NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 2, ISSUE 4, APR.-2015

EFFECTIVE KEY GENERATION FOR MULTIMEDIA AND WEB APPLICATION

Mr. Sagar Sharad Bhuite
Department of Computer Science and Engg, College of Engg. Pandharpur
Solapur University, Solapur, India
Prof. Yoginath R. Kalshetty
Asst. Prof. in CSE Dept., College of Engg. Pandharpur
Solapur University, Solapur, India

ABSTRACT

The Effective Key Generation for Multimedia and Web Application is used as the core component of many web and multimedia applications such as pay-TV, teleconferencing, real-time distribution of stock market price and etc. The main challenges for secure multicast are scalability, efficiency and authenticity. In this project, we propose a scalable, efficient, authenticated group key agreement scheme for large and dynamic multicast systems. The proposed key agreement scheme is identity-based which uses the bilinear map over the elliptic curves. Compared with the existing system, the proposed system provides group member authenticity without imposing extra mechanism. Furthermore, we give a scalability solution based on the subgroups, which has advantages over the existing schemes. Security analysis shows that our scheme satisfies both forward secrecy and backward secrecy.

INTRODUCTION

AIM OF THE PROJECT

A)Scalable, Efficient, Authenticated group key agreement scheme for large and dynamic multicast systems.

B)The proposed key agreement scheme is identity-based which uses the bilinear map over the elliptic curves.

C)To Provides Group Member Authenticity.

D)Scalability solution based on the subgroups.

E)To analyze security for forward secrecy and backward secrecy.

GENERAL INTRODUCTION

Effective Key Generation for Multimedia and Web Application provides an efficient way of Group key Agreement in terms of Scalability and Authenticity between the Sub group members and to other group members in the network. The Existing system have the drawbacks such as the Group Controller takes all responsibilities of key generation, re keys generation, message transmission to its sub group members and also to any other group controllers. So lot of bottleneck's to the group controller in the sub group.

The sub group's members are not able to send information's to any other subgroup at the time of re keying process. So performance of the sub group degrades at that time. The re keying process is done every time once a communication is completed between the users in the same group or to any other group members. One of the main challenges for secure

multicast is access control for making sure that only legitimate members of multicast group have access to the group communication. In the passed two or three decades, cryptography has become the well established means to solve the security problems in networking. However, there are still a lot of difficulties for directly deploying cryptography algorithms into multicasting environment as what has been done for unicasting environment.
The commonly used technique to secure multicast communication is to maintain a group key that is known to all users in the multicast group, but is unknown to anyone outside the group. Efficiently managing the group key is a difficult problem for large dynamic groups. Each time a member is added to or evicted from the communication group, the group key must be refreshed.
The members in the group must be able to compute the new group key efficiently, at the same time forward and backward secrecy must be guaranteed. Because the group re keying is very consumptive and frequently performed due to the nature of multicast communication, the way to update it in a scalable and secure fashion is required.

LITERATURE REVIEW

We describe fast new algorithms to implement recent cryptosystems based on the Tate pairing. In particular, our techniques improve pairing evaluation speed by a factor of about 55 compared to previously known methods in characteristic 3, and attain performance comparable to that of RSA in larger characteristics. We also propose faster algorithms for scalar multiplication in characteristic 3 and square root extraction over Fpm, the latter technique being also useful in contexts other than that of pairing-based cryptography.
We construct two efficient Identity-Based Encryption (IBE) systems that admit selective identity security reductions without random oracles in groups equipped with a bilinear map. Selective-identity secure IBE is a slightly weaker security model than the standard security model for IBE. In this model the adversary must commit ahead of time to the identity that it intends to attack, whereas in an adaptive-identity attack the adversary is allowed to choose this identity adaptively. Our _rst system|BB1|is based on the well studied decisional bilinear Di_e-Hellman assumption, and extends naturally to systems with hierarchical identities, or HIBE. Our second system|BB2|is based on a stronger assumption which we call the Bilinear Di_e-Hellman Inversion assumption and provides another approach to building IBE systems. Our rst system, BB1, is very versatile and well suited for practical applications: the basic hierarchical construction can be efficiently secured against chosen-cipher text attacks, and further extended to support efficient non-interactive threshold decryption, among others, all without using random oracles.
Multicast communication is becoming the basis for a growing number of applications. It is therefore critical to provide sound security mechanisms for multicast communication. Yet, existing security protocols for multicast offer only partial solutions. We first present taxonomy of multicast scenarios on the Internet and point out relevant security concerns. Next we address two major security problems of multicast communication: source authentication, and key revocation. Maintaining authenticity in multicast protocols is a much more complex problem than for unicast; in particular, known solutions are prohibitively inefficient in many cases. We present a solution that is reasonable for a range of scenarios. Our approach can be regarded as a ‘midpoint’ between traditional Message Authentication Codes and digital signatures. We also present an improved solution to the key revocation problem.

Secure and reliable group communication is an increasingly active research area by growing popularity in group-oriented and collaborative application. One of the important challenges is to design secure and efficient group key management. While centralized management is often appropriate for key distribution in large multicast-style groups, many collaborative group settings require distributed key agreement. The communication and computation cost is one of important factors in the group key management for Dynamic Peer Group. I extend TGDH (Tree-based Group Diffie-Hellman) protocol to improve the computational efficiency by utilizing pairing-based cryptography. The resulting protocol reduces computational cost of TGDH protocol without degrading the communication complexity.

PROBLEM DEFINITION AND SCOPE

In the Existing system we use Iolus approach proposed the notion of hierarchy subgroup for scalable and secure multicast. In this method, a large communication group is divided into smaller subgroups. Each subgroup is treated almost like a separate multicast group and is managed by a trusted group security intermediary (GSI). GSI connect between the subgroups and share the subgroup key with each of their subgroup members. GSIs act as message relays and key translators between the subgroups by receiving the multicast messages from one subgroup, decrypting them and then re multicasting to the next subgroup after encrypting them by the subgroup key of the next subgroup. The GSIs are also grouped in a top-level group that is managed by a group security controller (GSC).

When a group member joins or leaves only affect subgroup only while the other subgroup will not be affected. It has the drawback of affecting data path. This occurs in the sense that there is a need for translating the data that goes from one subgroup, and thereby one key, to another. This becomes even more problematic when it takes into account that the GSI has to manage the subgroup and perform the translation needed. The GSI may thus become the bottleneck.

LIMITATIONS OF EXISTING SYSTEM

- The Group controller takes all responsibilities for the group such as key generation, re keying process and message transfer to any other groups
- The group members are not able to communicate with any other groups during the re keying process
- The Group controller maintains logical key tree where each nodes represents a key encryption key. The root of the key tree is the group key used for encrypting data in group communications and it is shared by all Users

RESULT

The advantages over the existing system are, we use an identity tree instead of key tree in our scheme. Each node in the identity tree is associated with an identity. The leaf node's identity is corresponding to the user's identity and the intermediate node's identity is generated by its children's identity. Hence, in an identity tree, an intermediate node represents a set users in the sub tree rooted at this node.

The keys used in each subgroup can be generated by a group of key generation centers (KGCs) in parallel. All the members in the same subgroup can compute the same subgroup key though the keys for them are generated by different KGCs. This is a desirable feature especially for the large-scale network systems, because it minimizes the problem of concentrating the workload on a single entity.

ADVANTAGES OF PROPOSED SYSTEM

- The Group controller responsibilities are shared by the Group control intermediater such as Re keying process and scalability of the group process
- Use the Identity tree based structure
- The group members are not affected by the key generation process when they are willing to communicate with any other group members
- The Centralized key server used for key generation process and the KGC is also act as a Router for group to group communication
- The Re keying process is done only to the particular group members not to the entire group member.

CONCLUSION

The Proposed system is an efficient, authenticated, scalable key agreement for large and dynamic multicast systems, which is based on the bilinear map. Compared with the Existing system, we use an identity tree to achieve the authentication of the group member. Further, it solve the scalability problem in multicast communications. Since a large group is divided into many small groups. Each subgroup is treated almost like a separate multicast group with its own subgroup key. All the keys used in each subgroup can be generated by a group of KGC's in parallel. The intuitively surprising aspect of this scheme is that, even the subgroup controller aborts, it does not affect the users in this subgroup. Because every user in the subgroup can act as a subgroup controller. This is a significant feature especially for the mobile and ad hoc networks. From the security analysis we can see that our scheme satisfies both forward and backward secrecy.

REFERENCES

[1]Liming Wang, and Chuan-Kun Wu," *Efficient Key Agreement for Large and Dynamic Multicast Groups" in International Journal of Network Security, Vol.3, No.1, PP.8–17, July 2006 (http://isrc.nchu.edu.tw/ijns/)"*

[2] P. S. L. M. Barreto, H. Y. Kim, and M. Scott, *"Efficient algorithms for pairing-based cryptosystems," in CRYPTO 2002, LNCS 2442, pp. 354–368, 2002.*

[3]P. S. L. M. Barreto, B. Lynn, and M. Scott, "*On the selection of pairing-friendly groups," in SAC'2003, LNCS 3006, pp. 17–25, 2004.*

[4] Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography, Cambridge University Press, 2001.*

[5] D.Boneh and X.Boyen, "*Efficient selective-ID se-cure identity based encryption without random oracles," in Euro crypt 2004, LNCS 3027, pp. 223–238,2004.*

[6] D. Boneh and M. Franklin, "*Identity-based encryption from the weil pairing," in CRYPTO 2001, LNCS2139, pp. 213–229, 2001.*

[7] D. Boneh and J. Katz, "*Improved efficiency for CCA-secure cryptosystems built using identity-based encryption," in CT-RSA 2005, LNCS 3376, pp. 87–103,2005.*
[8] X. Boyen, "*Multipurpose identity-based signcryption: a swiss army knife for identity-based cryptography," in CRYPTO 2003, LNCS 2729, pp. 382–398, 2003.*
[9] R.Canetti, J.Garay, G.Itkis, K.Micciancio, M.Naor, and B. Pinkas, "*Multicast security: a taxonomy and some efficient constructions," in INFOCOM99, pp. 708–716, 1999.*
[10]Y. Kim, A.Perrig, and G.Tsudik, "*Tree-based group key agreement," ACM Transactions on Information and System Security, vol. 7, no. 1, pp. 60–96, Feb.2004.*