INTERPRETATIVE KEY MANAGEMENT FRAMEWORK (IKM)

SAMAN SHOJAE CHAEIKAR

A thesis submitted in partial fulfillment of the
requirement for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

APRIL 2010

This document is dedicated to my beloved father, mother, and sister.

ACKNOWLEDGEMENT

I would like to express my greatest gratitude to my supervisor of this project Dr. Shukor Bin Abd Razak for his great support and guidance. His trust and confidence in me throughout the entire project have contributed much in the completion of this project. I would also like to thank him for his time, opinions and suggestions.

ABSTRACT

Cryptography has been employed to establishing secure communication over insecure networks. Using symmetric keys to encipher and decipher data is one of common practices for achieving secrecy over networks. To employ symmetric key cryptography we require a secure and reliable key management framework for generating, distributing, and finally revoking keys. Many attacks endanger security of key management in each step and so need of secure key management frameworks now is felt more than ever. Proposed, Interpretative Key Management, framework reduces likelihood of attacks by eliminating key storage, reducing many times key distribution to just one time interpreter distribution, and increases security by means of using minutely, hourly, or daily key without need of key distribution. Also key revocation is automated process and IKM doesn't require revocation call.

ABSTRAK

Kriptografi telah digunakan untuk membina saluran komunikasi yang selamat di atas talian rangkaian yang tidak selamat. Salah satu amalan yang digunakan untuk encipher dan decipher data ialah dengan menggunakan kekunci simetrik untuk mencapai kerahsiaan di atas rangkaian. Untuk menggunakan kekunci simetrik, kita memerlukan kerangka pengurusan kekunci yang selamat dan boleh dipercayai untuk membina, mengagih dan akhirnya menghapuskan kekunci. Banyak serangan keselamatan berlaku di dalam setiap langkah pengurusan kekunci dan ini menyebabkan kerangka pengurusan kekunci diperlukan daripada sebelumnya. Cadangan mentafsir pengurusan kekunci, rangka kemungkinan serangan dengan menghapuskan simpanan kekunci, mengurangkan masa pengagihan kekunci dengan hanya menggunakannya sekali sahaja, dan meningkatkan keselamatan dari segi ketelitian, setiap jam atau kekunci harian tanpa perlu mengagihkan kekunci. Tambahan penghapusan kekunci dilakukan secara automatik dan IKM tidak memerlukan arahan penghapusan.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CCA	-	Common Conference Agreement
CKDS	-	Conference Key Distribution System
DeGKMP	-	Decentralized Group Key Management Protocol
GC	-	Group Controller / Group Center
GK	-	Group Key
GSA	-	Group Security Association
HIBE	-	Hierarchical Identity-Based Encryption
ID	-	Identity
KDS	-	Key Distribution System
KMP	-	Key Management Protocol
LASSB	-	Location-Aware and Secret Share Based
LOCK	-	Localized Combinatorial Keying
MAC	-	Message Authentication Code
MANET	-	Mobile Ad hoc Network
MSEC	-	Multicast Security
PKG	-	Private Key Generator
PRF	-	Pseudorandom Functions
SDNS	-	Secure Data Network System
SGC	-	Secure Group Communication
SGK	-	Subgroup Key
SMKD	-	Scalable Multicast Key Distribution
SMuG	-	Secure Multicast Group
WSN	-	Wireless Sensor Network

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

One of common methods for establishing secure connections across insecure communication channels is employing symmetric key cryptography practices to guarantee secrecy of transmitted data. Key management is process of generation, distribution, and revocation of cryptographic keys among all parties going to use cryptographic keys to enhance security of data transmission.

Although seems that enciphering guarantees secrecy, but many attack types endanger using cryptography from beginning which is generating key to the end which is revocation of distributed key. Attackers try to crack in process of key issuance, and then interceptors try to capture keys while is distributing among key users. In addition some techniques exist for achieving keys like analysis of sent packets, or performing exhaustive key search.

Many types of key management practices are deployed today to apply required security features, but every practice has its own weaknesses. For some key distribution is main difficulty, for some storing and retrieving keys for future use, for some the traffic imposes network and servers, for some attacks that endanger security of specific step, and many other dangers are difficulties key management schemes are facing with today.

Main traffic flow of current key management schemes is from key producer toward nodes. It means that a single or limited number of computers have duty of producing keys for nodes and distributing it among users and repeating these processes continuously. But in proposed framework, in this dissertation, near hundred percent of key production process is within nodes and key server is mostly supervisor of nodes' activities.

Most important features of proposed framework are:

- Eliminating key storage;
- One time distribution of interpreter rather many times key distribution;
- Using fresh key;
- Reducing likelihood of replay attack;
- Unique (or multiple) key per session;
- No necessity of key revocation; and
- Reducing key server and network traffic.

1.2 Problem Background

"Cryptography (or cryptology; from Greek κρυπτός, kryptos, "hidden, secret"; and γράφω, gráphō, "I write", or -λογία, -logia, respectively) is the practice and study of hiding information."[1]

Heretofore cryptography referred almost exclusively to enciphering, which is the process of hiding ordinary information (plaintext) into unmeaning gibberish. Deciphering is the reverse action, in other words, moving from the unmeaning enciphered text back to plaintext. A cipher is a couple of algorithms which make possible encryption and decryption. Cipher in depth is controlled both by an algorithm and in each instance a key that is secret parameter (that should be known only to the communication parties) for a particular message exchange context.

Ciphers without changeable keys are trivially breakable and therefore useless for most purposes.

Symmetric key cryptography is a technique that both parties use same secret for encryption/decryption or sometimes employing different keys while both are trivially related together and computable from each other.

Today's study of symmetric key ciphers focuses mainly on the research on block ciphers and stream ciphers and their usage. Block cipher takes in chunk of plain text and after enciphering with using a key produces same length cipher text. Since length of messages in most cases is longer than a block length, therefore string of blocks is required to provide block coverage. Almost always last block requires padding to make required length.

Key management is providing cryptography system design that includes production, exchange, saving, safeguarding, employing, vetting, and rekeying of keys. Key management involves keys in user level between users or key management technique which is in contrast to key scheduling; key scheduling is internal handling of keys within the cipher operation.

Prosperous key management is vital for security of a cryptosystem. In practice it is approximately the most difficult approaches of cryptography because it involves system policy, user awareness, organizational and departmental interactions, and cooperation between all of mentioned elements.

These concerns are not limited to cryptographic experts. Key management is two sided and requires both technical and organizational decisions, and as a result, some approaches of key management risk have been ignored by managers and engineers, regardless of concern that the problem is technical or managerial.

1.3 Problem Statement

Today, two types of cryptography keys exist which are symmetric and asymmetric cryptography keys. Symmetric key cryptography is using same key for enciphering and deciphering process, but in asymmetric cryptography encryption and decryption keys are different, so we need extra infrastructure to establish asymmetric cryptography.

Once a symmetric key has been created, needs to be distributed, be employed, and finally be revoked, but many issues exist besides running these processes.

First difficulty of key management is creating secure key. After key creation some keys must be omitted from key pool to achieve a group of trustworthy keys. Length, randomness, creation method, and lifetime of generated keys are main important items in key issuance (or generation) process.

Second difficulty rises from key distribution which is second step of key management. Key distribution is process of spreading generated key among all nodes going to use the key to make secure session for safe data transferring. First-time key distribution is second issue of key management process. Some methods today exist for secure first time key distribution over insecure communication facilities and the most common way is establishing secure channel between key generator and node by means of Diffie-Hellman scheme. Diffie-Hellman establishes the required secure channel after performing some computations between sender and recipient, but the process is highly resource consumer because there are up to 300 digit numbers in computations. Making secure channel is required for distributing first required key but afterward in many cases we want to utilize fresh keys or in fact enhance security by employing a new key per session. Key distribution resource consumer process is second issue key management is faced with.

Last process of key management is informing all nodes that issued key is not valid afterward for session use. It again requires consuming time and resources to

inform all nodes that last key no more is valid. Also after nodes became aware about revoked key, generating and distributing a new key is required again.

In addition of three mentioned main issues, another issue is existence of key storage. Key storages increases probability of compromising generated key against adversaries. Resolving need of key storage is one of crucial factors in enhancing security.

Employing fresh key or utilizing key per session is very hard and expensive process by means of current key management frameworks. In addition need of key storage is another issue enumerated above. So here we propose a new key management framework which lightens some difficulties and omits some other to achieve easier and more secure key management.

1.4 Project Aim

Current key management practices have many issues in each step that increase likelihood of compromising. Aim of this study is to enhance security of key management to achieve more secrecy in encrypted session establishment.

1.5 Research Question

What are current key management schemes?

What are issues of current key management practices?

How to enhance security of key management?

1.6 Research Objectives

Overall objective of this study is designing a new key management framework which enlightens issues of currently practiced key management schemes. In fact goal of this study is proposing a new workflow which removes some difficulties and enlightens some other to achieve easier and more secure framework. Specific objectives of new framework are listed as follow:

- To investigate current key management issues;
- To design a framework that enhances security of key management by reducing likelihood of attacks and enhances security of transactions by means of using fresh keys; and
- To evaluate effectiveness of proposed framework by publishing it in international conferences and testing in simulator.

Features of new framework will enhance and ease process of key management by devolving most of duties on nodes.

1.7 Significance of study

Nowadays, we need computer network communications to do what is needed in our daily lives. We search the web for a flight, download books, play games, watch movies, participate in social networks, and many so on without observing security measures. But not any kind of activity like doing online banking, or transferring sensitive data is possible to be done without considering it.

To achieve secure data transmission over computer networks, data should be encrypted before being transmitted. First need of establishing secure session is having a key in hand of both sender and receiver. Process of creating, distributing, and revoking keys is called key management. Although it is in fact heart of

cryptography but has many issues which endanger safety of establishing secure communications.

This study tries to enhance security of key management to reduce likelihood of compromising and modifies key management work flow to decrease number of attacks. Results of this study makes organizations capable to establish more secure network connections than before with less cost.

1.8 Research Scope

Scope of this study firstly is limited to use of symmetric key cryptography. Because of having same process of key generation both in server side and client side, interpretative key management only can support use of symmetric keys. Second limitation is that we consider engaged nodes as trustworthy points. This framework is more suitable for ATM like networks or companies which are spread worldwide and nodes are well known and under control.

Outlined scope points are:

- Use of symmetric cryptographic keys;
- Having well knows key users like ATM machines or distinguished computers of a company (or counterpart companies);
- Deploying in environments going to have secure connections for more than one month;
- Because of popularity of Windows OS and compatibility of Delphi features for developing needed simulator, chosen platform and programming language for developing simulator are Windows XP and Borland Delphi 7.

1.9 Summary

This chapter discusses about role of cryptography in our daily life and importance of key management in cryptography deployment. Key management issues are explained and those which are in scope discussed in more details. Research objectives and scope show exact extent of project and the way that this research is headed.