Name : Om Pal

Supervisor : Dr. Bashir Alam

Department : Computer Engineering, Faculty of Engg. & Technology

Title of Thesis : Study of Cryptographic Key Management in Perspective of Cyber Security

Abstract

In present era of cyber security, many encryption tools are available. Encryption tools ensure the confidentiality of sensitive information. To encrypt or decrypt the information, there is a need of cryptographic infrastructure which includes the cryptographic keys. To protect the interest of enterprises and nations, each country or designated body frames its security standards and regulatory compliances. To achieve a desired level of secrecy, cryptographic systems use a large number of encryption keys. Confidentiality of information is preserved as long as the encryption keys are secured and managed efficiently.

There are numerous Key Management challenges for efficient and secure cryptographic systems. Most of the cyber security applications such as multimedia transmission, defence systems, distributed computing etc require true authentication of participants, lower re-keying cost, lower storage cost of keying material, lower encryption/decryption cost, secure multicast communication over the network etc therefore, to meet the key management challenges of cyber security applications, there is a need to design and develop the suitable cryptographic key management schemes. Considering the challenges of cyber security applications, focus of the proposed work is 'Study of cryptographic key management in perspective of cyber security'.

In the proposed work, various key management schemes have been analyzed and key management life cycles for symmetric as well as asymmetric cryptographic systems are proposed. Key management model is a framework which provides the guidelines for generation, activation, distribution, use, deactivation, revocation, suspension, update, storage, destruction etc for cryptographic keys. Framework defines the life of key and also provides the guidelines how to manage the key during the various stages. To revoke the cryptographic keys timely and efficiently, a key revocation model is proposed.

The Diffie-Hellman key exchange protocol provides the opportunity to arrive at a common secret key by exchanging texts over insecure medium without meeting in advance. Due to lack of authentication of entities, this protocol is vulnerable towards man-in-middle attack. To deal this vulnerability, an improved key exchange approach based on third party authentication is proposed.

In present-days, most of the cyber security applications use common key for encrypting and decrypting the common information. In such systems like multimedia transmission, conditional access systems, distance learning, video conferencing, distributed network, cloud computing, multi-party games etc. common information is transmitted to more than one recipient. Multicast or group communication enables efficient large-scale content distribution, by providing an efficient transport mechanism for one-to-many and many-to-many communications. Today, the applications that are of multicast in nature have increased significantly. Since most of the group communications take place over the Internet, security is an issue of major concern. For secure group communication, there is a need of distribution of common key to each member of the group. In group communication the main challenges are rekeying cost, storage cost, higher computational load at central server, dynamicity of group, forward and backward secrecy of the data. To address group communication issues, two group key management schemes are proposed. One Group Key Management scheme is based on algebraic group theory and another is based on Elliptic Curve Cryptography. Security and performance analysis of proposed schemes is also done with existing group key management schemes.

In Digital TV service, subscribers get the access of channels of their interest. In Conditional Access Systems, Control Word is used to deliver the multimedia content to legitimate subscribers securely. In order to update the Control Word frequently, a large number of messages are exchanged in the conventional key distribution systems. Due to large number of messages, quality of the multimedia content and timely delivery of the multimedia content are major concerned. To address the issues of key distribution in Conditional Access Systems, two key management schemes are proposed. Out of these two proposed key management schemes, one is based on Elliptic Curve Cryptography and in this scheme, channel package key is computed using the secret polynomial share of the subscriber. Second scheme is based on algebraic group theory, in this scheme channels package search time is optimized using the Optimal Binary Search Tree and Finite State Machine.

Blockchain Technology has the capability to eliminate the requirement of third party to validate the transactions over the Peer-to-Peer network. Public Key Infrastructure is used in Blockchain decentralized infrastructure to authenticate the entity nodes. Confidentiality of the sensitive records over the Blockchain infrastructure is least addressed in the available research literature. To achieve the confidentiality of sensitive records over the Blockchain network, a Group Key Management framework for secure group communication is also proposed.