On Forensics: A Silent SMS Attack

Neil Croft
Information and Computer Security Architectures (ICSA) Research Group
Department of Computer Science
University of Pretoria
Pretoria
South Africa
Email: ringtingting@gmail.com

***Abstract*—Silent messages often referred to as Silent SMS or Stealth SMS, when delivered to a mobile handset is indicated neither on the display nor by an acoustic alert signal. In the paper [2], the authors highlighted the technical details of sending a silent SMS, furthermore sending multiple incessant silent SMSs performing A silent SMS denial of Service (DoS) attack. These stealth messages are not only used to perform DoS attacks but are increasingly sent in order to force the continuous update of subscriber location information. In doing so, anyone with access to the network infrastructure, may use the technology to better track the movements of any subscriber on the mobile network.**

This paper describes, from a forensic perspective, how a silent application-generated SMS (attack) is discovered. We then investigate the possibilities of retrieving silent SMS evidence at both the handset and network level. Furthermore, using propositional logic, we explore related SMS network configurations which might thwart the forensic ability of a silent SMS attack.

Keywords: Forensics, mobile, SMS, silent, stealth

I. Introduction

The Mobile Station (MS) is the mobile phone or mobile network compliant device. The MS provides access to the network and consists of Mobile Equipment (ME) and a Subscriber Identity Module (SIM) card [5] which is connected to an ss7 [6] network. The Short Message Service (SMS) message, sometimes referred to simply as a Text message, is specified by the ETSI organization in documents GSM 03.40 [3] and GSM 03.38 [4]. SMS is a store and forward service, in other words, short messages are not sent directly from sender to receiver, but always to a MS via a SMS Centre (SMSC). Message delivery is ”best effort”, so there are no guarantees that a message will actually be delivered to its recipient, but delay or complete loss of a message is uncommon. If delivered successfully, the SMS message is usually stored on the recipients SIM card under USER-DATA.

SMS messages can be up to 160 characters long, where each character is represented by the 7-bit default alphabet. Eight-bit messages (max 140 characters) are usually not viewable by the phones as text messages; instead they are used for data messages e.g. smart messaging (images and ringing tones) .16-bit messages (max 70 characters) are used in the display of Unicode (UCS2) text messages, viewable by most phones. A 16-bit text message (not commonly used anymore) will on some phones appear as a Flash SMS (aka blinking SMS or alert SMS). GSM 03.40 [3] describes a short message of type 0 which indicates that the Mobile Equipment (ME) or handset must acknowledge receipt of the short message but may discard its contents. Such an SMS is useful, in particular, for the police services to send an application-generated SMS to detect the presence of a mobile handset without the intended party knowing about the request. The Short Message Peer-To-Peer Protocol (SMPP) [8], [9] is a telecommunications industry protocol for exchanging SMS messages between SMS peer entities or applications and short message service centres (SMSCs). It is often used to allow third parties to submit, at an application layer, SMS messages using data packets (PDUs). Data exchange is synchronous, where the sender must wait for a response to each PDU being sent, or asynchronous, where the receiving and sending of PDU executes independently making use of buffers and timers while adhering to throughput limits. The protocol is based on pairs of request and response PDUs exchanged over OSI layer 4 (TCP session). PDUs are binary encoded for efficiency. The latest version of SMPP is v5.0 [9].

Using the SMPP protocol, an SMS application system called the External Short Message Entity (EMSE) may initiate an application layer connection with an SMSC over TCP/IP or x.25 network connection and may then send short messages and receive short messages to and from the SMSC respectively [8]. An EMSE is capable of manipulating the sender_id or originator of the message using the SMPP protocol. This is commonly referred to as number masquerading. Using international mobile number formatting, messages are sent globally between mobile networks.

When a mobile terminated message (of type class 0) is sent, and if the MS has the capability of displaying short messages, the MS shall display the message and confirm delivery back to the SMSC. If a MS is incapable of displaying a message, it is simply ignored and discarded (not saved under USER-DATA) by the handset.

One can locate a user by identifying the three antennas (base stations) closest to the mobile, and then deduce (using triangulation) the location by the speed is takes the signal to make the return trip. In other words, location can be approximated by simply using the signalling layer of the mobile network. The mobile handset updates its presence periodically on the network, but when a subscriber moves, this information is not necessarily updated immediately. By

978-1-4673-2159-4/12/$31.00 ©2012 IEEE

sending a silent SMS, the handset is forced to update its location information on the network. A network authority may perform a silent SMS attack for the sole purpose to better track a subscriber. Using this approach, without the subscribers knowledge, gives a more accurate account of the subscribers movements. A stealth SMS follows the principles of a round-trip signal or essentially a ping of the handset. Is information available as to whether silent SMS messages are being used for location purposes? This question was answered at the 28th Chaos Communication Congress in Berlin (Germany), where it was allegedly confirmed by a member of the Interior Minister, that the German police and German intelligence services sent an average of 440 000 stealth SMS over the last year [1].

In this paper we investigate how we would forensically obtain evidence of a silent SMS attack. We investigate, both at a network and handset level, what evidence is present that indicates such an attack. We further highlight network configurations which may enhance a forensics investigation. In some instances, using an anti-forensic configuration, render it impossible to gather any evidence of a silent SMS attack whatsoever.

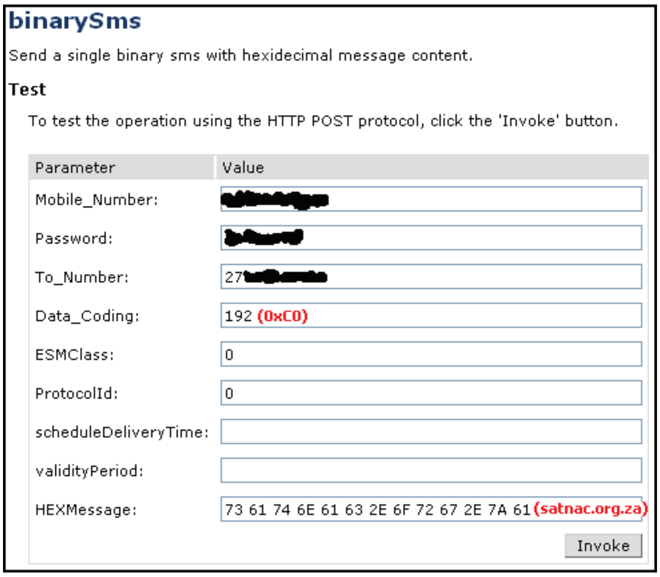
This paper is structured as follows: Section 2 covers background work on the technical details of sending a silent SMS by either manipulating the data coding scheme or by manipulating the scheduled delivery time of the SMS message. In Section 3, we investigate the possibilities of retrieving silent SMS evidence at both the handset and network level. Some suggested network and handset configurations will impede or assist with the forensic investigation. Section 4 concludes this paper.

II. Background

In the paper [2], we showed two ways to send a silent SMS. Although there are indeed a number of ways to manipulate and ultimately malform a SMS PDU, we showcased two common examples. The first being simply a change the data coding scheme in the message headers (UDHI) when creating the SMPP submit_sm PDU request. The second is to affect the scheduled_delivery_time and validity_period by setting the delivery time to a date in the past and or by making the message valid for an extremely short period of time, again when creating the SMPP submit_sm PDU request. In both instances, when tested across several SMPP gateways, messages did not arrive on the handset. Successful delivery receipts for these silent test messages were received corresponding to the original message_id.

A. Manipulating the Data Coding Scheme

Using GSM 0.3.38 [4] as a reference, if the data_coding is set to 192 (0xC0)(11000000), then this sets the Message Waiting Indication Group identifier. In doing so, this translates to the handset that the message MUST BE discarded. If bits 7..4 are set to 1100, the mobile may discard the message [4]. If the silent SMS landed on the handset successfully, and the SMSC requested a delivery receipt, a deliver_sm PDU with status text DELIVRD is returned to the EMSE. An example submit_sm PDU (in hex) is shown in Figure 1. The resulting successful response deliver_sm is shown in Figure 2.



binarySms

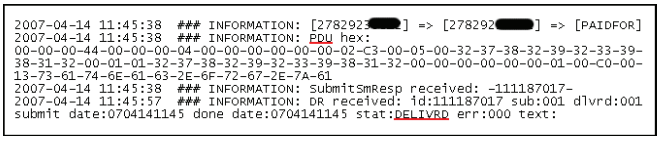
Send a single binary sms with hexidecimal message content.

Test

To test the operation using the HTTP POST protocol, click the 'Invoke' button.

Parameter	Value
Mobile_Number:	[redacted]
Password:	[redacted]
To_Number:	27[redacted]
Data_Coding:	192 (0xC0)
ESMClass:	0
ProtocolId:	0
scheduleDeliveryTime:	
validityPeriod:	
HEXMessage:	73 61 74 6E 61 63 2E 6F 72 67 2E 7A 61 (satnac.org.za)

Fig. 1. Webservice Binary SMS PDU builder



```
2007-04-14 11:45:38  ### INFORMATION: [2782923[redacted]] => [278292[redacted]] => [PAIDFOR]
2007-04-14 11:45:38  ### INFORMATION: PDU hex:
00-00-00-44-00-00-00-04-00-00-00-00-00-00-02-C3-00-05-00-32-37-38-32-39-32-33-39-
38-31-32-00-01-01-32-37-38-32-39-32-33-39-38-31-32-00-00-00-00-00-00-01-00-C0-00-
13-73-61-74-6E-61-63-2E-6F-72-67-2E-7A-61
2007-04-14 11:45:38  ### INFORMATION: SubmitSmResp received: -111187017-
2007-04-14 11:45:57  ### INFORMATION: DR received: id:111187017 sub:001 dlvrd:001
submit date:0704141145 done date:0704141145 stat:DELIVRD err:000 text:
```

Fig. 2. deliver_sm response PDU Dump

1) Manipulating the Timing and Validity Scheme: Again making use of GSM 0.3.38 [4], we may manipulate the scheduled_delivery_time and validity_period of a message. Although not completely transparent and tested in different network environments, this approach achieves a silent SMS result. By setting the scheduled_delivery_time or validity_period to before todays date in the format (YYMMDDhhmmsstnn) the message delivers but does not show on the handset. Again, if the silent SMS landed on the handset successfully, and the SMSC requested a delivery receipt, a deliver_sm PDU with status text DELIVRD is returned to the EMSE.

III. Silent SMS Forensics

A Stealth SMS allows a sender to send one message to another mobile without the knowledge of its owner. The message is discarded from the handset without a trace. This is not only problematic for privacy, but legally too, as it is unclear by definition if such messages form part of communication, since no content is delivered. This is convenient for some as such surveillance technologies are not governed by legal frameworks designed to manage the inviolability of telecommunications. This legal vacuum allows police and intelligence services to reactive inactive suspects (subscribers) and improves geo-location information. In doing so, an investigator may refer to a map to relate movements of a handset in near real-time. Silent SMS is the only practical method for immediate update of location information, when the subscriber is constantly moving but the handset is not in use. Thus, silent SMS is a valuable tool for investigation which when ordered by a judge, for a specific case, in some countries, might ever violate the fundamental right to a subscribers protection of privacy. The benefits of silent SMS do not stop there: by sending a large number of SMS can cause a disruption of other services and discharges the battery due to the continual arrival of SMS PDUs.

We now know technically how silent SMS messages are sent and what these messages can be used for, but how can we extract evidence (if ordered by a court of law) which shows an attack occurred. We begin by investigating what information is available to the forensic investigator at a network level and continue with information available on the handset.

A. On the Network

Delivery Reports (DR) contain details of SMS delivery, logged for the sole purpose to bill subscribers on the network. At an application layer (EMSE) it is possible to submit a request in order not to receive a delivery report. Turning a DR off simply stops the SMSC or SMPP server from generating a delivery report. The receiving network does not get informed whether or not to return a delivery report it will always return a positive acknowledgment if the handset received the SMS. The SMSC decides to create the delivery report from this acknowledgement. The DR generated by the SMSC would not be any different for a silent SMS compared to a standard SMS. Forensically, we will only be able to confirm if a SMS was sent to a particular number. As a forensic investigator, our only other option is to scrutinize ss7 network logs. However, again, any destination network ss7 logging would record a silent SMS in the same way as a normal SMS. Even if we had access to such information, not all networks do keep logs due to ss7 protocol analysis overheads and space demands.

At a network layer, the only evidence of an attack might lie in the analysis of the throttling of SMS messages. We are able to detect a number of messages being sent to the same number in quick succession if a sc-alert is requested. A simple number count would indicate how many requests for sc-alert for a particular mobile number (msisdn) it has received. It would be more difficult to detect if no sc-alert was requested, generally though all SMSCs request sc-alert PDUs. If it were visible enough to see any sort of originator of the silent SMS, it would also be visible to see the originating SMSC and, therefore, trace it. However, this may prove difficult if the msisdn (mobile number) used, is masqueraded. On the SMSC we could see how the message was sent to the SMSC, however this wouldnt give us visibility of the EMSE but just the account information linked to the EMSE.

B. On the Handset

If the silent SMS is sent as a flash SMS, then technically speaking there isnt any evidence available on the handset. In other words, no data is stored in the USER-DATA on the SIM card. To thawte a silent SMS attack, the recipient could simply use a handset that doesnt support silent SMSs. An example of such a handset is some of the first versions of the iPhone. Of interest, a GSM modem would receive a silent SMS in the same way as a normal SMS is received.

To trace a silent SMS attack, the only available option is to develop an application (mobile OS dependant) that links directly to the phone OS and intercepts its received SMS messages. It would be at the discretion of the application to determine whether to display, hide, log or remotely transfer the SMS message details. UDHI (header information), showing messages of type 0 must be captured. Such an application would have to be pre-installed before a silent SMS attack occurred. A form of social engineering is a means to trick a user into installing such a piece of software on their handset. One such example is a clickable URL (containing the application installation file) sent to the handset. This arrives on the handset and is usually displayed as a service message and when opened, will launch the handsets default browser and redirect to the entered URL. The user may be coursed into installing the application under false pretences. Once the application is installed, there are various techniques which will hide or make invisible the application to the handset owner. One such example of a stealth or rogue application is mobistealth [7] which tracks and monitors all subscriber activity. The application is downloadable for a number of mobile operating systems including iOS, RIM OS, Symbian and Android.

If there is no means to forensically access silent SMS data, how would we test a handset is under an attack? One rudimentary approach is to place the handset next to a speaker and listen for about 2-3 second bursts of loud interference noise; this indicates GSM data transfer of an SMS or Call. If such a noise persists, as a forensic investigator, we may assume that the handset is under attack.

C. Anti-Forensic configuration

In propositional logic, modus ponendo ponens [10] or implication elimination is a valid, simple argument form and rule of inference. It can be summarized as ”P implies Q; P is asserted to be true, so therefore Q must be true”. An argument may be valid, but this has no bearing on whether any of the statements in the argument are true; for modus ponens to be a sound argument, the premises must be true for any true instances of the conclusion. An argument can be valid but unsound if one or more premises are false; if an argument is valid and all the premises are true, then the argument is sound.

From a technical perspective and using porpositional logic, if you cant ”see” messages then you cant forward them on, if you can then messages may be forwarded via any SMSC, unless the reply-path SMSC is set. By default the reply-path is not set. In other words, as part of the original GSM specification, an SMSC may forward messages and at the same time set the message centre. This allows an SMS to be replied to using the same message centre that the SMS was sent from, in order to guarantee coverage. Typically networks can detect this and sometimes charge an additional fee when using third party SMSCs. In essence, this is the same as changing the message centre to something else in your phone settings. By forwarding messages through a number of SMSCs, with no reply-path SMSC set, it becomes nearly impossible for a forensic investigator to trace the origin of an attack from network data. This argument is valid and sound.

If we choose a handset with no silent SMS support and or configure the handset to disallow any application installations (by enabling phone security settings), it too becomes impossible for a forensic investigator to trace the origin of an attack from the handset. If the above scenario presents itself, the investigator is faced with a complete anti-forensic situation. No data collection implies no data and, consequently, no forensic ability implies an anti-forensics situation.

IV. Conclusion

In this paper, we highlighted the use of silent SMS (attack) as a means to continuously update subscriber location information. The use of Silent SMS messages to better trace subscribers is no doubt a contentious issue. However, the focus of this work was to research the data (network and handset) available for extraction during a forensic investigation where a silent SMS is concerned.

In this paper, we showed there is very little data available for extraction by a forensic investigator. This is typically due to the nature and configuration of existing mobile networks and capacity constraints. At a network level, we may only infer the existence of an attack through analysis of the number of messages received. Only by using rudimentary techniques, with the mobile device in hand, can a forensic investigator confirm (through radio interference), the existence of a continual stream of inbound network data. Likewise, only through the installation of an application, whose sole purpose is to intercept SMS messages at a mobile operating system level, are we able to extract silent SMS data. Furthermore, it is evident that through some network configuration (SMSC forwarding with no reply-path) and handset security settings (preventing application installations), no forensic data is available to the investigator.

Acknowledgment

The authors would like to thank mahalamobile pty ltd for access to various sms gateways for testing purposes.

References

[1] 28th Chaos Communication Congress in Berlin website (2011), http://events.ccc.de/congress/2011/wiki/Welcome (Accessed 29 February 2012).

[2] Croft, N.J., and Olivier M.S. (2007), A Silent SMS Denial of Service (DoS) Attack, Southern African Telecommunication Networks and Applications Conference 2007 (SATNAC 2007) Proceedings, Sugar Beach Resort, Mauritius.

[3] Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS); Point to Point (PP)(GSM 03.40 version 6.0.0), European telecommunications Standard Institute, ETSI, March 1998.

[4] Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information (GSM 03.38 version 7.0.0 Release 1998), European telecommunications Standard Institute, ETSI, July 1998.

[5] European digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIMME) interface (GSM 11.11), European Telecommunications Standards Institute, Sophia Antipolis, France, 1998.

[6] Lin, Y.B., Signalling System Number 7, IEEE Potentials, pages 5-8, August 1996.

[7] MobiStealth website (2012), Home page, http://www.mobistealth.com (Accessed 29 February 2012).

[8] Short Message Peer to Peer Protocol Specification v3.4, The SMS Forum, October 1999.

[9] Short Message Peer to Peer Protocol Specification v5.0, The SMS Forum, February 2003.

[10] Stone, J.R., Latin for the Illiterati: Exorcizing the Ghosts of a Dead Language, isbn:9780415917759,Routledge,1996