EFFICIENT KEY GENARATION MANAGEMENT IN A BIG ORGANIZATION FOR SYMMETRIC CRYPTOGRAPHY SYSTEM

ATEFEH MIRZAEE

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Information Security (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

2013

To my beloved mother and father

ACKNOWLEDGEMENT

I would like to take this opportunity to first and foremost thank God for being my strength and guide in the writing of this thesis. Without God help, I would not have had the wisdom or the physical ability to do so. I express my gratitude to my thesis advisor Dr.Majid Bakhtiari for devoting much time to reading my work over and over again. His special interest and knowledge in issues related my research to give me the right guidance and also provided me with much needed motivation. At the end I thank my Family and my friends for always being supportive of my education.

ABSTRACT

Nowadays big organizations have complex administrative structure with scattered offices to face with serious problems related to key management like financial and security problems based on symmetric encryption system. This project proposes an efficient solution related to symmetric key crypto system to solve this problem and provide the opportunity for the organization have a secure, affordable, efficient, easier and faster symmetric key crypto system. Symmetric key cryptography with the less key size have more secure in comparison to asymmetric cryptography. Therefore using symmetric key cryptography is more secure and Advantageous. The speed of processing symmetric cryptography is higher than asymmetric cryptography. The purpose of this project is to product the software for all of the employees in the organization to have the secret symmetric key cryptography to have communicatation to each other through the secret key. However, the security of symmetric key cryptography is higher than asymmetric key cryptography. Key derivations algorithm which used in this project is very important for symmetric cryptosystems in comparison with other algorithm because one key can be derived to the others. This Method is chosen by key derivation one-way function and implemented by Delphi programming language. This implemented method give the manager of the organization an opportunity to generate the secret key for all of the employees and so each employee has the symmetric secret key and if the employees need to communicate with each other their request will be sent to the manager. This project has been done in three phases and one of the outcomes of this project is an application which generates random key, according to hierarchy of organization.

ABSTRAK

Kini organisasi besar yang mempunyai struktur pentadbiran yang kompleks dengan pejabat berserakkan, berhadapan dengan masalah yang serius berkaitan dengan pengurusan utama seperti masalah kewangan dan keselamatan berdasarkan sistem enkripsi simetri. Projek ini mencadangkan satu penyelesaian yang berkesan berkaitan dengan sistem kunci kripto simetri untuk menyelesaikan masalah ini dan memberi peluang kepada organisasi mempunyai sistem kunci kripto simetri yang selamat, murah, cekap, mudah dan cepat. Kunci kriptografi simetri dengan saiz yang kurang lebih selamat berbanding dengan kunci kriptografi tidak simetri. Oleh itu menggunakan kunci kriptografi simetri adalah lebih selamat dan berfaedah. Kelajuan pemprosesan kriptografi simetri adalah lebih tinggi daripada kriptografi tidak simetri. Tujuan projek ini adalah untuk menghasilkan perisian untuk semua pekerja dalam organisasi mempunyai kunci kriptografi simetri rahsia untuk berkomunikasi antara satu sama lain melalui kunci rahsia. Walau bagaimanapun, keselamatan kunci kriptografi simetri adalah lebih tinggi daripada kunci kriptografi tidak simetri. Algoritma Kunci Terbitan yang digunakan dalam projek ini adalah sangat penting bagi sistem kripto simetri berbanding dengan algoritma lain kerana satu kunci boleh diterbitkan kepada yang lain. Kaedah ini dipilih oleh fungsi terbitan kekunci sehala dan dilaksanakan oleh bahasa pengaturcaraan Delphi. Kaedah ini dilaksanakan dengan memberi peluang kepada pengurus organisasi untuk menjana kunci rahsia untuk semua pekerja supaya setiap pekerja mempunyai kunci rahsia simetri dan jika pekerja perlu berkomunikasi antara satu sama lain permintaan mereka akan dihantar kepada pengurus. Projek ini telah dilaksanankan dalam tiga fasa dan salah satu hasil daripada projek ini adalah sebuah aplikasi yang menjana kunci rawak, mengikut hierarki dalam organisasi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

In key management, it is important to recall that there are two basic types of cryptography:

i. Symmetric or secret key
ii. Asymmetric or public key.

Symmetric cryptography is characterized by the fact that the same key is used to perform both the encryption and decryption. This means that the communicating parties must have copies of the same cryptographic key, and a method to securely communicate these keys for the appropriateness of parties must be available. Compromise of the secret key naturally leads to the compromise of any data that was encrypted using that key (Van Tilborg and Jajodia, 2011).

Asymmetric cryptography is characterized by the fact that the key used to perform a cryptographic operation such as digital signature creation is not the key used to perform the inverse cryptographic operation such as digital signature verification. Public key cryptography is based on the notion of key pairs. One key is referred to as the public key and can be revealed to anyone. The other key is referred to as the private key and is not revealed to anyone other than the end-entity

associated with that key (although there are exceptions such as private key backup with a trusted third party when required). These keys are mathematically related; however, knowledge of the public key does not disclose enough information to allow an attacker to verify the private key efficiently. The concept of asymmetric cryptography was first introduced to the general public in 1976, but much of the technology necessary to support public key cryptography was not available until the mid-1990s (Van Tilborg and Jajodia, 2011).

Symmetric cryptography and asymmetric cryptography are not necessarily mutually exclusive. In fact, these techniques can be used together in order to offer a complementary set of services. For example, symmetric cryptography can be used to encrypt a message and asymmetric cryptography can be used to securely transfer the secret key used to encrypt the file to the intended recipient(s). However, this is not always possible and other distribution mechanisms may be required. To illustrate these concepts in more detail, key management is first discussed in the context of a secret key only system. This will be followed by a discussion of public key cryptography and how public key and secret key cryptography can be used together (Van Tilborg and Jajodia, 2011).

When the first electronic symmetric cryptosystems were deployed, key management was physical in nature and it required a significant amount of human involvement. Keys were centrally generated and recorded on media such as paper or magnetic tape, and the keying material was physically distributed to the appropriate locations. This was sometimes accomplished through the use of couriers (sometimes humorously referred to as “sneaker net”). The keying material was physically destroyed when no longer needed (Van Tilborg and Jajodia, 2011).

However, modern symmetric cryptosystems are more advanced and typically use some form of electronic key distribution. One possible model for electronic distribution of symmetric keys is based on a trusted third-party component known as a Key Distribution Center (KDC). Before an end-entity (e.g., an end user) can access a target resource (e.g., a server), the end-entity makes a request to the KDC to

establish a session key that can be used to secure the communication between the end entity and the target resource. This model is illustrated in Figure 1.1 (Van Tilborg and Jajodia, 2011).

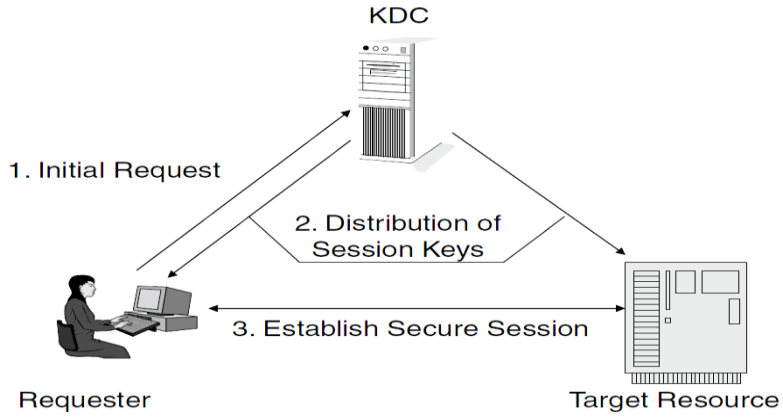

Figure 1.1 Key distribution center model

The terminology of Table 1.1 is used in reference to keying material and Classify keys by algorithm type. A symmetric cryptographic system is a system involving two transformations – one for the originator and one for the recipient – both of which make use of either the same secret key (symmetric Key) or two keys easily computed from each other. An asymmetric cryptographic system is a system involving two related transformations – one defined by a public key (the public transformation), and another defined by a private key (the private transformation) – with the property that it is computationally infeasible to determine the private transformation from the public transformation (Vanstone et al., 1996).

Table 1.1 Definition of existing keys

Term	**Meaning**
private key, public key	paired keys in an asymmetric cryptographic system
symmetric key	key in a symmetric (single-key) cryptographic system
secret	adjective used to describe private or symmetric key

Key management involves all the operations related to cryptographic keys, including key generation, distribution, storage, update, and cancellation (Van Tilborg and Jajodia, 2011). The life cycle associated with this keying material such as the initialization, distribution, and cancellation of the keys is referred to as key management.

One of the most challenging aspects of setting up a cryptographic security system is Key management. In order to work and be secure for a cryptosystem, each of its users must have a set of secret keys (in a secret-key system) and or a public-private key pair (in a public-key system). This involves generating the keys and securely distributing them to the users or providing the users with a way of generating the keys. It also involves providing the users with the capability to securely store and manage secret and private keys. In public-key systems, key management includes the capability to verify and manage the public keys of other users who are signed in the form of digital certificates. Figure 1.2 provides an overview of these key management activities (Jaworski et al., 2000).

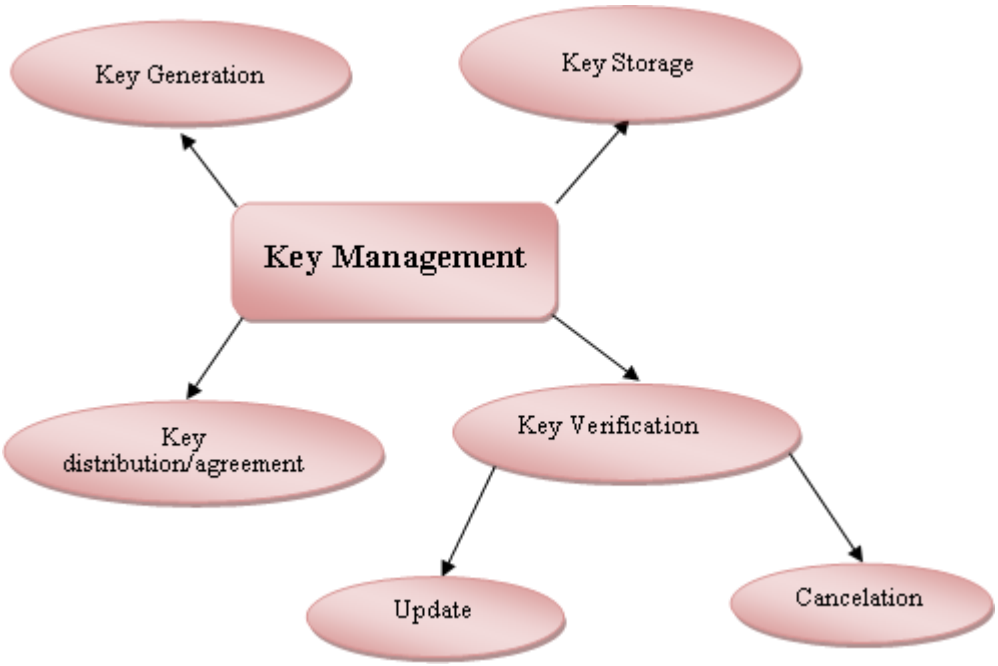

Figure 1.2 Key management Activities

Key management plays a fundamental role in cryptography as the basis for securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures. The goal of a good cryptographic design is to reduce more complex problems to the proper management and safe-keeping of a small number of cryptographic keys, ultimately secured through trust in hardware or software by physical isolation or procedural controls. Reliance on physical and procedural security (e.g., secured rooms with isolated equipment), tamper-resistant hardware, and trust in a large number of individuals is minimized by concentrating trust in a small number of easily monitored, controlled, and trustworthy elements (Vanstone et al., 1996).

Keying relationships in a communications environment involve at least two parties (a sender and a receiver) in real-time. In a storage environment, there may be only a single party, which stores and retrieves data at distinct points in time (Vanstone et al., 1996).

The objective of key management is to maintain keying relationships and keying material in a manner which counters relevant threats, such as:

i. Compromise of confidentiality of secret keys.
ii. Compromise of authenticity of secret or public keys. Authenticity requirements include knowledge or verifiability of the true identity of the party a key is shared or associated with.
iii. Unauthorized use of secret or public keys. Examples include using a key which is no longer valid, or for other than an intended purpose (Vanstone et al., 1996).

In practice, an additional objective is conformance to a relevant security policy (Vanstone et al., 1996). Key management is usually provided within the context of a specific security policy. A security policy explicitly or implicitly defines the threats a system is intended to address. The policy may affect the stringency of cryptographic

requirements, depending on the susceptibility of the environment in question to various types of attack. Security policies typically also specify:

i. Practices and procedures to be followed in carrying out technical and administrative aspects of key management, both automated and manual;
ii. The responsibilities and accountability of each party involved; and
iii. The types of records (audit trail information) to be kept, to support subsequent reports or reviews of security-related events (Vanstone et al., 1996).

Key management is the set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. Key management encompasses techniques and procedures supporting:

i. Initialization of system users within a domain;
ii. Generation, distribution, and installation of keying material;
iii. Controlling the use of keying material;
iv. Update, revocation, and destruction of keying material; and
v. Storage, backup/recovery, and archival of keying material (Vanstone et al., 1996).

One of the most important protocol for communication between two point in key management that contain of Authentication, Authorization, and Accounting (AAA) key management protocols (Harney et al., 2006) .AAA key management often includes a collection of protocols, one of which is the AAA protocol. Other protocols are used in conjunction with the AAA protocol to provide an overall solution. These other protocols often provide authentication and security association establishment (Aboba and Housley, 2007).

The protocol that is AAA Given the complexity and difficulty in designing secure, long-lasting key management algorithms and protocols by experts in the field, it is almost certainly inappropriate for IETF working groups without deep

expertise in the area to be designing their own key management algorithms and protocols (Aboba and Housley, 2007).

1.2 Background of the Problem

There are many financial and security problems related to the key management in a big organization that have scattered offices .Therefore, most of big organization by compromising the security, prefer using from asymmetric key crypto system. This study proposes a new solution related to symmetric key crypto system.

1.2.1 Reduce Complex Problem with Different Methods

Key management plays a fundamental role in cryptography as the basis for securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures. The goal of a good cryptographic design is to reduce more complex problems to the proper management and safe-keeping of a small number of cryptographic keys, ultimately secured through trust in hardware or software by physical isolation or procedural controls. Reliance on physical and procedural security (e.g., secured rooms with isolated equipment), tamper-resistant hardware, and trust in a large number of individuals is minimized by concentrating trust in a small number of easily monitored, controlled, and trustworthy elements (Vanstone et al., 1996).

1.2.2 Addressing the Protection of Information Processing Applications

Key management has been identified as a major component of national cyber security initiatives that address the protection of information processing applications

(Iyer, 2011). Numerous problems have been identified in current key management methodologies, including the lack of guidance, inadequate scalability of the methods used to distribute keys, and user dissatisfaction because of the "unfriendliness" of these methods (Barker et al., 2009).

1.2.3 Future Key Management Methods: David McGrew, Cisco

The focus of the talk was from a manufacturer's perspective and included the challenges of the equipment distribution problem and creating a manufacturer's device certificates. A manufacturer often ships devices to customers with a hardwired private key, device certificate, and device identifier. This would give the capability for devices to authenticate each other from a distance, but would not solve the authorization problem (Barker et al., 2009). The future key management methods are:

i. Threshold cryptography was discussed such as M out of N keys must be available to perform an operation, as well as manufacturing certificates, automating manual key distribution, and a symmetric key generation system (Barker et al., 2009).
ii. Threshold cryptography is useful for encrypted data storage access such as a minimum number of people must cooperate in order to retrieve sensitive, stored information (Barker et al., 2009).
iii. There is a problem with replacing the keys and updating revocation lists. We need to be able to streamline the distribution process and replace manual key distribution with a minimal impact process (Barker et al., 2009).
iv. We need an automated CKM system that can be implemented in existing systems (Barker et al., 2009).
v. Requirements include: the authenticated/authorized distribution of keys, keys must persist over a long term, a system that replaces/updates keys when needed, key creation should not be centralized, minimal operational impact, and the CKM should be interoperable with Multipoint Key Distribution

(MKD). Candidates for this type of KM system would be Kerberos (for session keys), OASIS (for storage keys) or GDOI (for group key management) (Barker et al., 2009).

1.2.4 Problem of Key Management in an Access Hierarchy

The problem of key management in an access hierarchy has elicited much interest in the literature. The hierarchy is modeled as a set of partially ordered classes (represented as a directed graph), and a user who obtains access such as a key to a certain class can also obtain access to all descendant classes of her class through key derivation. Our solution to the above problem has the following properties (Atallah et al., 2005):

i. Only hash functions are used for a node to derive a descendant's key from its own key;
ii. The space complexity of the public information is the same as that of storing the hierarchy;
iii. The private information at a class consists of a single key associated with that class;
iv. Updates (revocations, additions, etc.) are handled locally in the hierarchy;
v. The scheme is provably secure against collusion; and
vi. Key derivation by a node of its descendant's key is bounded by the number of bit operations linear in the length of the path between the nodes (Atallah et al., 2005).

The Table 1.2 shows NIST guidelines for public key sizes. It present that 128 key size in AES equal to 3072 key size in RSA and it means that in symmetric key cryptography with the less key size have more security and on the other hand in asymmetric cryptography with more than key size have the same security so that using the symmetric key cryptography is more secure and Advantageous.

Table 1.2 NIST guidelines for public key sizes

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	**1024**	**1:6**	
256	**3072**	**1:12**	**128**
384	**7680**	**1:20**	**192**
512	**15 360**	**1:30**	**256**

1.3 Problem Statement

Nowadays big organizations have complex administrative structure with scattered offices to face with serious problems related to key management like financial and security problems that based on symmetric encryption system. However, the key management problems are already in a current problem in asymmetric and symmetric key crypto system.

Therefore, most of big organizations by compromising the security prefer using from asymmetric key crypto system. This study proposes a new solution related to symmetric key crypto system so that with solving this problem the organization can have a secure, affordable, efficient, easier and faster symmetric key crypto system.

In symmetric key cryptography with the less key size have more security and on the other hand in asymmetric cryptography with more than key size have the same security so that using the symmetric key cryptography is more secure and Advantageous. The speed of the symmetric cryptography is higher than the asymmetric cryptography because the key size of the symmetric key is more less

than the asymmetric key cryptography so that with consider that the security of symmetric key cryptography is higher than asymmetric key cryptography.

1.4 Project Objective

1. To study on key management in symmetric key and asymmetric crypto system.
2. To purpose an efficient solution of key generation management in a big organization that use symmetric cryptography.
3. To test, evaluate and implement of an efficient solution of key generation management in a big organization.

1.5 Research Questions

1. What is the significance of key management in symmetric key and asymmetric crypto system?
2. What is the efficient solution of the key generation management in a big organization that uses symmetric cryptography?
3. How implement, evaluate and test of this efficient solution of key generation management in a big organization?

1.6 Project Scope

The domain of this study concentrated on symmetric key and asymmetric crypto system independent of the encryption algorithm. This project is explained the definition of key management in symmetric key and asymmetric crypto system. In most of the big organization by compromising the security, prefer using from

asymmetric key crypto system. This study proposes a new solution related to symmetric key crypto system.

1.7 The Project Importance

There are many financial and security problems in big organization related to the key management that have spread over offices .Therefore, most of big organization by compromising the security, prefer using from asymmetric key crypto system. This study proposes a new solution related to symmetric key crypto system so this solution can be the importance tip about this project. Also this study can solve some of the problems related to the key management by using symmetric key crypto system.

1.8 Organization Report

This study focuses on Efficient Key Management in a Big Organization for Symmetric Cryptography System.

In Chapter 1, the study has explained the definition of key management in symmetric key and asymmetric crypto system and also is surveyed about the different background of problems and problem statement. At the end of this chapter the different objective of this study has stated. In Chapter 2, the study has explained literature review that is about previous researches related to key management for symmetric cryptography system. In Chapter 3, the study has presented the road map of research, according to its frame work of study. In Chapter 4, the study will analysis and design an efficient key generation management for a big organization with dynamic hierarchy. In Chapter 5, the study will implement and test each of

achievement which have stated in Chapter 1, and finally in Chapter 6, the conclusion of the study will be presented.

REFERENCES

ABOBA, B. & HOUSLEY, R. (2007) Guidance for Authentication, Authorization, and Accounting (AAA) Key Management.

AMIR, Y., KIM, Y., NITA-ROTARU, C. & TSUDIK, G. (2004) On the performance of group key agreement protocols. ACM Transactions on Information and System Security (TISSEC), 7, 457-488.

ATALLAH, M. J., FRIKKEN, K. B. & BLANTON, M. (2005) Dynamic and Efficient Key Management for Access Hierarchies.

BARKER, E., BARKER, W., BURR, W., POLK, W. & SMID, M. (2011) Recommendation for key managementâ€“part 1: General (revision 3). NIST special publication, 800, 57.

BARKER, E., BRANSTAD, D., CHOKHANI, S. & SMID, M. (2009) Cryptographic Key Management Workshop Summary. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg.

BURNETT, S. & PAINE, S. (2001) The RSA Security's Official Guide to Cryptography, McGraw-Hill, Inc.

BURNETT, S. & PAINE, S. (2004) RSA Security's official guide to cryptography.

CALLEGARI, S., ROVATTI, R. & SETTI, G. (2005) Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos. Signal Processing, IEEE Transactions on, 53, 793-805.

CHEHAL, R. & SINGH, K. (2012) Efficiency and Security of Data with Symmetric Encryption Algorithms. International Journal, 2.

CRAMPTON, J. (2003) On permissions, inheritance and role hierarchies. Proceedings of the 10th ACM conference on Computer and communications security. ACM.

HALLIDEN, P. (1997) The management of symmetric keys. Information Security Technical Report, 2, 44-53.

HARNEY, H., METH, U., COLEGROVE, A. & GROSS, G. (2006) GSAKMP: group secure association key management protocol. RFC4535, IETF, June.

IYER, S. (2011) Cyber Security for Smart Grid, Cryptography, and Privacy. International Journal of Digital Multimedia Broadcasting, 2011.

JAWORSKI, J., PERRONE, P. & CHAGANTI, V. S. (2000) Java security handbook, Macmillan Press Ltd.

NOOR, A. (2007) Symmetric Key Management Systems. ISSA, 26-29.

RAFAELI, S. & HUTCHISON, D. (2003) A survey of key management for secure group communication. ACM Computing Surveys (CSUR), 35, 309-329.

RUSHTON, A. (2010) The handbook of logistics and distribution management, Kogan Page.

SHERMAN, A. T. & MCGREW, D. A. (2003) Key establishment in large dynamic groups using one-way function trees. Software Engineering, IEEE Transactions on, 29, 444-458.

TILBORG, H. C. A. V. & JAJODIA, S. (2011) k-Anonymity. Encyclopedia of Cryptography and Security.

VAN TILBORG, H. C. A. & JAJODIA, S. (2011) Encyclopedia of cryptography and security, Springer.

VANSTONE, S. A., VAN OORSCHOT, P. C. & MENEZES, A. (1996) Handbook of applied cryptography. XP-002250459, 553.

WANG, L. & WU, C.-K. (2006) Efficient key agreement for large and dynamic multicast groups. International Journal of Network Security, 3, 8-17.

WONG, D. S. & CHAN, A. H. (2001) Mutual authentication and key exchange for low power wireless communications. Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE. IEEE.