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

A Self –Destructing Secure Messaging System Using Multi Key Management Scheme

Amrapali Holkar
Pallavi Powar
Pooja Mhaske
Shiveta Tak
Computers,M.E.S. College Of Engineering ,Pune,Maharashtra,India

Abstract

We propose the Pandora Messaging, an enhanced secure instant messaging architecture which is equipped with a self-message-destructing feature for sensitive personal information applications in a mobile environment along with Multi Key Security Management using Shamirs algorithm. The proposed system will be beneficial for Government officers for communicating very sensitive and confidential messages. We design the Pandora Message Encryption and Exchange Scheme and the format of a self-destructible message to show how to exchange these messages atop the existing instant messaging service architecture. The Pandora Messaging-based system enables senders to set time, frequency, and location constraints. These conditions determine when the transmitted messages should be destructed and thus become unreadable for receivers. The Pandora Messaging-based system securely sends self destructible messages to receivers in a way that it uses ephemeral keys to encrypt the messages and transmits the encrypted messages to the designated receiver's instant messaging service in real time. When the transmitted messages‟ constraints are satisfied, the ephemeral key used for encryption will be deleted .Thus, the encrypted messages become unrecoverable. The most important part is that the Key are managed by the system. The system generates a pool of key and any group of the same pool can be used to encrypt and decrypt the message.

Keywords: Pandora ,Shamirs key, AAA, LFSR

Introduction

The popularity of instant messaging has grown in an exponential way. However, most popular instant messaging services often trade speed for security. Thus, the users are Subjected to constant eavesdropping, unwanted leakage of confidential information, and even compromises of users‟ media used in instant messaging. There are several secure instant messaging services for personal or enterprise use. The server may contain the unencrypted messages for administrative purposes. Thus, the user cannot guarantee the confidentiality of the message delivered. The unwanted consequence of leaving unencrypted messages on servers may cause leakage of personal information, or even identity theft. For example, the commercial instant messaging providers may choose to mine these plaintext messages for target advertisements. To solve the aforementioned issues we presented a secure instant messaging protocol preserving confidentiality against administrator. A limitation of their protocol is that it needs to modify the instant messaging server

to satisfy the protocol requirements. In addition to encrypting the messages for confidentiality, there are some systems with a "self-data-destructing" feature. These systems focus on making data disappear after a pre specified time. In other words, data is encrypted and the encryption key is deleted after the expiration time, so that the encrypted data becomes unrecoverable, i.e., self-destructed. To our knowledge, the concept of "self-destructing" data was first mentioned by Boneh and Lipton in a revocable backup system. Then some systems such as Ephemerizer, Vanish and Porter Devices were proposed. However, none of them integrate this concept with the instant messaging service using mobile devices and take account of their limitation. We present a secure instant message encryption and exchange scheme, which can be used directly atop an existing instant messaging service architecture, so that it is easily deployable, leveraging the existing infrastructure. Specifically, we add a self-message-destructing feature to get the enhanced secure instant messaging architecture, named Pandora Messaging. Project is not only limited to Pandora system but it has many other features for securing the message. The most importantly is the steganography part. We present concealment of information using steganography. Our aim is to have an application less vulnerable to steganalysis and create a user friendly steganography application. Steganography is a technique of communicating between sender and a receiver over a communication channel by hiding the relevant information in the cover media so that avoiding the information to be exposed to an intruder.

A possible carrier of secret information is applied to media such as images. The process of detecting steganographic messages is known as steganalysis and a particular steganalysis technique is called an attack. Steganalysis can be viewed as a two-stage process:

1) Classification of an image as being stego-bearing or not, and

2) Finding the location of stego-bearing pixels (i.e. the pixels containing the hidden message bits) with an aim to extracting, manipulating or sterilizing the message Steganography makes the job of the attacker more difficult because the very existence of the asset is hidden.

The importance of steganography in maintaining confidentiality can be illustrated with a simple example. Imagine two coworkers, A and B, are communicating with each other over the internet. A is sending confidential information to B, such as specifications for their company's latest project, and then A probably does not want adversary (E) to be able to read these messages and so, A will likely encrypt his message. The problem arises because the encrypted text is likely garbled, nonsensical data. Thus, E cannot read the encrypted messages, however, he will be aware that hidden message has been communicated between A and B. E can then take the encrypted message and attempt to crack it. This is a very real problem because as computational power increases, encryption is becoming easier to break. However, if A uses steganography, and hides his secret message in a generic image file, then A can transmit his secret message to B without evoking E"s suspicion. E will think A is just sending harmless picture to B, so E will ignore that communication between A and B. Thus, A and B defeat E. As mentioned in the example, attackers have more computing power now than ever before. DES, an encryption standard that was used by many national governments, however, mentions a cryptanalytic attack that can break DES in only a few minutes. Another example of a broken encryption algorithm isWEP, designed to provide confidentiality to users on wireless networks. Illustrates how WEP can be broken within hours. Steganography applications that hide data in images generally use a variation of least significant bit (LSB) embedding. Here images play a leading role in carrying confidential information because they can be modified to some degree if the corresponding steganographic media cannot be recognized as different from the carriers. In LSB embedding in the image, changing the LSB will only change the integer value of the byte by one. This small change is not noticeable. The visual appearance of a color and hence the image itself is not changed. A

proportionally greater change in the visual appearance of a color could be achieved by making up the RGB value of the pixel. This should have very little effect on the appearance of the image. In our application we are not only hiding the user's data within an image, but it also encrypts the user's data using the AES Cryptosystem.

Lastly the system is configured to deliver messages at a specific location based on Latitude and Longitude. The recipients of the message need to be in their destined location to view the message. The user can login but cannot view the messages if the location criteria do not matches with configured location in the message header. All the messages that do not match with predefined criteria which are set by the sender then the messages are displayed as lock to recipients. Only on matching the desired criteria the recipients can unlock the messages.

Enhanced Messaging System

A. Cryptography on Message

Cryptography is a process of sending a message securely. It is a technique for secure communication of protecting information by transforming it into an unreadable format.

For cryptography we are using Shamir's Secret Sharing [1]algorithm in which the secret is divided into parts, giving each participant its own unique part, where some of or all the parts are needed in order to reconstruct the secret.

B. Steganography on encrypted data

Steganography deals with hiding of data in images and steganalysis reveals the presence of data.

By using LFSR[2] steganography technique, we compute the suitability measure of the various random sequences of cipher bits against the given image.

C. Location based Authentication

Today's information systems require explicit identification between communicating entities (often entities are users). Process of entity identification is in general called authentication. The authentication is defined as affirmation of the identity of certain object in centralized systems, as refers [3]. More generally, authentication can be referred as message origin validation. Authentication is one of the three main processes of AAA systems (Authentication Authorization Accounting) [2]. Generic AAA system is in Figure 1.

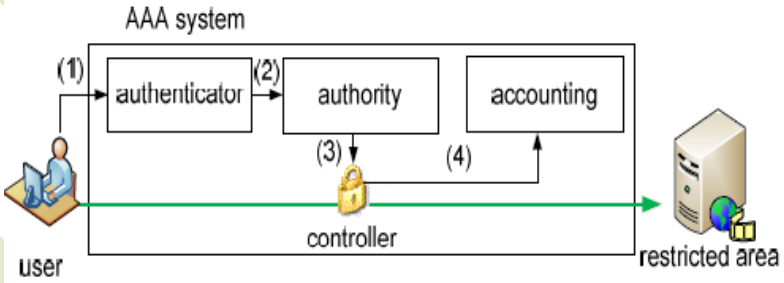

Figure 1. Generic system AAA

When a user wants to get access to the restricted area, he has to be authenticated by authenticator (1). It depends on user's identity authority whether grant or not the access to the restricted area (2). If the access is granted, controller establishes connection between the user and the restricted

area (3). Accounting records information related to user's actions (4) is created. Authentication techniques are commonly classified into three main groups as [3]:

- User has something – techniques using RFID (Radio Frequency Identification Device), hardware keys, etc.;
- User knows something – this group is based on knowledge of confidential information, for example password authentication;
- User is someone – biometric techniques that are limited to a human authentication.

Nowadays, many papers discuss using of user's location as a new factor of authentication. Location-based authentication can be useful in many cases. The advantages of location-based authentication present. The first place of usage can be found in the hospital sector. A doctor shouldn't handle with patients' privacy information out of hospital's border.

ALGORITHMS

In this section, algorithms for different processes of text and image based steganography used both in the sender side and receiver side are discussed.

- Shamirs Algorithm is used for data encryption and decryption
- Location and time constraints are applied.
- For Steganography ,LFSR is used.

Following Flow chart shows the basic flow for proposed Model:

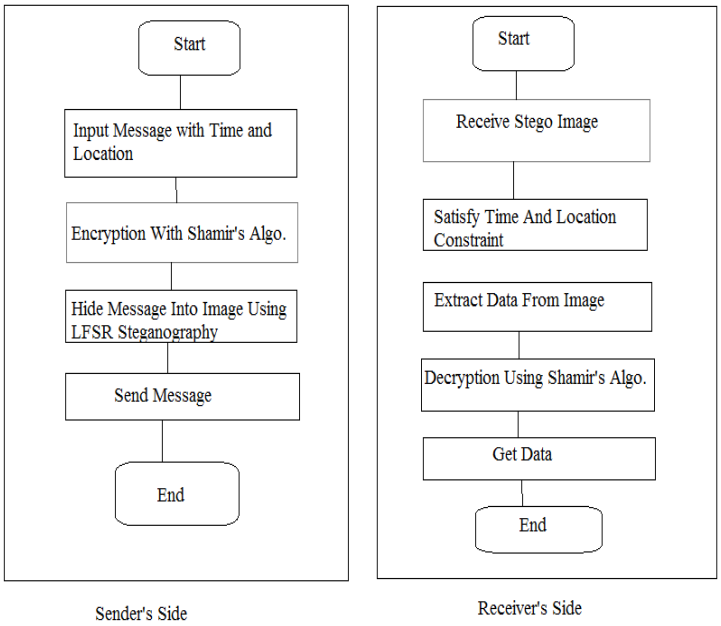

Figure2:ProposedAlgorithm for Steganographic model

A. Shamir Secret sharing

In cryptography, secret sharing refers to a method for distributing a secret amongst a group of participant search of which is allocated a share of the secret.
The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.

- Goal is to divide some data D (e.g., the safe combination) into n pieces D1,D2….Dn in such a way that:
- Knowledge of any k or more D pieces makes D easily computable.
- Knowledge of any k -1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).
- This scheme is called (k,n) threshold scheme. If k=n then all participants are required together to reconstruct the secret.

B. Data Hiding Algorithm

The difference between our application and the other programs implementation on LSB embedding is that our application ranks the seeds based on their suitability as cover images for our data. In our scheme we are using L.F.S.R's to generate random permutations of binary string. Details about L.F.S.R can be seen in [11]. In this, any random number generator can be used to permute the string instead of L.F.S.R's but information of the generator should also be communicated along with message. Inthe application the user first specifies the data that they would like to hide is in any file format, and encrypts this data using the recipient's El Gamal public key. Once the encrypted data is obtained, follow the below procedure.

Procedure:

1) a) Determine the length of the encrypted data (n).
b) Choose a cover image where it has more pixel than 'n+ p', where 'n' is the length of the encrypted data and 'p' is the length needed to embed the encrypted information of L.F.S.R string, and its initial seed value.
2) Calculate L.F.S.R (Linear Feedback Shift Register) bit length (m) such that 2 m > n.
3) Construct an m-bit length L.F.S.R, and represent the same in binary notation (one indicates bit location is tabbed and zero indicates otherwise)
4) Set the initial value randomly for m-bit L.F.S.R, referred as a seed.
5) a) Using this (L.F.S.R, seed) generates random permutation of f1, 2,....n as fl1, l2,... .
b) Permute the encrypted data using the permutation obtained above, to obtain a permutation string.
6) Test for suitability of this permuted string to be hidden into the cover image.
7) Each bit of permuted encrypted data is embedded in to the least significant bit of the pixel bytes of the cover image for which the suitability is above the threshold. If suitability is below the some fixed threshold, repeat from step 2 to 6.
8) Encrypt the L.F.S.R information that produced the above permutation and embedded this in last 'p' pixels of the coverimage.0

System Architecture

The project mainly works on Pandora, Steganography and Location based Message Delivery. We use the term Pandora means a self destructing Message communication.

In this section, we discuss Pandora Messaging, an enhanced secure instant messaging architecture with a self message destructing feature. The Pandora Messaging-based system is for handling the sensitive data encryption and transmission problems in an insecure mobile environment, and making sure the encrypted data is unrecoverable for any one once the destructible message's constraints are satisfied. Its components include: sender, receiver, Instant Messaging Server, and an optional Ephemeral Public Key Manager which is used by the receiver to delegate their ephemeral public keys.

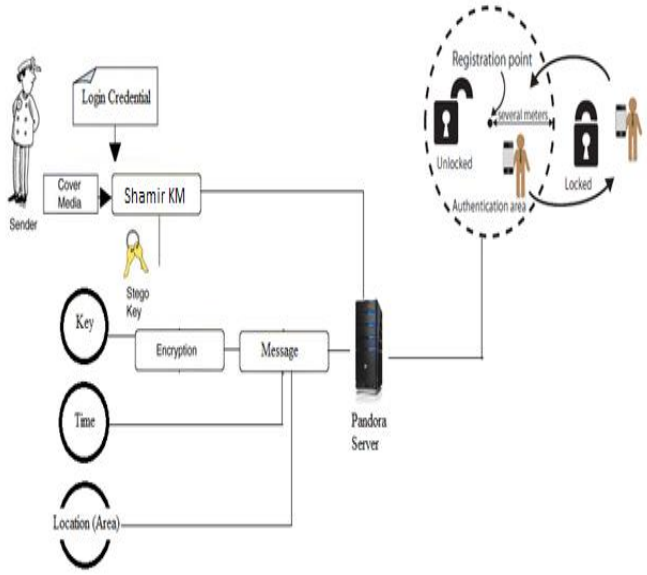

Figure3:System Architecture

The project mainly works on Pandora, Steganography and Location based Message Delivery. We use the term Pandora means a self destructing Message communication.
In this section, we discuss Pandora Messaging, an enhanced secure instant messaging architecture with a self message destructing feature. The Pandora Messaging-based system is for handling the sensitive data encryption and transmission problems in an insecure mobile environment, and making sure the encrypted data is unrecoverable for any one once the destructible message's constraints are satisfied. Its components include: sender, receiver, Instant Messaging Server, and an optional Ephemeral Public Key Manager which is used by the receiver to delegate their ephemeral public keys. We give below the details of each component.

A. Sender
The sender acts as an instant messaging client. When a sender would like to send a receiver the message containing sensitive personal information, the Pandora Messaging based application installed in sender's mobile device must be able to do the following tasks:
(1) generate a long-term public and private key pair;

(2) obtain an ephemeral public key from the receiver via an instant messaging service (IMS) and assign the constraint governing the condition to delete this ephemeral key; (3) generate the encrypted message using this ephemeral public key;
(4) send the destructible encrypted message, including the cipher text encrypted with a secret session key, the related encryption information encrypted with this ephemeral public key, and this ephemeral public key's identifier, to the receiver via an IMS;
(5) provide the ephemeral public key when requested by the receiver via an IMS.

B. Receiver
The receiver also acts as an instant messaging client. To receive the destructible messages, the Pandora Messaging based application installed in receiver's mobile device must be able to do the following tasks:
(1) Generate a long-term public and private key pair;
(2) Generate a series of ephemeral key pairs;
(3) Receive the destructible encrypted message from the sender via an instant messaging service (IMS);
(4) Decrypt the destructible encrypted message;
(5) provide the ephemeral public key when requested by the sender via an IMS;
(6) Show the sensitive personal information plaintext on screen after decryption without storing the plaintext in stable storage;
(7) Securely delete the ephemeral private key (i.e., overwrite it with random data) when the destructible encrypted message's constraints are satisfied.

C. Instant Messaging Server
An instance messaging server is a communication server which includes the basic features such as the authentication of the user accounts, the management of the user's presence status, and the instant message transmission between users. It may also support the enhanced features, such as the encryptions of the authentication process and the transmission channel, to protect the authentication information and the confidentiality of messages respectively.

D. Ephemeral Public Key Manager Ephemeral Public Key
Manager is an instance messaging agent which runs on a serves to keep itself available for senders and receivers, and supports ephemeral public keys management. It is needed if we intend to support off-line messaging that allows a sender to send the messages to an off-line receiver. Receivers can delegate their ephemeral public keys to the Ephemeral Public Key Manager's database prior to getting off-line, so that senders can still get the required ephemeral keys from the Ephemeral Public Key Manager, rather than awaiting receivers to become on-line later. The key manager is an important role to support the message push and synchronization technologies among mobile devices connected in the system because mobile devices are not always online.

Conclusion

This paper proposes an algorithm for data privacy. Data privacy has become increasingly important in the Cloud environment. We have used randomization of cipher bits for secured image steganography which is different than the existing steganography methods..Also, new approach for protecting data privacy from attackers who retroactively obtain, through legal or other means, a user's stored data and private decryption keys.

ACKNOWLEDGMENT

It gives us great pleasure and satisfaction in presenting this paper on "A Self-Destructing Secure Messaging System Using Multi Key Management Scheme"
We take this opportunity to express our profound gratitude and deep regards to our guide for her exemplary guidance , monitoring and constant encouragement throughout the course of this thesis .The blessing, help and guidance given by her time to time shall carry us a long way in the journey of life on which we are about to embark.
We are obliged to staff members of our college for the valuable information provided by them in their respective fields.

REFERENCES

[1] Tsai-Yeh Tung, Laurent Lin, D.T.Lee"Pandora Messaging: *An Enhanced Self-Message-Destructing Secure Instant Messaging Architecture for Mobile Devices" in 26th International Conference on Advanced Information Networking and Applications Workshops*

[2]Subba RaoY.V,Brahmananda Rao S.S,Rukma Rekha"*Secure Image Steganography based on Randomized Sequence of Cipher Bits" in 2011 Eighth International Conference on Information Technology: New Generations*

[3]David Jaros, Radek Kuchta, *"Location-Based Authentication and Authorization Using Smart Phones " in Trust, Security and Privacy in Computing and Communications (TrustCom), JUNE2012 IEEE 11th International Of Conference*