On forensics: A silent SMS attack

Neil Croft

Research conducted in the Information and Computer Security Architectures (ICSA) Research Group in the Department of Computer Science at the University of Pretoria has been investigating how one would forensically obtain evidence of a silent SMS attack. Both at a network and handset level, what evidence is present that indicates that such an attack has taken place? Using an anti-forensic network configuration may render it impossible to gather any evidence of a silent SMS attack.

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, which is connected to an ss7 network. The short message service (SMS) message, sometimes simply referred to as a text message, is a store-and-forward service, in other words, short messages are not sent directly from sender to receiver, but always to an MS via an 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 recipient's SIM card under user data.

How are silent SMS messages sent?

The 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) is a telecommunications industry protocol for exchanging SMS messages between SMS peer entities or applications and SMSCs. It is often used to allow third parties to submit, at an application layer, SMS messages using protocol data units (PDUs). Data exchange is synchronous, where the sender must wait for a response to each PDU (data packet) either being sent immediately or asynchronously (where the receiving and sending of PDUs are executed 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 the Open Systems Interconnect (OSI) layer 4, which is a Transmission Control Protocol (TCP) session. PDUs are binary encoded for efficiency.

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

What are stealth SMS messages used for?

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 it 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 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 of better tracking a subscriber. Using this approach without the subscriber's knowledge gives a more accurate account of the subscriber's movements.

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, in 2011 where it was allegedly confirmed by a member of the Minister of the Interior that the German police and German intelligence services had sent an average of 440 000 stealth SMSs over the last year.

How can evidence be extracted to show that an attack occurred?

Although there are indeed a number of ways to manipulate and ultimately malform an SMS PDU, two common examples can be showcased. The first is simply a change to the data coding scheme in the message headers 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 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 from a legal perspective too. 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 members of the police and intelligence services to reactivate inactive suspects (subscribers) and improves geo-location information.

What information is available to the forensic investigator?

A silent SMS is the only practical method to immediately update 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 even violate the fundamental right to a subscriber's protection of privacy.

A stealth SMS allows a sender to send a 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 from a legal perspective too.

The use of silent SMSs to trace subscribers is no doubt a contentious issue. However, the focus of the research conducted was to examine the data available for extraction during a forensic investigation.

It was found that 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, one may only infer the existence of an attack through an 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, is one able to extract silent SMS data. It is evident that through some network configuration and handset security settings, no forensic data is available to the investigator.

References

1. 28th Chaos Communication Congress in Berlin website. 2011. Available: http://events.ccc.de/congress/2011/wiki/Welcome (accessed on 29 February 2012).
2. Croft, NJ & Olivier, MS. 2007. A silent SMS denial of service (DoS) attack. In: *Southern African Telecommunication Networks and Applications Conference 2007 (SATNAC 2007) Proceedings*. Sugar Beach Resort, Mauritius.
3. European Telecommunications Standard Institute (ETSI). 1998. Digital cellular telecommunications system (Phase 2+). In: *Technical realization of the Short Message Service (SMS); Point to Point (PP)(GSM 03.40 version 6.0.0)*.
4. ETSI. 1998. Digital cellular telecommunications system (Phase 2+). In: *Alphabets and language-specific information (GSM 03.38 version 7.0.0 Release 1998)*.
5. ETSI. 1998. European digital cellular telecommunications system (Phase 2). *Specification of the Subscriber Identity Module - Mobile Equipment (SIMME) interface (GSM 11.11)*.
6. Lin, YB. 1996. Signalling System Number 7, IEEE Potentials: August (pp 5–8).
7. MobiStealth website. 2012. Available: http://www.mobistealth.com (accessed on 29 February 2012).
8. Short Message Peer to Peer Protocol Specification v3.4. 1999. In: *The SMS Forum*, October.
9. Short Message Peer to Peer Protocol Specification v5.0. 2003. *The SMS Forum*, February.
10. Stone, JR. 1996. *Latin for the Illiterati: Exorcizing the ghosts of a dead language*. Routledge.

***Neil Croft** is a member of the Information and Computer Security Architectures (ICSA) Research Group in the Department of Computer Science at the University of Pretoria.*