SECURE RSA WITH CIPHER TEXT DIGEST

Himanshu Gupta[1], Mr. Arvind Kumar Singh[2]
Department of Computer Science and Engineering, SHEAT Group of Instititions, Varanasi.

Abstract: There is need to protect the sensitive/relevant data whenever we wants to share on remote medium. There are many solution exist in computer world. In this paper, I'm developing integrated solution for data protection when we want to share to other over internet. There is need to protect the sensitive/relevant data whenever we wants to share on remote medium. There are many solution exist in computer world. In this paper, I'm developing integrated solution for data protection when we want to share to other over internet.
Keywords: Asymmetric key, Encryption,Decryption.

I. INTRODUCTION

Overview

The need for data security is very important factor in shared file system over internet, because the value of data is much more than the value of the underlying devices. The theft and attack in shared system is the risk of identifying theft in addition to the loss of integrity or leakage ofmessage.

Hence, it is fast becoming necessary to protect stored data from unauthorized access and protect data over internet when message file send using strong cryptographic methods.

In this thesis for above mentioned purpose we are working on RSA cryptographic algorithm. With this approach I'm using an extra digest method for maintaining the inconsistency of the message that is need to share over internet.

Motivation

An enterprise-ready data protection system is vital in military organizations where classified and secret data need to be shared and secured simultaneously. Recent news reports of security breaches and data thefts from India's military and intelligence agencies accentuate the critical need for a cryptographic solution to thisproblem.

Data protection systems are increasingly playing a crucial role in commercial environments too. So, there is a need to design and develop secure and usable data protection Computer Application that form to the above application scenarios. Encrypting file systems enables to individuals and organizations to keep their storage data highly available and protected from unauthorized access at the same time.

II. RELATED WORK

There is a need to provide security for system level data files, security of networking level data remains a largely neglected area both in the development and use of such systems. Nonetheless, various implementations of encrypting file systems exist. We first elaborate on some common design paradigms and then describe some popular related systems. The choice of the basic design approach greatly influences the security, performance and usability features provided by these systems.

System DesignApproaches

Essentially, encryption of the files to be send over the network that introducing an extra layer of an appropriate mechanism in the system that provides the necessary cryptographic functionality. Hence, the first decision to be taken when designing an encrypting system concerns the placement of this layer. On this basis, encryption systems may be classified into the followingtypes:

Application level: In such a design, files are individually encrypted at the discretion of the end user. A separate suite of applications may be developed that encrypts and decrypts files as and when required by the user. Although such software provide a high degree of flexibility in choosing the exact files to be encrypted, send the file over internet toreceiver.

Device level: Such software, also known as RSA Encryptor solve the transparency issue by placing the solution at a lower layer that is conceptually closer to the physical storage device. Although RSA encryptor (RSAC) system would naturally work for the best performance, they are unmanageable and inflexible. Typically, such systems use only one key to encrypt the all files making them vulnerable to theattacks.

III. DOMAIN

3.1 Implementation Domain

To implement RSA using mathematical function developed by me. It is working as message digester that gets a numeric value of cipher text.

In this implementation we are working on encryption of two files. These two files are the .txt formatted files.

In this implementation we can save the encrypted files and send to the receiver using

receiver's email-id and it's required to enter the sender email-id and password.

A generic asymmetric key class has been integrated that provides to call public key encryption, decryption and verification functions from within the platform library. Public key cryptosystems RSA are implemented to underlying the generic asymmetriclibrary.

It must be noted that a scheme that calls on a user-space service for only certificate verification is as insecure as one in which all public key management and operations occur in user-space. Thus, a skeletal Public Key Infrastructure support library must also be integrated into the kernel that provides functionality to decode and parse Base64- encoded PEM format X.509 certificates, verify their validity and extract the publickey.

3.2 RSAC (Secure File Transmitter) inAction
We now describe the installation, usage and operation of this project and provide overview of its implementation.

3.2.1 Enterprise deployment
The following prerequisite activities must first be carried out when RSAC is being deployed in an enterprise environment:
A public and private key pair must be generated for all users in the authentication domain who require access to encrypted file systems.

3.2.2 Encrypted file creation andDigest
A generic asymmetric key class has been integrated that provides to call public key encryption, decryption and verification functions from within the platform library. Public key cryptosystems such as RSA are implemented to underlying the generic asymmetric library.
Using library class generated private key, follow the encryption process for .txt file. This process applied to both selected files.
After producing the cipher text files we apply the mathematical digest function to find the digest value of encrypted file. To find the digest value of the cipher text we develop a mathematical function shown in fig. 4.1 and 4.2. This function produce two separate numbers for both encrypted files.
There are send these numbers to the receiver's mail id also with both encrypted files.

3.2.3: Decryption to encrypted file and Digest
After sending the cipher text files we apply the decryption process at end of receiver using public key that is append with themessage.
After successful Decryption we get two digest number, these two numbers must be equal to the received digest number in message. This mathematical digest function is used to maintaining the integrity security in themessage.

IV. CONCLUSION

This section presents a detailed comparison of the features, working style and design choices of RSAC against the surveyed related work. Finally, we end by summarizing the main aspects of RSAC.

In RSAC we can encrypt the two files and can send over internet to receiver. In that case also it find the digest number separately for both encrypted files and append with

them and also send with receiver's mail-id. At receiver side perform decryption process using public key append with emailed and after that find digest number for both files. It must be equal as forreceived.

REFERENCES

[1] The mathematics of the RSA public key cryptosystem. Website. http://www. Mathaware.org/mam/Cryptography.
[2] DI Management Home >Cryptography >RSA> RSATheory
[3] High-Speed RSA Implementation. C_ etin Kaya Ko_c/ RSA Laboratories.
[4] www.cacr.uwaterloo.ca/hac
[5] Arms dealers got Navy plans and deployment details. Website. http://www. indianexpress.com/story/8028.html.
[6] Cryptographic signatures on kernel modules.Website.http://lwn.net/ Articles/92617/.
[7] dm-crypt:a device-mapper crypto target for Linux. Website. http://www.saout.de/misc/dm-crypt/.
[8] EncFS: Virtual Encrypted Filesystem for Linux. Website. http://encfs.sourceforge.net/.
[9] Clemens Fruhwirth. New Methods in Hard Disk Encryption. Website. http://clemens.endorphin.org/nmihde/nmihde-letter-os.pd

