorized member. Group key management element is responsible for decision making roles which are essential for the operation of the secure multicasts system also rekeying algorithm properties are grouped secrecy but in a dynamic multicasts surroundings. Group members can't be optionally denied access to previous group session keys and function block that can't be unusual. *Security of Encrypted Rlogin Connections Created with Kerberos IV [7]*. Propagating Cipher Block Chaining: Kerberos authentication is used, client and server identity to each other as a side effect, share a key between client and server once the connection created which allows successive message to be encrypted. Common application is rlogin in Kerberos which uses DES (Data encryption Standard) algorithm.DES is a symmetric key block cipher which is encrypted with a block of eight bytes. Propagation cipher block chaining modes are used in Kerberos. PCBC mode, before encryption the plaintext is order exclusive with cipher text and the plaintext of the previous block. Using constant initial vector, defects the purpose of using a chaining mode if data length is not as much of as block size. *Efficient Kerberized Multicast in a Practical Distributed Setting [8]*. The purpose of a capable protocol for secure group communication through multicast, using Kerberos. They regard as a practical distributed setting where users exist in different intranets (realms) linked through the internet. This setting is adequately general as almost any type of network can be characterized and present useful structure, especially the presence of a trusted server surrounded by each intranet. They reflect on an extension to the creative Kerberos protocol that enables crossrelam procedure and proposed a new standard for cross realm Kerberos authentication that notably decreases slow communication over the internet, makes most procedure local, and the workload of the implicated components. Furthermore they describe the new addition of multicast encryption schemes to the case of multiple centers. Finally, they come together the new crossrelam protocol with those for the multi-server multicast encryption.

Kerberized Multimedia Internet Keying [10]. Multimedia group communication is attractive a common channel for everyday work within Enterprises. Protecting the confidentiality and privacy of its content is paramount in network security. In group communication, two or more principals form an entity called a group. Group communication, and its fundamental technology, multicast, has important applications in both Internet-scale, and enterprise. Bootstrapping is the transport of an initial cryptographic key which can be used to secure future communications, including the transport of other keys. Group key management protocols are examples of security protocols that allow the association of keying materials that can be used by its fundamental transport layer's encryption mechanism. This basically is what the Internet Engineering Task Force (IETF)'s multicast security working group (MSec) calls a registration protocol. Its intention is to transport an initial cryptographic key to authorized members of a group so they are able to then communicate securely with extra members of the group. All members of the group hold this key. However, the process of bootstrapping for such a protocol or system is not always trivial. *Authenticate Group Key Transfer Protocol Based On Secret Sharing [11]*. In establishing group key transfer protocol the key generation center accidentally selects a session key and then transports it that has been encrypted by a different secret key. After that assemble authentication key transfer protocol based on secret sharing as a substitute of encryption algorithm. Protocol based on a secret sharing scheme based on language interpolation polynomial which provide mutual authentication to ensure that only the authorized group members can recover the right session key "One time assign, many times apply". The reconstruction of the group key can be completed by the user-self which reducing storage cost, civilizing computation efficiency and providing mutual authentication. The group key more convenience and does not secure where the time cost is unavoidably too high.

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

III. PROPOSED WORK

Transport of secure group key on the environment should be authenticated, for that deploy Kerberos for authentication and deploy multimedia, internet keying for secure key transport which is IETF standard. MIKEY used in the registration protocol for group keys. Use of registration protocol we can defects the attacker/intruder at the starting point itself.

Multimedia internet keying support different types of modes which use DH-MAC (HMAC Authenticate Diffe-HellMan) and Reverse RSA, which also involves an existing mode but make use of asymmetric key. By using this mode, which avoid unauthorized member to access the server. DH-MAC is light version it uses HMAC to authenticate two parties each other. Reverse RSA is a key exchanged with the help of public key encryption, which sender sends its public key to the receiver, where receiver selecting the common secret and send it back to the sender encrypted with the sender's public RSA key. This also inherent tradeoff between security and performance. So composing these protocols for key transport and authentication of cryptographic keys for group communication in public safety setting.

Group controller and key management (GCKS) also deploy for providing more secure group key management and also for cryptographic key management. It provides authentication when members join the group at any time. All components need integral with group controller and key management. It avoids unauthorized members by considering sender and receiver as an entity for transmitting and receiving files, respectively which may multiple sender or single sender to send data to multiple receivers and via to receiver also. Where it may allow all members of the group to be sender which initiator and responder have need of admission control, authentication and key downloading from the GCKS. For that policy server is managed extend and accessed via GCKS to the group members. Policies are necessary in multicast security group key management, which will pick on how keys are to be managed and cryptographic action to be performed. By this prevent unencrypted passwords from being sent across the network.

A. Kerberos

Kerberos provides authentication in an enterprise and public safety setting through symmetric key encryption, key management, key transport protocol and key distribution center. Kerberos provides authentication under the condition of cryptographic which also provide the following requirement like secure, reliable, transparent, scalability. Fig 3.1 shows the main components of Kerberos and its transaction of messages between the components.

- Authentication Service Exchanged
- Ticket Granting Service Exchanged

B. MIKEY

Multimedia Internet Keying (MIKEY) describes key management, which can be used for secure real time application (for peer to peer and group communication). Group controller and key management (GCKS) also deployed for
Providing more secure group keys management and also for cryptographic key management. It provides authentication when members join the group at any time. MIKEY provides a lot of methods to share the session key and authenticate participant.

- Group Key Confidentiality
- Group Key Acquisition

IV. WORKING MODEL

A. Authentication Service Exchanged

C is a client sends a request to the Authentication Server (AS) for a ticket with a client login name and password. AS issues a TGT is a ticket granting ticket corresponding to the login name & ticket granting server (TGS). The Kerberos authentication Server has a copy stored in its database is encrypted form the user password is used to encrypt the Ticket Granting Ticket to secure from eavesdropping. Kerberos authentication service Registration will get user working time for the security process.

B. Ticket Granting Service Exchanged

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

The client sends a request (REQ) to the TGS with TGT which is issued by AS. Now TGT is decrypted with the session key issued by AS, not by client's password.TGS check to make sure login names; client addresses and TGS server name are all correct and also makes sure the authenticator (AUTH) is recent then TGS authenticates tickets and issues a ticket for the resources as well as the encryption key (K) to client for communication with the service.
Server S relies on the KAS and TGS to have authenticated client.

$$REQ: AUTH_{C,S,}\ \{TKT\}_{K\,(s,\,tgs)} \quad (1)$$

$$AUTH_{C,S} = \{S,C,T\}_{K\,(c\,,\,s)} \quad (2)$$

$$TKT = C, S, LIFETIME, K_{(C,\,S)} \quad (3)$$

Where both modules under Kerberos process for authentication, but it's having some weakness where clients have $K_{C,TGS}$ to protect group keys which client is authorized Security of all group key to which a client is authorized relies on the security key of $K_{C,TGS}$. For that we need partial delegation of group authorized to the TGS by GCKS are specified for each group.

C. Group Key Confidentiality

Group key confidentiality is under MIKEY process. If a user possesses the key, then it is an authorized member of the group and has an average time for a client to complete its request for a group key. The Client has a key that it wants to transport to the responder which initiator communication by sending an I_MESSAGE like,

$$I\_MESSAGE:HDR,T,RAND,[ID_I],[ID_R],\{SP\},KMAC. \quad (4)$$

Where HDR is a MIKEY Header, RAND is a Random seed for key generation, ID_I is an Identity of Initiator, ID_R is an Identity of Responder, SP is a Security policy, KMAC is a Hash Message Authentication Code for the receiver to verify authenticity and integrity.

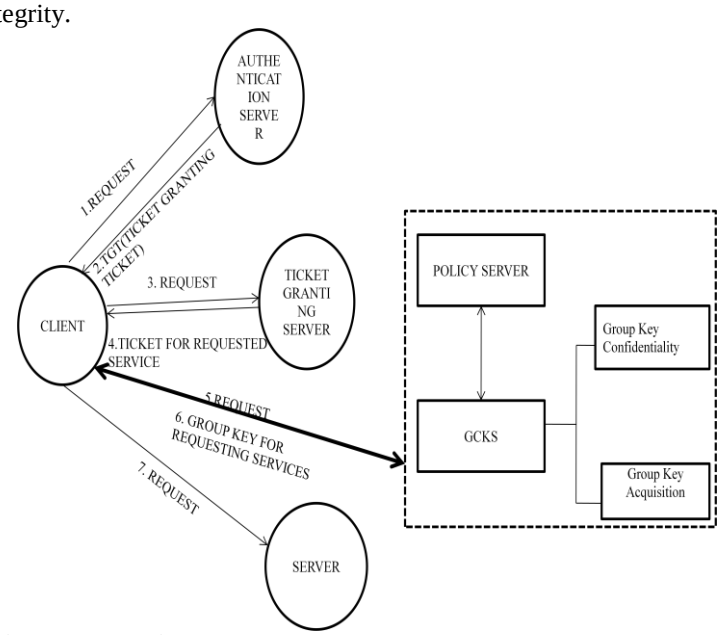

Fig. 1. Overview of System design of Kerberos and MIKEY Transaction to access the server securely at registration level.

D. Group Key Acquisition

Group Key Acquisition is the property that if a user is a member of the group (G), then it is able to acquire the group key (Γ). It ensures the property that only those clients that are authorized by the GCKS to be members of a group can possess the group key for that group. Which is under MIKEY process with group controller key server GCKS which have policy security to manage multiple sender and receiver to acquire the group for access file servers. Policy security from group acquisition of client for transport group keys MIKEY Message is used to transport the group key, from GCKS to the client C.

GCKS handles the following process for the authenticator to access the server, such as

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

GCKS [

Receive tkt .enc $_{c,s}$
Text $_{txt}$: = asymdec tkt , K $_{(GCKS)}$
Match text $_{txt}$ as (c) . (GCKS) . t´ . K $_{(c) ,(GCKS)}$
Text $_{C, S: =}$ asymdec enc $_{C, S,}$ K $_{(C, GCKS)}$
Match text $_{C, S}$ as G.C.t
Enc $_{S, C}$: = asymenc Γ, K $_{(G, GCKS)}$
Send t.enc $_{(s, c)}$] S

Fig.2. GCKS and client group key exchange

Now client access the file server with group key in secure manner at registration itself.

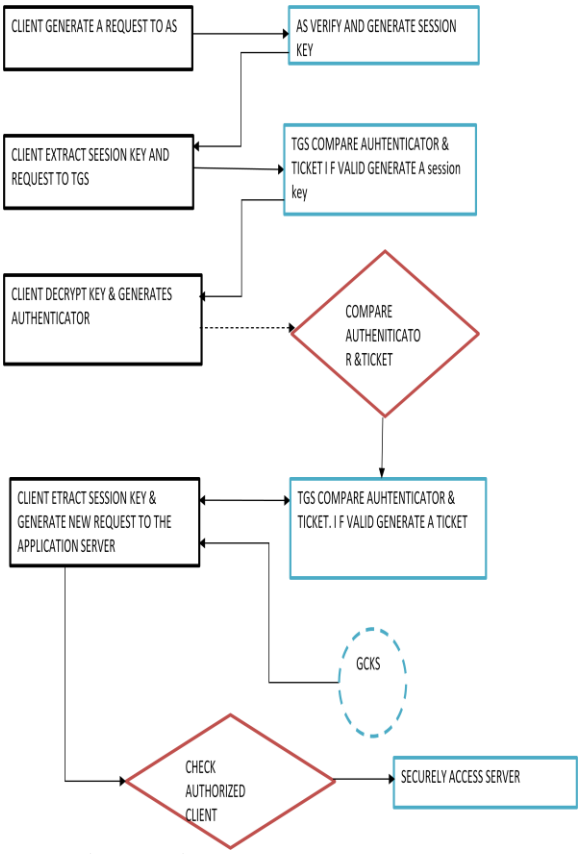

Fig.3. A flow chart for describing the new authentication protocol

V. CONCLUSION

The composing of the Kerberos for authentication protocol and the Multimedia Internet Keying (MIKEY) for secure transport key is a good choice for authentication and key transport. Furthermore, security properties are provided by Reverse RSA, HMAC and AES crypto engine algorithm which is authenticate group members by security polices server as GCKS. Future work regards other designs that may be possible and alternatives to our design, and a study of the properties that these new designs have that may be superior to our designs and also a deeper study on how the

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

GCKS can be realized in a way that it is bound more tightly to the components of Kerberos to make the overall system more efficient.

ACKNOWLEDGEMENT

The authors acknowledge the contributions of the students, faculty of P.S.R Rengasamy College of Engineering for Women for helping in the design of simulation result , and for tool support. The authors also thank the anonymous reviewers for their thoughtful comments that helped to improve this paper**.** The authors would like to thank the anonymous reviewers for their constructive critique from which this paper greatly benefited.

REFERENCES

[1]. R.M. Needham and M.D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Comm. ACM, vol. 21, pp. 993-999, Dec. 1978.
[2]. S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," ACM Computing Surveys, vol. 35, pp. 309-329,http://doi.acm.org/10.1145/937503.937506, Sept.2003.
[3].IETF,"MulticastSecurity(Msec),"http://datatracker.ietf.org/wg/msec/charter/, Sept. 2011.
[4]. A. Datta, A. Derek, J.C. Mitchell, and A. Roy, "Protocol Composition Logic (PCL),"Electronic Notes in Theoretical Computer Science, vol. 172, pp. 311-358, Apr. 2007.
[5]. N. Durgin, J. Mitchell, and D. Pavlovic, "A Compositional Logic for Proving Security Properties of Protocols," J. Computer Security, vol. 11, no. 4, pp. 677-721, http://seclab.stanford.edu/pcl/ papers/dmp-jcs03.pdf, 2003.
[6]. T. Hardjono and B. Weis, "The Multicast Group Security Architecture," RFC 3740, available from http://tools.ietf.org/ html/rfc3740, http://www.rfc-editor.org/rfc/rfc3740.txt, Mar.2004.
[7]. K. Hildrum, "Security of Encrypted Rlogin Connections Created with Kerberos IV," Proc. Network and Distributed System Security Symp. (NDSS), 2000.
[8]. G.D. Crescenzo and O. Kornievskaia, "Efficient Kerberized Multicast in a Practical Distributed Setting," Proc. Fourth Int'l Conf. Information Security (ISC '01), pp. 27-45, http://dl.acm.org/citation.cfm?id=648025.744363, 2001.
[9]. C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)," available from http:// tools.ietf.org/html/rfc5996, Sept. 2010
[10]. J. Woo, "Kerberized Multimedia Internet Keying", https:// github.com/jltwoo/Kerberized-Multimedia-Internet-Keying, Mar. 2012.
[11]. L. Harn and C. Lin, "Authenticated Group Key Transfer Protocol Based on Secret Sharing," IEEE Trans. Computers, vol. 59, no. 6, pp. 842-846, June 2014

BIOGRAPHY

A.Kandapriya has received B.E degree in Computer Science and Engineering from Scad College of Engineering and Technology, Tirunelveli District in 2013. She is currently pursuing Master of Engineering in Computer Science and Engineering in P.S.R Rengasamy College of Engineering for Women under Anna University, Chennai. Her areas of interest in research are Cryptography and Information Security.

S.Subash prabhu has received B.Tech degree in Information Technology from the Kamaraj College of Engineering and Technology, Virudhunagar District in 2009 and M.Tech-Information Technology in SRM University, Chennai in the year 2011. He is working as an Asst.Professor in the department of CSE, P.S.R Rengasamy College of Engineering for Women, Sivakasi. He has published papers in various international and national journals. His areas of interest are Network Security.