Falsifying SMS Messages

Thomas Marryat John Corcoran

Abstract - **Mobile telephone examiners are frequently asked to comment upon whether SMS messages presented in mobile telephone device reports have been modified or falsified. An additional examination of the mobile telephone is often required to confirm that the report provides an accurate representation of the mobile telephone's content; however, it may be asked if SMS messages have been falsified on the phone itself.**

An investigation was undertaken to establish whether it was possible to falsify SMS messages on a mobile telephone handset without access to privileged hardware or software. Using a commonly available flasher/service tool we were able to modify existing SMS messages on a Nokia 6021 handset including altering the sender's number and message content. Techniques for identifying falsified SMS messages were also investigated which can be pursued in the event suspicions are raised.

Index Terms - **Cell Phone Forensics, Mobile Phone Forensics, SMS, Text messages.**

I. Introduction

We have been asked on a number of occasions if the SMS messages presented as evidence could have been modified or falsified. This leads to three questions on the examiner's part: 1) has the software used in the examination generated an inaccurate report, 2) has the report been modified after the examination, 3) is it possible to modify/falsify the messages on the handset?

The first two questions can be both answered with an examination of the relevant exhibit and a comparison drawn between the report findings and the SMS messages present on the phone, assuming that the integrity of the data stored on the handset has been maintained.

The third question requires research into the capabilities and support for such processes. From performing HEX dump examinations of mobile telephone handsets and observing the capabilities of the software/hardware tools commonly used in these examinations, it was suspected these tools could be used to falsify SMS messages stored on a handset. A search was conducted to find supporting research to collaborate this idea. As our search found no supporting information, it was deemed necessary to conduct our own research to ascertain whether it was possible to falsify an SMS message on a handset this and the skills and tools that would be required.

II. Terminology

- *AT Commands* – a set of commands that, when sent to compatible devices, will instruct the device to return information relating to the command in question.
- *Commercial Off-The-Shelf (COTS)* - Software or Hardware available to the general public that has not been modified outside of its standard operating parameters.
- *Flasher/Service tools* – commercially available products, usually comprising of a bespoke combination of hardware and software, which allow the user to read/modify the otherwise inaccessible internal storage of compatible handsets. These devices are typically used for unlocking mobile telephones or upgrading their software.
- *HEX Dump* - A form of mobile telephone examination which can, depending on the handset, recover deleted and/or hidden system information.
- *Out of Bounds Testing* - Tests designed to evaluate the response of a system for inputs outside the expected range of values. For example, 11:21:63 being entered as a time value.
- *PM Tables* - A logical structure used to store user and system data in many Nokia mobile telephone handsets. The tables consist of keys and subkeys. Keys identify a category (such as SMS messages or SIM card information) and the subkeys store the related data (for example individual SMS messages, or the IMSI of the last used SIM card).
- *Within Bounds Testing* - Tests designed to evaluate the response of a system for inputs within its expected range of values. For example, 11:21:30 being entered as a time value.

III. Approach and Equipment

Commercial Off-The-Shelf (COTS) software and hardware were used for all aspects of the experiments to ensure that results would be replicable and achievable without considerable financial backing or privileged access to hardware or software.

A Nokia 6021 (Nokia Europe – Nokia 6021, n.d.) handset was used for all experimentation. This handset was chosen for a number of reasons. Firstly, in general Nokia handsets exhibit highly structured and standardised storage techniques using PM tables. It is, therefore, expected that our findings would be transferable to a large number of other models of Nokia mobile telephones. Secondly there is large support for Nokia handsets in COTS flasher/service tools. Finally, Nokia retains a large market share of the mobile telephone handset sales (Gartner Press Release, n.d., Table 1).

The flasher/service tool Sarasoft UFS/HWK (UFSxHWK, n.d.), also commonly known as "Tornado", was used for its extensive capabilities for Nokia handsets which reflect the advertised capabilities of other COTS flashing/service tools, including the Cyclone Box (CYCLONE-Box, n.d.) and the Advance Turbo Flasher (Advance Turbo Flasher by AdvanceTeam, n.d.) .

IV. Structure and storage of SMS messages on a Nokia 6021 handset

The Nokia 6021 was found to store received SMS messages in key 140 of the PM tables. The format of several received SMS messages was examined to identify the elements of interest. It was found that the Nokia 6021 handset did not store SMS messages in the format described in GSM 3.40 (Technical realization of the Short Message Service (SMS), 1998) but instead reordered the same elements and included its own parameters/fields. Appendix 1 provides an example received SMS message complete with annotation of known fields.

The Nokia 6021 handset appeared to store the index of the SMS message/part of SMS message at offset 6. This may extend to include offset 4 to allow more than 255 SMS messages to be indexed. Further testing would be required to confirm this.

The Nokia 6021 handset appeared to store two length parameters within the SMS entry. A parameter containing the SMS entry's length was found at offset 14 (perhaps also including the octet at offset 12). The value of this parameter was equal to the number of octets from offset 12 to the end of the entry. A second parameter containing the length of the encoded message structure was at a negative offset of 6 from the message content, and its value was equal to the number of octets from a negative offset of 8 from the message content to the end of the message entry.

The elements of the date and time stamps were stored in reversed decimal values (for example, the 1st of the month would be stored as "10") in the format YYMMDDhhmmssTZ as per the GSM specifications. The service centre number and sender's number similarly followed the GSM specification with the address length followed by type of address, such as International, National, Network specific number etc, and then the respective number.

The SMS message content was stored in PDU format and was preceded by length fields that included the User Data Length (number of characters in the user's message), the length of the encoded PDU content, and the previously discussed encoded message structure length. As required, each message was suffixed with 0x55 in order to reach a message length equal to a multiple of 4 octets. For example, a message with content "Abcdef" ("41F1985C3603" in PDU encoding) is represented as "41F1985C36035555" - this has been suffixed with 0x55 octets to make the whole message length equal to 8 octets.

Multipart SMS messages were stored as their individual parts across multiple subkeys. The date and time stamp displayed on the handset related to the last part of the SMS message.

V. Test and Results

Attempts to create new SMS messages were met with limited success, presumably due to the handset's reliance on index values that may not be stored within key 140 and its subkeys. As such, all subsequent experiments were performed by editing a previously stored SMS message.

It should be noted that early in the experimentation the handset failed to boot correctly after writing back an edited PM file. As a result, the phone was reflashed with firmware V5.22 and the tests were repeated on this new firmware.

All documented tests were produced using a UFS/HWK flasher/service box using DCTxBB5 version V2.0.8.0 and all editing of the PM tables was made using PSPad (editor PSPad, n.d.) version 4.5.3.

A. Within Bounds Testing

Tests were derived to ascertain how the Nokia 6021 handset reacted to modified inputs that were indicative of content that could be received through the mobile telephone network. These tests included modifying the service centre address, sender's address, date and time stamp and content of an existing message.

The service centre address and sender's address could be modified provided that the respective lengths were updated to reflect the new value. If the modified addresses were the same length as those they replaced then the length parameters did not require to be updated.

The date and time stamp could be modified to any valid date and time. The time zone sector of the time stamp could also be modified, although this change was only visible within the PDU encoded version retrievable via AT commands, as well as MicroSystemation's XRY extracted copy of the SMS.

The content of the SMS message could be modified provided that the User Data Length and the handset's own length field (at offset 8) were updated to reflect the new lengths of the data (including the previously discussed 0x55 padding). The content could be modified without updating the length parameters if the modified content length was equal to, or less than, the original message's length (for example, the content "I hate you" could be modified to "I love you" (both 10 characters in length) without updating the length parameters.

All modifications made to the service centre address, sender's address, date and time stamp (with the exception of time zone) and content were visible in the SMS message's further details submenu on the handset and did not provide any indication on the handset that they had been modified. With regards to electronic data extraction, MicroSystemation's XRY and Envisage Systems's Phonebase reported values of the modified fields that matched those presented on the 'further details' submenu, again with no indication that modification had occurred. XRY was also able to display the modified time zone in the form of an offset from GMT.

B. Out of Bounds Testing

Tests were derived to establish how the Nokia 6021 handset reacted to modification using data which was not valid if it was received over the mobile telephone network. Tests were performed to modify the date and time stamp of an existing message with data that was invalid. This was used to test if error correction or input validation was present in the handset.

The year field of the date and time stamp allowed an input of between 00 and 99. The handset displayed the year 2000 for an input of 00 and the year 1999 for the input of 99. No further testing was performed to establish which other inputs were prefixed with 19 (20th Century) and which were prefixed with 20 (21st Century).

Restricted fields that only permitted values between a certain range included the month field (01 to 12), the day field (01 to 31) and the hour field (00 to 23). Values outside these ranges resulted in the whole date and time screen being inaccessible on the handset's further details submenu (however the message content and other elements present on the further details submenu were still accessible).

It was observed that the permitted values for the day field (of 01 to 31) remained static regardless of the month. As such, invalid dates could be made to display on the handset. An example of this would include the 31st February.

Both valid (00 to 59) and invalid (60 to 99) values were permitted for the minutes and the seconds elements of the date and time stamp and were visible in the further details submenu. The handset would therefore be able to display a modified time value of 23:99:99.

For out-of-bounds data, the values reported by electronic extraction tools did not match those listed within the 'further details' submenu on the handset. As an example, an SMS message was modified to contain a date and time stamp equal to "31/02/90 13:99:99", which the handset reported under 'further details' as "31/02/2090 13:99:99". Using electronic extraction, MicroSystemation's XRY reported a date and time stamp of "31/02/1990 (UTC)" (no time is reported), while Envisage System's Phonebase reported a date and time stamp of "03/03/1990 14:40:39". AT commands can be used to extract the SMS in PDU format, which when decoded provided the "31/02/90 13:99:99" date and time stamp originally specified. It therefore appears likely that the electronic tools have different ways of interpreting the underlying data, which may not correspond with the values reported by the handset.

Figure 2, below, provides a photograph of our test Nokia 6021 showing a modified SMS message with the date 31st February 2090 at 13:99:99.

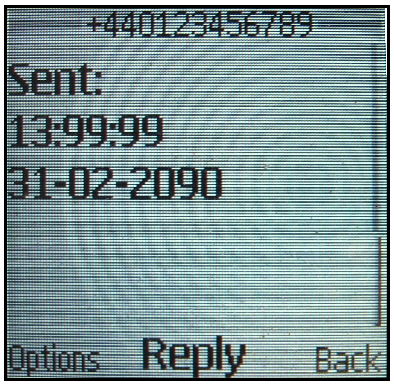


Fig. 2. Example Modified Date and Time as shown on a Nokia 6021 handset.

VI. Techniques for identifying falsified SMS messages

Without an external prompt, it would be unlikely for an examiner to consider whether an alteration has been made to an SMS message.

To assess if the service centre number, sender's number or date and time stamp have been modified, an examination of the connection records relating to the recorded sender's telephone number could be performed. For an unmodified SMS message, the details present on the mobile telephone handset should match those retained by the network provider. Should any of those details not match, it may be the case that those elements have been altered.

As the connection records do not generally record SMS content, identifying an SMS message which has had its contents, but not its service centre number, sender's number or date and time stamp modified may prove difficult. An examination of the alleged handset used to send the SMS message may provide an indication of the original content. However, consideration would have to be given to the fact that the date and time stamp of the sent SMS message may be inaccurate (or non-existent) due to being time stamped according to the handset's clock.

As the length of the modified SMS content is likely to have changed, it may be worthwhile determining how many parts would have had to be used to transfer the SMS message and compare this to the number of entries present in the reported sender's connection records. Should these not match it may be the case that the content has been modified.

Finally, if allegations have been made, or suspicions raised that someone has been using the techniques outlined in this paper to falsify a SMS message, an examination of the suspect's computer may provide log files relating to the flasher/service box's usage or backup files of PM tables. Further examination of these files may provide the original content of the modified SMS message.

VII. Conclusions

The purpose of our tests was to establish if SMS messages could be falsified on a mobile telephone handset, specifically the Nokia 6021 handset. Although attempts to inject an

entirely new SMS message into the handset's memory were unsuccessful, it was found that modifying an existing SMS message was possible using COTS software and hardware. As all the user visible parameters of the SMS message could be modified, an SMS message's origins and original content could be hidden from an examiner. As such, with minimal financial investment, any determined user with technical knowledge of the structure and encoding of the SMS message could falsify the details and content of an SMS message.

Acknowledgements

The authors, Mr Thomas Marryat and Mr John Corcoran would like to thank Dr David Schudel and Dr Jane Bloor for their contributions to this document.

References

Advance Turbo Flasher by AdvanceTeam. (n.d.). . Retrieved March 24, 2010, from http://advance-box.com/index.php?p=products

CYCLONE-Box. (n.d.). . Retrieved March 24, 2010, from http://www.cyclonebox.com/index.php?page=Home

editor PSPad - freeware HTML editor, PHP editor, XHTML, JavaScript, ASP, Perl, C, HEX editor. (n.d.). . Retrieved March 12, 2010, from http://www.pspad.com/

Gartner Says Worldwide Mobile Phone Sales Declined 6 Per Cent and Smartphones Grew 27 Per Cent in Second Quarter of 2009. (n.d.). . Retrieved March 12, 2010, from http://www.gartner.com/it/page.jsp?id=1126812

Nokia Europe - Nokia 6021 - Support. (n.d.). . Retrieved March 12, 2010, from http://europe.nokia.com/find-products/devices/nokia-6021

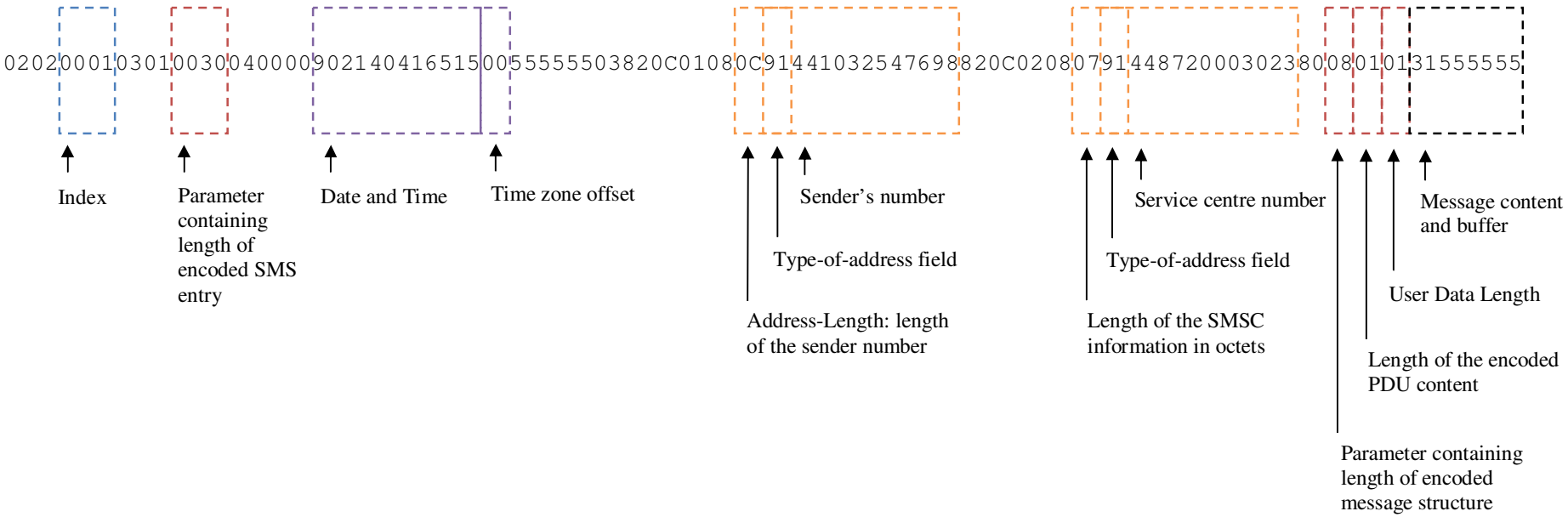
Technical realization of the Short Message Service (SMS), 3GPP TS 03.40, version 7.5.0, (1998)

UFSxHWK. (n.d.). . Retrieved March 12, 2010, from http://www.ufsxhwk.com/

Mr Thomas Marryat is a graduate of the University of Durham, where he received a BSc with Honours in Software Engineering. He joined Keith Borer Consultants in July 2007 where he undertakes the examination of digital devices, specialising in mobile telephones. He is instructed in approximately 50 to 60 cases a year. He can be contacted by e-mail at thomas.marryat@keithborer.co.uk.

Mr John Corcoran is a graduate of the University of Durham, where he received a BSc with Honours in Computer Science. He joined Keith Borer Consultants in August 2009 and is a member of the digital forensics team. He can be contacted by e-mail at john.corcoran@keithborer.co.uk.

Appendix 1


0202000103010030040000902140416515005555550382OC01080C914410325476988 20C0208079144872000302380080101 31555555
Index
Parameter containing length of encoded SMS entry
Date and Time
Time zone offset
Sender's number
Type-of-address field
Address-Length: length of the sender number
Service centre number
Type-of-address field
Length of the SMSC information in octets
Message content and buffer
User Data Length
Length of the encoded PDU content
Parameter containing length of encoded message structure