International Journal of Machine Intelligence, ISSN: 0975–2927, Volume 1, Issue 2, 2009, pp- 30-33

MMSSEC Algorithm for securing MMS

Priyanka Sharma* and Mijal Mistry

*Institute of Science and Technology for Advanced Studies and Research (ISTAR), Vallabh Vidya Nagar , Gujarat. India, Ph: 99989 88902 (M), E-mail: pspriyanka@yahoo.com

Abstract- MMS is the popular technology that is being misused heavily in the present times. In this paper, we are suggested MMSSEC algorithm to prevent unauthorized users from viewing messages which are not meant for them. This algorithm uses encryption and decryption technique for securing communication.

Introduction

The Multimedia Messaging Service (MMS) can be seen as the 'best of the breed' of several messaging services such as the Short Message Service (SMS), the Enhanced Messaging Service (EMS) and the Internet mail. Since 2002, the first MMS wave offers basic messaging features to mobile users and a second MMS wave is already appearing. This second wave builds up from basic messaging functions to offer more sophisticated features, from photo messaging to video messaging. The roots of the MMS lie in the text-based SMS and the Internet electronic mail. Indeed, features already supported by these services have not been forgotten in MMS. MMS supports the management of reports (delivery and read reports), message classes and priorities and group sending. In addition, MMS differs from other messaging services with its multimedia capabilities, its support for email and phone number addressing modes, its efficient transport mechanism and flexible charging framework.

MMS architecture

The MMS client is the software application shipped with the mobile handset, which allows the composition, viewing, sending, retrieval of multimedia messages and the management of reports. For the exchange of a multimedia message, the MMS client that generates and sends it is known as the *originator MMS client*, whereas the MMS client that receives the multimedia message is known as the *recipient MMS client*. The MMS Environment (MMSE) refers to the set of MMS elements, under the control of a single administration (MMS provider), in charge of providing the service to MMS subscribers. Recipient and originator MMS clients are attached respectively to the recipient and originator MMSEs. A key element in the MMS architecture is the MMS Centre (MMSC). The MMSC is composed of an MMS relay and an MMS server. The relay is responsible for routing messages not only within the MMSE but also outside the MMSE, whereas the server is in charge of storing messages [1].

MMS Interfaces*:* In an MMSE, network elements communicate via a set of interfaces. Each interface supports a number of transactions such as message submission, message retrieval and message forwarding. Each operation is associated with a set of protocol data units with corresponding parameters.

MMS Client*:* The MMS client is the software application that resides in MMS-enabled mobile devices and which offers the following features:

a. Management of message, notification and reports: Devices are commonly shipped with a unified message box for the management of MMS elements (messages, notifications and reports) and other elements such as SMS/EMS messages, WAP push messages, and so on.
b. Message composition: The message composer is used for creating new multimedia messages.
c. Message viewing: The message viewer is used to render received messages or to preview newly created messages before sending.
d. Configuration of MMS preferences and connectivity parameters.
e. Handling of a remote message box stored in the user personal network-based storage space. Such storage space is known as a Multimedia Message Box (MMBox). The support of an MMBox is optional.
f. MMS Centre: The MMS Centre (MMSC) is a key element in the MMS architecture. The MMSC is responsible for handling transactions from MMS phones and transactions from other messaging systems (e.g. other MMS systems, email systems, etc.). The server is also in charge of temporarily storing messages that are awaiting retrieval from recipient MMS clients. Optionally, the server may also support a persistent message store where users can store messages persistently in their MMBoxes. This feature is particularly useful when devices have limited storage capabilities.

Working Of MMS through MULIPART

In the MMS Environment (MMSE), a multimedia message can take multiple forms in order to be efficiently conveyed over the various transport bearers composing the full message transfer path. The link between an MMS client and the

MMS Centre (MMSC) is often bandwidth-limited (particularly over the radio part); therefore, multimedia messages are binary-encoded for efficient transfer over this link. Alternatively, the multimedia message is text-encoded for transfers over Internet protocols between MMSCs, from an MMSC towards the Internet domain or from/to Value Added Service (VAS) servers. Contents of a multimedia message range from simple text to sophisticated media objects with optional inter media synchronization. Multimedia message objects are wrapped into an *envelope*, which allows various network elements to route the message towards the recipients (addresses of primary and secondary recipients) and which characterize the message contents (class, priority, subject, etc.) [8].

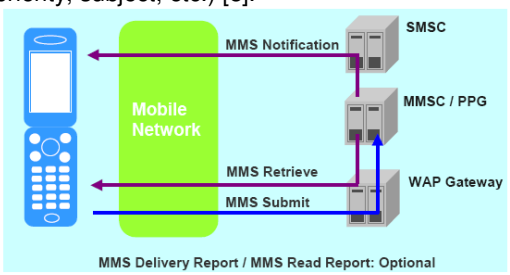


Figure 1: Framework of MMS

Message Envelope*:* A multimedia message consists of an envelope (also known as message header) and message contents (encapsulated in message body parts).The envelope informs about the following message characteristics: Address of the message originator (From)

- Address of the message recipient(s), organized into primary recipients and secondary recipients (To, Cc and Bcc)
- Priority of the message (low, medium or high).
- Class of the message (auto, auto, personal, informational or advertisement)
- Date and time when the message was sent
- Validity period
- Reply charging parameters
- Request for delivery and/or read reports
- Message subject
- Sender visibility
- Earliest delivery time
- Message distribution indicator
- MMSBox status.

Multiple parts of a message are separated by boundary delimiters. The name of a boundary delimiter is assigned to the subtype parameter called boundary. The name of a boundary delimiter has a size ranging from 1 to 70 characters. With a multipart textual representation, each part begins with two hyphens (- -) followed by the boundary delimiter name. The multipart message is terminated by a carriage return/line feed followed by two hyphens, the boundary delimiter name and two additional hyphens. *Media Types:* MMS devices may support one or more media types (still image, video, speech, etc.). And for each supported media type, the MMS device supports at least one media format/codec (e.g. AMR for speech, H.263 for video, GIF and WBMP for bitmap images, etc.). It supports: Text, Bitmap and Still Images, Vector Graphics, Speech, Audio and Synthetic Audio, Video, Personal Information Manager Objects.

MMS transaction model

MMS entities (MMS clients or MMS centers) communicate by invoking transactions over a set of eight interfaces. A transaction is typically composed of a service *request* and a corresponding service *response/confirmation* containing the transaction results (e.g. message sending request and message sending confirmation). However, several transactions are limited to a service request only and are also known as *indications*. A Protocol Data Unit (PDU) is associated with each service request or response that can occur over one of the MMS interfaces. A PDU is composed of a set of mandatory, optional or conditional parameters.

Implementation of Proposed MMSSEC Algorithm

Nowadays many immoral MMS are spreading all over. Even without the knowledge of user these MMS intend to come on their mobile and if the cell is in the hand of unauthorized person it could be a problem. Here we have proposed MMSSEC Algorithm for securing MMS. Suppose someone sends to message to other user then it will ask for the credentials and once verified the credentials then it will allow sending the MMS and same techniques is used at receiver end. At the receiver end it will display a message that a new message has been arrived and also state that the message is for manager, assistant manager, operator etc. If the person is trying to open the message then it will ask the credentials and once provided the correct credentials it will allow to view the message. Now for encryption we must have two keys - a public key and a private key. The public key will be decided by the network provider by your phone number and the private key is decided by the user, but he must intimate the network operator about any change in that. We are suggesting three types of users for cell phones – Administrative (for the owner), Limited Users each having their unique private keys. These profiles will be predefined such as Administrator has full permissions. The steps to be carried out in this algorithm are as follow:

Algorithm MMSSECURE

STEP 1: While sending the MMS the user need to pass the credentials along with the message

so that the service provider will check whether the person is authorized to send the message.

STEP 2: If he/she is authorized, then he/she will send MMS to selected users

STEP 3: The designated user will receive a message stating the new MMS

STEP 4: For viewing purpose password is needed so that it can be opened by the designated user for which the message belongs.

STEP 5: For that UTF technique is used along with the private key for checking it is authorized person to view the message.

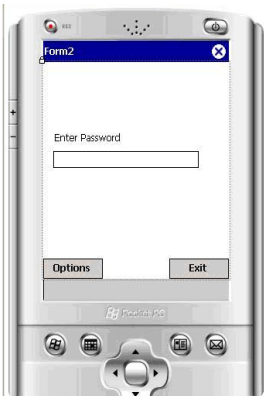
STEP 6: After successfully checking credentials it will allow user to read the message.

STEP 7: If the credentials does not match then it won't allow user to read the message.

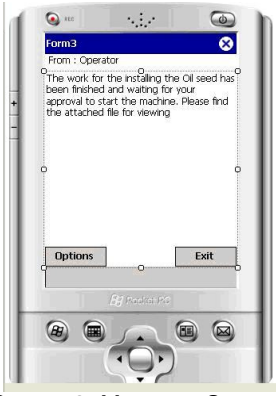
In the SMIL header, the public key should also be included. Now when an MMS reaches MMSC, it intimates the user that a MMS has arrived. Now if a user is willing to see the MMS, he goes to download or view option. While doing so, a push message is automatically send to the network operator about the current profile of the cell phone. Actually only the private key of the current profile will be send. By this the network operator will get to know the current profile of the cell phone and it checks whether the current profile is authorized to view the MMS or not and then the required action is taken. Same method is for sending the MMS. While sending, along with MMS the information about current profile is to be send via push message and then the action is taken by the network operator. Assume a simple addition example:
Suppose public key is 10101010
And the private keys are:
For Eg.
Manager: 01010101
Assistant Manager: 1 2 1 2 1 2 12
Now the network operator will only keep the public key and the sum of the public key and the private key i.e
Manager: 11111111
Assistant Maanger: 2 2 2 2 2 2 22

When a push message is send to the network operator he will just add the incoming private key with the user's public key and check for the account. Suppose the current profile is of guest, then the network operator will get 23232323. After adding will public key (10101010+23232323), he gets 33333333. So he now knows that guest is trying to view or send an MMS. So the action taken will be permission denied in this way the problem can be reduced much but not fully as the main culprit is not the technology but in the mind of people who are responsible for such acts. The same algorithm was developed using software .Net of which screen shots are shown as below:

Screen 1: Message Received Screen



Screen 2: Password Screen



Screen 3: Message Content

The software was tested on mobile and it works well by preventing authorized viewings. Here we have tested model for authorized and unauthorized users of a company. In his company authority chain is like manager, assistant management, senior officer, officer operator and technicians. It has various branches all over India. Now, if manager wants to send some mms having confidential designs,

drawings, etc than this algorithm MMSSEC filters users and only valid users can view MMS.

Conclusion: Algorithm MMSSEC secures MMS so that only valid user can view/send MMS so that confidential information is not misused.

References

[1] Gwenael Le Bodic (2003) *Multimedia Messaging Services – engineering approach to MMS: Wiley Publications*
[2] Scott C. Guthery, Mary J Cronin (2000) *Developing MMS Applications: Multimedia Messaging McGraw-Hill Professional*
[3] www.eu.anritsu.com
[4] www.hsenag.info.com
[5] www.forums.wirelessadvisor.com
[6] www.research.ibm.com
[7] www.practicallynetworked.com/support/wireless_secure.htm
[8] www.wikipedia.com
[9] www.general-wireless-discussion/58190-mms-security.html