ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Modified Kerberos and Multimedia Internet Keying (MIKEY) for Authenticated Transport of Group Keys using Blum Shub algorithm

P. Aditya Pavan Kumar[1], S. Kesava Rao[2], Dr. A. Chandra Sekhar[3]

PG Scholar, Dept of C.S.E., Avanthi Institute of Engineering & Technology, Visakhapatnam, India[1]

Assistant Professor, Dept of C.S.E., Avanthi Institute of Engineering & Technology, Visakhapatnam, India[2]

Professor, Dept of C.S.E., Avanthi Institute of Engineering & Technology, Visakhapatnam, India[3]

Abstract: The introduced simple practical medications to the KDC database to overcome these attacks. In our modified version of Kerberos, the long-term secret key of the network principle will be independent of the principle's password. Instead, the KDC will save a profile for every instance in the realm that it manages. The type of the problem data contents may be audio, video, image, or simply text data. The KDC database may have mixed types of profiles. The network principle may be a client or a server. Every principle in the network is registered in the KDC database by the principle ID. Then the KDC maps this ID to the proper profile where the profile is named with the principle's ID that belongs to that profile. In order to generate the principle's secret key, we apply a hashing algorithm to the principle's profile and then encrypt the output digest. We control the lifetime of the secret key using the current KDC system time that is appended to the principle's profile every predefined period(this period is a design parameter, i.e. a site constant).By this way, we change the input to the hashing function, and consequently, the output of the hashing function and the secret key will change too. In our implementation, we use Triple-DES in CBC mode as an encryption algorithm, SHA-256 as a hashing algorithm, and Blum Shub as a random number algorithm. The introduced medications to the KDC database will enhance the performance of the protocol since the principle's long-term secret-key will be independent of the user password. Thus, our modified Kerberos version is no longer vulnerable to password guessing attacks. We tested our implementation on a small LAN and we are looking forward to extend our implementation to cover cross-realm operations.

Keywords: Computer security, cryptographic protocols, authentication, multicast communication and random numbers.

I. INTRODUCTION

Multimedia group communication is becoming a common channel for everyday work within enterprises and institutes. Protecting the privacy and confidentiality of its content is paramount in network security.

In group communication, two or more principals (e.g., humans or IP addresses) form an entity called a group. When the principals communicate in the context of the group, anything trans- mitted by a member of the group is received by all others in the group. Group communication, and its underlying technology, multicast, has important applications in both Internet-scale, and enterprise and public-safety settings.

In this document's context, 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 establishment of keying materials that can be used by its underlying transport layer's encryption mechanism.
This essentially is what the Internet Engineering Task Force (IETF)'s multicast security working group (Mesc) calls a registration protocol. Its intent is to transport an initial cryptographic key to authorized members of a group so they can then communicate securely with other members of the group. All members of the group possess this key. However, the process of bootstrapping for such a protocol or system is not always trivial. This project attempts to address this problem.

II. EXISTING SYSTEM

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. These collective processes are considered important for effective network management and security. Mutual authentication

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

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 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.

III.PROPOSED METHOD

We introduce simple practical medications to the KDC database to overcome these attacks. In our motive version of Kerberos, the long-term secret key of the network principle will be independent of the principle's password. Instead, the KDC will save a profile for every instance in the realm that it manages. The type of the problem data contents may be audio, video, image, or simply text data. The KDC database may have mixed types of profiles. The network principle may be a client or a server. Every principle in the network is registered in the KDC database by the principle ID. Then the KDC maps this ID to the proper profile where the profile is named with the principle's ID that belongs to that profile. In order to generate the principle's secret key, we apply a hashing algorithm to the principle's profile and then encrypt the output digest. We control the lifetime of the secret key using the current KDC system time that is appended to the principle's profile every predefined period(this period is a design parameter, i.e. a site constant).By this way, we change the input to the hashing function, and consequently, the output of the hashing function and the secret key will change too. In our implementation, we use Triple-DES in CBC mode as an encryption algorithm, SHA-256 as a hashing algorithm, and Blum Shub as a random number algorithm.
The introduced medications to the KDC database will enhance the performance of the protocol since the principle's long-term secret-key will be independent of the user password. Thus, our modified Kerberos version is no longer vulnerable to password guessing attacks. We tested our implementation on a small LAN and we are looking forward to extend our implementation to cover cross-realm operations.

Key Calculation:
In the following, we define a general method (pseudo-random function) to derive one or more keys from a "master" key. This method is used to derive:

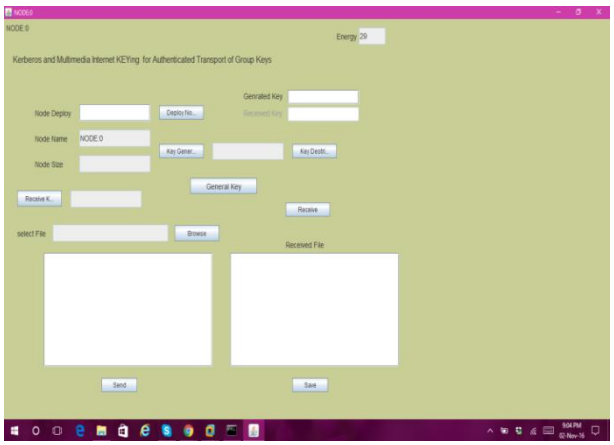
- TEKs from a TGK and the RAND value,
- Encryption, authentication, or salting key from a pre-shared/envelope key and the RAND value.

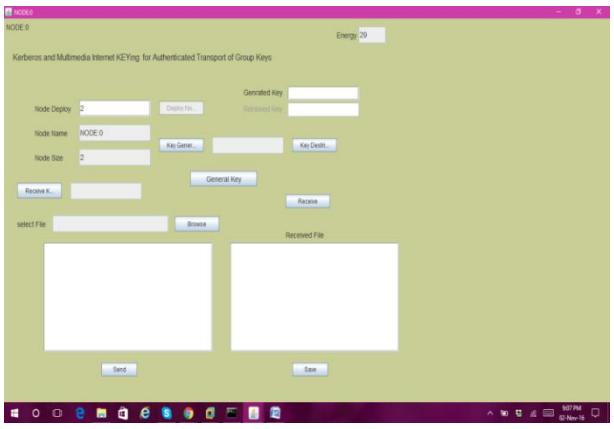
We assume that the following parameters are in place:
csb_id: Crypto Session Bundle ID (32-bits unsigned integer)
cs_id: the Crypto Session ID (8-bits unsigned integer)
RAND : (at least) 128-bit (pseudo-)random bit-string sent by the Initiator in the initial exchange.

The key derivation method has the following input parameters:
Inkey : the input key to the derivation function
Inkey_len : the length in bits of the input key
Label : a specific label, dependent on the type of the key to be derived, the RAND, and the session IDs
Outkey_len: desired length in bits of the output key.

IV. EXPERIMENTAL RESULTS

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained.





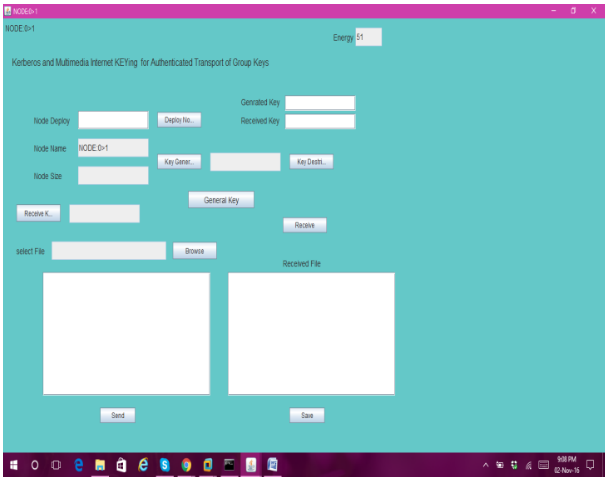
IJARCCE

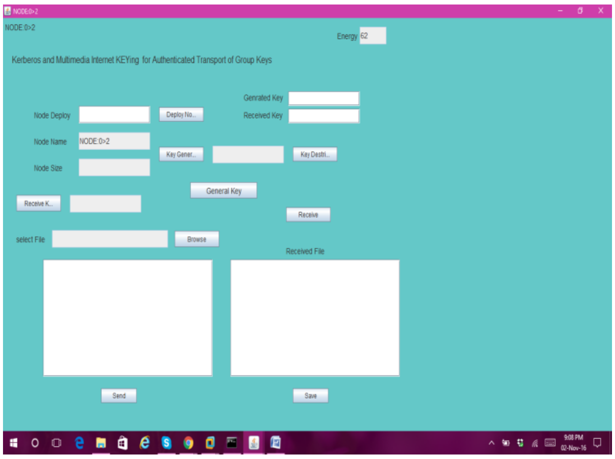
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

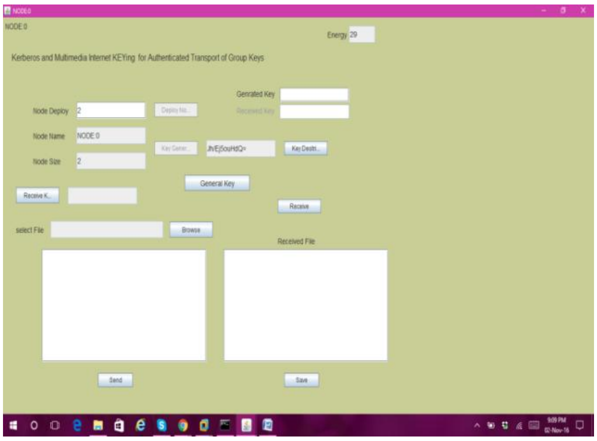
International Journal of Advanced Research in Computer and Communication Engineering

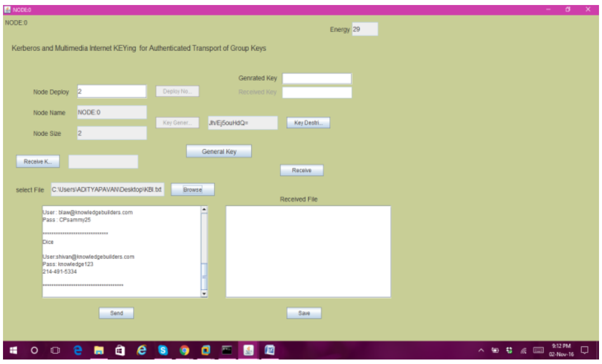
ISO 3297:2007 Certified

Vol. 5, Issue 11, November 2016









V. CONCLUSION

In this project, we have proposed a novel design in using a GDC for user authentication and key establishment. In our design, a GDC does not contain the user's public key. Since the user does not have any private and public key pair, this type of digital certificate is much easier to manage than the X.509 public-key digital certificates. We have also implemented the DL-based protocol based on the concept of GDC, which works successfully and efficiently by generating optimized values at each and every module. We have also embedded an additional facility in this project by providing the data exchange module based on one-time session-key generated by using the secured AES Cryptographic Algorithm.

For future enhancement, the proposed system can be extended by implementing another protocol which is more secured, efficient, and feasible when compared to the DL-based protocol. Another alternative is the IF-(Integer Factoring) based protocol whose security depends on the combination of RSA Signature and One-way-hash function. The protocol provides deniable authentication and protects privacy of the digital certificate. In this project, we have used AES algorithm for secure exchange of data between the entities for further extension our approach can be applied to more advanced and secured cryptographic techniques for secure exchange of data.

.

REFERENCES

[1] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service (V5)," RFC 4120, http://tools.ietf. Org/html/rfc4120, http://www.rfc-editor.org/rfc/rfc4120.txt, July 2005.

[2] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, "MIKEY: Multimedia Internet KEYing," RFC 3830, available from http://tools.ietf.org/html/rfc3830. http://www.rfc-editor.org/rfc/rfc3830.txt, Aug. 2004.

[3] IETF, "Multicast Security (Msec)," http://datatracker.ietf.org/wg/msec/charter/, Sept. 2011.

[4] M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm, "Multicast Security (MSEC) Group Key Management Architecture," RFC 4046 (Informational), Internet Eng. Task Force, http://www.ietf. org/rfc/rfc4046.txt, Apr. 2005.

[5] Kerberos Consortium, "Why is Kerberos a Credible Security Solution www.kerberos.org/software/whykerberos.pdf, 2008.

[6] A. Roy, A. Datta, A. Derek, and J.C. Mitchell, "Secrecy Analysis in Protocol Composition Logic," Proc. 11th Ann. Asian Computing Science Conf., 2006.

[7] G. Bella and L.C. Paulson, "Kerberos Version 4: Inductive Analysis of the Secrecy Goals," Proc. Fifth European Symp. Research in Computer Security, pp. 361-375, 1998.

[8] F. Butler, I. Cervesato, A.D. Jaggard, A. Scedrov, and C. Walstad, "Formal Analysis of Kerberos 5," Theoretical Computer Science, vol. 367, pp. 57-87, Nov. 2006.

[9] W. Diffie, P.C. Van Oorschot, and M.J. Wiener, "Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography, vol. 2, pp. 107-125, June 1992.

[10] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution,"Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cryptology, pp. 232-249, 1994.

[11] M. Baugher, B. Weis, T. Hardjono, and H. Harney, "The Group Domain of Interpretation," http://tools.ietf.org/html/rfc3547, July 2003.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

[12] H. Harney, A. Colegrove, and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol," http://tools.ietf.org/html/rfc4535, June 2006.
[13] 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.
[14] 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.
[15] 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.
[16] D.E. Denning and G.M. Sacco, "Timestamps in Key Distribution Protocols," Comm. ACM, vol. 24, pp. 533-536, Aug. 1981.
[17] A. Roy, A. Datta, A. Derek, J.C. Mitchell, and J.-P. Siefert, "Secrecy Analysis in Protocol Composition Logic," technical report, Carnegie Mellon Univ., http://www.andrew.cmu.edu/user/danupam/secrecy-pcl-mbdf.pdf, 2006.
[18] MIT Kerberos Team, "MITKeberos: Kerberos – The Network Authentication Protocol," http://web.mit.edu/Kerberos/, Feb.2011.
[19] "MiniSIP" http://www.minisip.org/, Feb. 2011.
[20] J. Woo, "Kerberized Multimedia Internet Keying," https://github.com/jltwoo/Kerberized-Multimedia-Internet-Keying, Mar. 2012.
[21] 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 2010.
[22] F. Jordan and M. Medina, "A Complete Secure Transport Service in the Internet," Proc. Network and Distributed Systems Security Symp. (NDSS '93), pp. 67-76, 1993.
[23] 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.
[24] 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.
[25] J. Mattsson and T. Tian, "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)," RFC 6043, http://tools.ietf.org/html/rfc6043, Mar. 2011.
[26] K. Hildrum, "Security of Encrypted Rlogin Connections Created with Kerberos IV," Proc. Network and Distributed System Security Symp. (NDSS), 2000.
[27] "Kerberized File Transfer Protocol (FTP) at MIT," http://ist.mit.edu/services/software/filetransfer/ftp, Sept. 2011.
[28] S. Sakane, K. Kamada, M. Thomas, and J. Vilhuber, "Kerberized Internet Negotiation of Keys (KINK)," RFC 4430, available from http://tools.ietf.org/html/rfc4430, Mar. 2006.
[29] 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.