# Extraction and Verification of Mobile Message Integrity

Rakesh Verma, Deepak Singh Tomar, Shashi Kant Rathore

*Computer Science and Engineering Department*

*Maulana Azad National Institute of Technology(MANIT) Bhopal[M.P.]*

rakeshmact@gmail.com

deepak.tomar@manit.ac.in

shashi.mnit@gmail.com

***Abstract* - Crime investigation in mobile phone is an important source of data acquisition. Offenders tamper Mobile phone technology is increasing rapidly. Now companies are expanding their horizon through mobile message services, making it essential. On other hand tight physical and border security may encourage criminals to use mobile SMS to communicate suspicious data. Message contents to effect message integrity. In this work common mobile phone attacks, SMS encoding and decoding techniques are presented. A prototype system is also implemented to verify the message integrity.**

***Keywords*- Mobile Phone Attacks, SMS Technology, SMS Encoding and Decoding**

## I. INTRODUCTION

Mobile phones are common thing in today's world, used by many people for both personal and professional purposes. Mobile phones vary in size, design and are continually undergoing change as existing technologies improve and new technologies are introduced. These compact devices are useful in managing information, such as contact details and appointments, and other information but at the same time, they are also becoming more creditable of attention as a new tool of crime, such as the use of mobile phones in the fraud, selling fake products, spreading rumors, and other illegal and criminal activities. Therefore, the judicial authorities need to invent mobile forensic. Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted approaches. Mobile Forensic process consists in several steps.

### *A. Data Acquisition*

Data Acquisition deals with extraction or collection of evidence from mobile phones. Evidence extracted from different sources of mobile phones.

### *B. Data Preservation*

Evidence are preserved using different cryptographic technique and hash function like MD5 and SHA-1 in secured manner.

### *C. Data Normalization*

Normalization offer convert different type of data formats into standard data format to maximize the usability of forensic tools. The normalizing process depends upon the nature of the data. Data files that contain timestamps must represent time in the same way. Similarly, files that contain machine names or IP address must use the same representation for all data [1].

### *D. Running Analysis*

Preserved and normalized data putted into forensic tools for analysis of evidence in investigation process.

## II. MOBILE PHONES ATTACK

Today mobile phones becoming tool for attackers to target the individuals or organization to impact financial loss or make unavailability of service.

### *A. Denial of service (DoS)*

Denial of service (DoS) attack is a malicious attempt by unauthorized users or attackers to bind or denies the communications and availability of other services. DoS attacks target a user or an entire organization and can affect the availability of target phones or the entire network. DoS offer an attacker sending large amounts of legitimate requests to targeted mobile phones to disruption of normal communications. DoS attack can be classified in different way.

#### *1). Bandwidth Consumption*

Attackers send large amount of data to consume available bandwidth of network. This can be achieved in two ways one is attacker has high speed network connection than the victim. Second is attacker magnifying their attack by engaging many websites to flood the victim's network

#### *2). Resource Starvation*

This kind of attack consumes a resource needed by the service. the target system is no longer able to operate normally and provide a service across the network. On entering a system the attacker will abuse their allocated quota of system resources to crash the machine. The target system may crash or be forced to reset due to the file system becoming full [2].

978-0-7695-4437-3/11 $26.00 © 2011 IEEE
DOI 10.1109/CSNT.2011.17

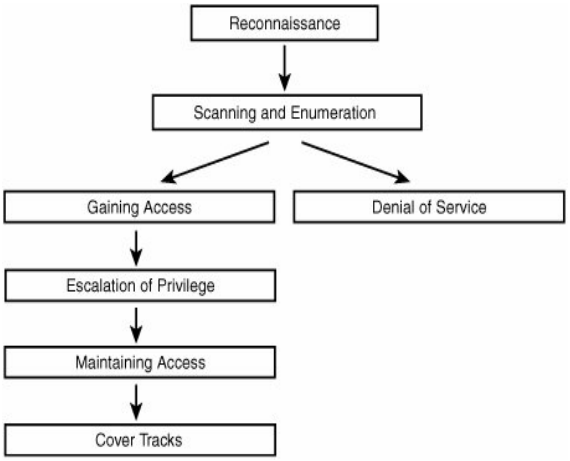


Fig. 1 Denial of Service Attack work-flow

*B. Phishing Attack*

Phishing attack is the act of steal personal identity data from cell phones, blackberries, and PDAs using many techniques. Bluetooth-enabled phones have serious security flaws that allow attackers to connect to the device without users' permission. The attacker can get access to the victims phone book database either stored on the phone or the SIM card[3]. In addition, the attacker can get access to the calendar, to-do list, and lists of missed and received calls. It is also possible to retrieve and send SMS messages from the victim's device or to initiate phone calls to any existing contact.

Blooover [4] is a proof-of-concept tool which runs on J2ME-enabled cell phones that exploits Bluebug. Bluebug is the name of a bluetooth security loophole on some bluetooth-enabled cell phones. It allows the attacker to not only initiate phone calls from the victim's device, but also eavesdrop on the victim calls when the victim passes by. Moreover, the attacker can read/write phone book entries, download call lists, set call forwarding, connect to the internet, and send/read SMS messages from the attacked phone. In consequence, The attacker can figure out the victim's phone number by sending himself an SMS message from the victims device.

*C. Evasion Attack*

Evasion attack focus on attacking the forensics tools to make them crash or execute arbitrary code when performing an acquisition of a suspected SIM or phone memory. Attackers hide suspected messages by tampering message headers from acquisition tools or software during forensic investigations. Attackers tamper message header by changing of length fields, encoding decoding bits, bitmask header value and user data header field

## III. SMS TECHNOLOGY

Short Message Service (SMS) is a technology of service enables the sending and receiving text form messages between mobile phones. SMS first appears in Europe, 1992 which include in GSM (Global System for Mobile Communication) and it is used as a means for sending text messages from one mobile phones user to another [5]. SMS is the ability to send and receive text message to and from GSM mobile phones and it is based on a 'stored and forward' concept. Short messages sent by a customer are stored in the mobile phone operator's Short Message Service Center (SMSC) and subsequently delivered to the recipient's mobile phone if no errors occur during the delivery [6].In mobile phone forensic, SMS is play valuable role in evidence gathering because SMS contain lot of information about sender, SMSC and handset. Messages are increasing being used as evidence in investigation. Messages are available in several forms.

*A. EMS (Enhanced Messaging Services)*

Enhanced Messaging Service (EMS) is a logical evolution in both form and function from the basic SMS structure. EMS messages allow the mobile phone user to personalize and express themselves with styled text, pictures, ring-tones and more. Enhanced Messaging Service (EMS) was developed to rectify drawback of SMS. EMS is an application level extension of SMS. An EMS message can include pictures, animations and melodies

*B. MMS (Multimedia Messaging Services)*

MMS enables users to send text, color photographs, color graphics such as maps & logos, voice and music audio files, and even video. Unlimited messages size, with even the first devices supporting messages of over 30Kb per message. Uses the Multimedia Message Service center (MMSc) for message delivery Uses open standard that are widely supported by many mobile phones.

*C. SMS (Short Messaging Services)*

SMS is the service of send and receive simple text messages up to 160 characters between mobile phone users.

SMS can be send, receive and read from mobile phones in two modes.

SMS Text Format: Text mode of SMS contains simple group of characters, words or lines.

SMS PDU Format: PDU Mode of SMS contains sequence of alphanumeric strings that encrypted and encoded in different encoding methods. Two PDU formats use in SMS service [7].

SMS Submit

| Len | Type of number | SCA | PDU Type | MR | len | Type of number | DA | PID | DSC | VP | UDL | UD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | |

SMS Deliver

| len | Type of number | SCA | PDU Type | Len | Type of number | DA | PID | DSC | SCTS | UDL | UD |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |

len: ”len” octet contains the number of octets required for the number of the Service Center .
Type of number: 81H: the following number is national
91H: the following number international
SCA: Service Center address
PDU Type: SMS Submit, SMS Deliver
MR(Message Reference): The MR field gives an integer (0..255) representation of a reference number of the SMS-SUBMIT submitted to the SMSC by the MS.
len: ”len” contains the number of BCD digits of OA or DA.
Type of number: 81H: the following number is national for OA or DA
91H: the following number international
SCTS: Service Center Time Stamp
OA/DA: Originated Address /Destination Address
PID: The PID is the information element by which the Transport Layer either refers to the higher layer protocol being used, or indicates inter working with a certain type of telematic device.
DCS: The DCS field indicates the data coding scheme of the UD (User Data) field, and may indicate a message class.
VP: The Validity-Period is the information element which gives an MS submitting an SMS-SUBMIT to the SMSC the possibility to include a specific time period value in the short message.
UDL: The UDL field gives an integer representation of the number of characters within the User Data field.
UD: The UD (User Data) field contain text message.

## IV. SMS ENCODING AND DECODING

SMS messages encoded and decoded using different encoding and decoding techniques [8].
GSM 7 bit
GSM 7 bit ASCII encoding technique encodes 160 characters length message. In this scheme we covert 8 bit message into 7 bit.
ASCII 8 bit
ASCII 8 bit scheme encode 140 character length messages into encoded user data string.
UCS-2 16 bit
This encoding technique encodes 70 character length messages. UCS-2 16 bit known as Unicode encoding scheme. The demerit of this encoding scheme is that it limits the message data to 70 characters.

### *A. SMS Decoding*

SMS decoding is reverse action of encoding that applied on message PDU string. SMS decoding decode encoded user data string of SMS PDU into original text message. In this paper we constraint GSM 7 bit [9] decoding scheme. Extract user data in hexadecimal octets and apply decoding scheme.
The need of decoding to convert extracted SMS PDU string into readable text form that gives information use in forensic investigation process. In this work, 7 bit GSM decoding method used. To decode extracted User Data string octets of PDU String.

**C82293F99C36A7**

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| C8 | 22 | 93 | F9 | 9C | 36 | A7 |
| 11001000 | 00100010 | 10010011 | 11111001 | 10011100 | 00110110 | 10100111 |

Perform reverse process of encoding. Here creating eight septets from seven octets. To do this seven most significant bits of octet seven and place them into eight septet as shown highlight.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 11001000 | 00100010 | 10010011 | 11111001 | 10011100 | 00110110 | XXXXXXX1 | 10100111 |

Now need to create septet number seven for this take six most significant bits of octet six and place them to least significant bit of septet number seven.

| 1 | 2 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|
| 11001000 | 00100010 | 11111001 | 10011100 | XXXXXX10 | 1001101 | 10100111 |

The five most significant bit of octet five goes to least significant bit of septet six and this process continue proceed until seven bit octets convert into eight bit septets.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 11001000 | 00100010 | 10010011 | 11111001 | XXXXX100 | 1010011 | 10011101 | 10100111 |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 11001000 | 00100010 | 10010011 | XXXX1001 | 1001111 | 1010011 | 1001101 | 10100111 |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 11001000 | 00100010 | XXX10011 | 10011100 | 1001111 | 1010011 | 1001101 | 10100111 |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 11001000 | XX100010 | 1001100 | 1001100 | 1001111 | 1010011 | 1001101 | 10100111 |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| X1001000 | 1000101 | 1001100 | 1001100 | 1001111 | 1010011 | 1001101 | 10100111 |

Now remain eight septets but need to eight octets to reconstruct original message. To reconstruct original message need to add least significant bit back on to each octet (which is zero). The result in highlight added bit.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 01001 000 | 01000 101 | 01001 100 | 01001 100 | 0100111 1 | 01010 011 | 01001 101 | 0101 0011 |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 01001 000 | 01000 101 | 01001 100 | 01001 100 | 0100111 1 | 01010 011 | 01001 101 | 010 100 11 |
| 48 | 45 | 4C | 4C | 4F | 53 | 4D | 53 |
| H | E | L | L | O | S | M | S |

To get the hex values and their equivalents ASCII and back at original messages strings.

The Decoded Message String

**HELLOSMS**

## V. Proposed Framework

In this work a methodology and prototype is proposed for SMS extraction and Integrity verification in mobile environment.

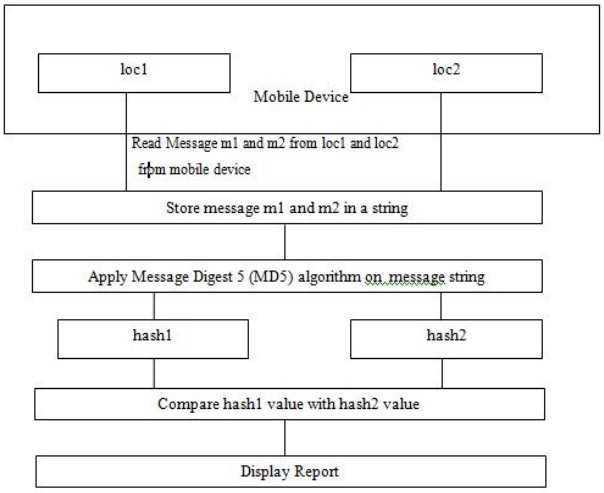


Fig. 2 Proposed Prototype

### *A. Proposed Methodology*

The proposed methodology works in different chronological steps.

1. Established connection between Mobile phone and Computer PC through Socket
2. Acquire the messages from different mobile location such as inbox, draft, sent and folder.
3. Store the message in the PC
4. Generate hash code of the message strings using MD5
5. Verify the integrity of the message ( Original/Redundant ).

## VI. Implementation and Results

In this work a system is implemented to acquire the message from mobile and verify integrity of mobile message contents stored at different location. The experimental setup is created using One PC and Nokia Mobile 5230 series. To Bluetooth connection is established between mobile phone and PC using script. The proposed prototype is implemented in java and python technology.

### *A. Results of SMS Extraction and Verification*

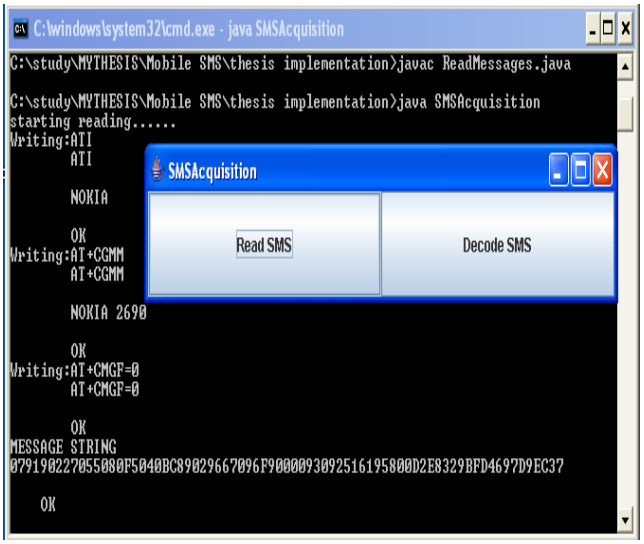


Fig. 3 SMS PDU String Extraction

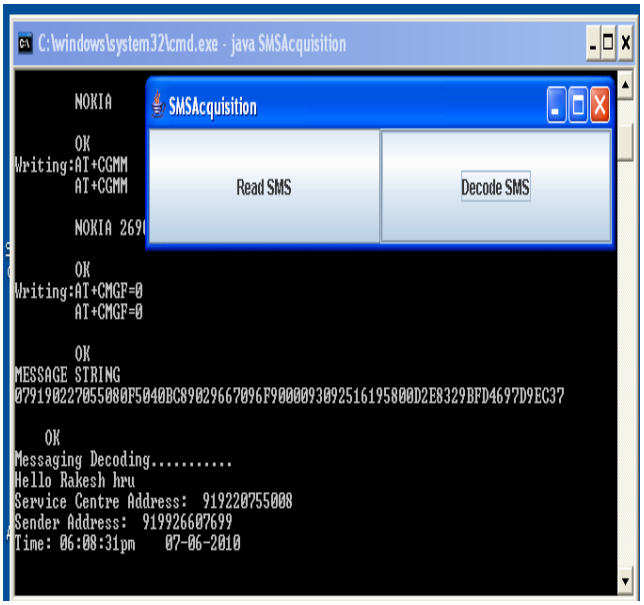


Fig. 4 SMS Decoding

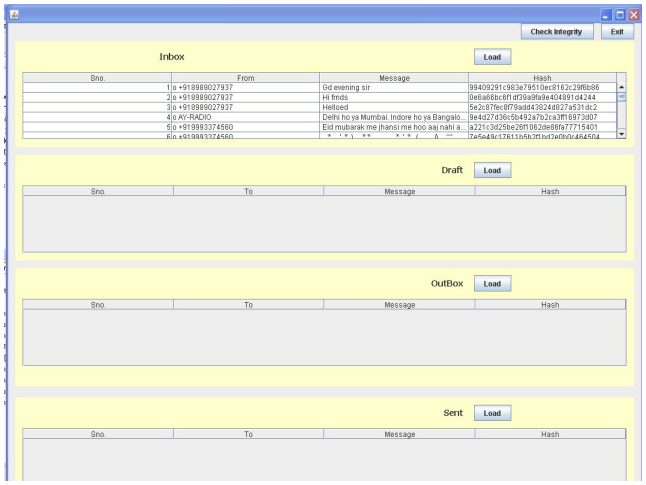


Fig. 5 Read Inbox Message Window

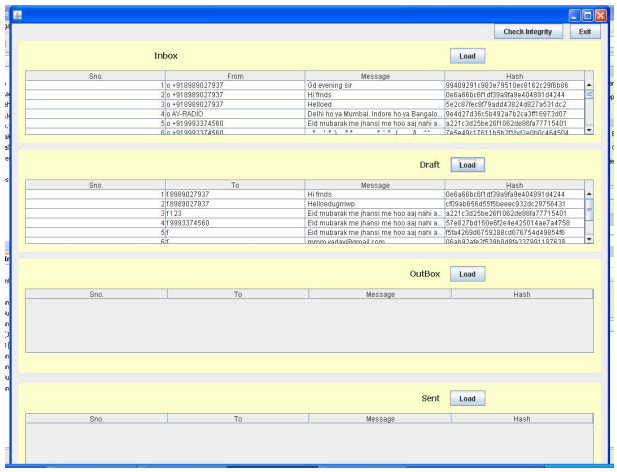


Fig. 6 Read Draft Message Window

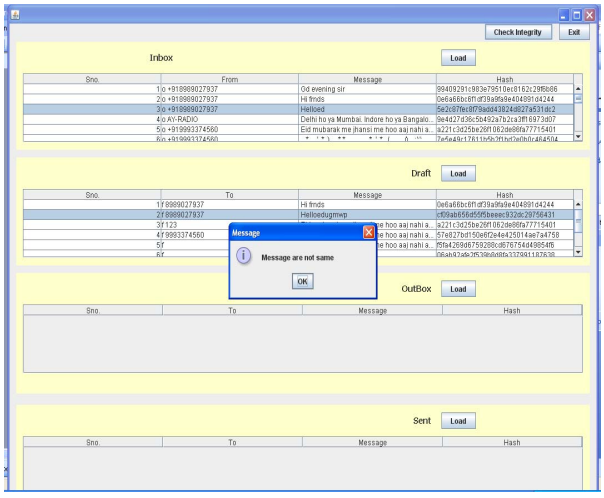


Fig. 7 Check Message Integrity for Altered Message

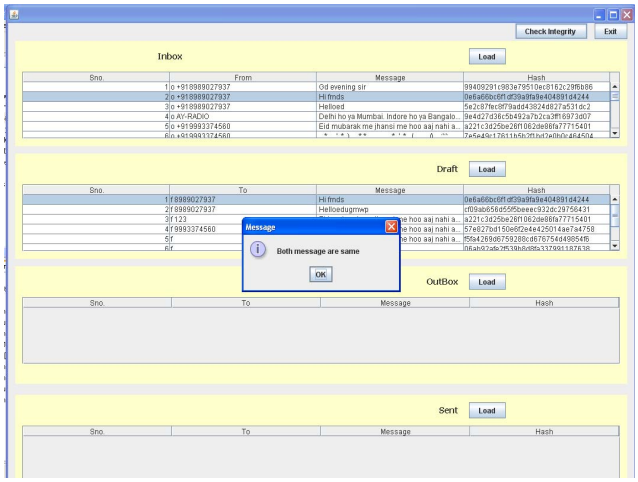


Fig. 8 Check Message Integrity for Unaltered Message

## VII. CONCLUSION

Message tampering is a one of serious threats in the mobile environment. Attackers can easily tamper a SMS and use it for conducting illegal activity which may affect individuals or organization. Digital evidence subjected to mobile may be easily modified either knowingly or accidentally. In this work a method is proposed and implemented for SMS acquisition and integrity verification. A successful verification of the SMS integrity check increases the confidence and trust in to end user. The proposed approach also help full for law enforcement agency which are evolved in the mobile crime investigation.

## REFERENCES

[1] "Frank Adelstein, "MFP: The Mobile Forensic Platform", Senior Principal Scientist, ATC-NY

[2] Matthew Hutchinson, "Study of Denial of Service", Queen's University of Belfast, Aug-2003

[3] Saeed Abu-Nimeh and Suku Nair, "Phishing Attacks in a Mobile Environment", SMU HACNet Lab Southern Methodist University Dallas, TX

[4] Saeed Abu-Nimeh and Suku Nair, "Phishing Attacks in a Mobile Environment", SMU HACNet Lab Southern Methodist University Dallas, TX

[5]http://www.developershome.com/sms/howToSendSMSFromC.asp.

[6] Low Hon Chuen, "Study of an Alert Device for Elderly to Detect Fall Motion", TZS402 CAPSTONE PROJECT 2007.

[7]http://www.gsmfavorites.com/documents/sms/packetform at

[8]http://developer.symbian.org/main/documentation/reference/s3/pdk/GUIDDF114F594DC95C77B7F9F1C93B8E71 4C.html

[9] Michael Harrington, "UNDERSTANDING SMS: Practitioner's Basics", CFCE, EnCE.

[10] http://www.forumnokia.com/AT Commands.