Technische Universität Berlin

Forschungsberichte
der Fakultät IV – Elektrotechnik und Informatik

Countering SMS Attacks: Filter Recommendations

Nico Golde and Collin Mulliner

Bericht-Nr. 2011 – 09
ISSN 1436-9915

Countering SMS Attacks: Filter Recommendations

Technical Report 2011-09

ISSN: 1436-9915

Nico Golde and Collin Mulliner
Security in Telecommunications
Technische Universität Berlin
{nico,collin}@sec.t-labs.tu-berlin.de

Abstract

In this paper we summarize the findings of our investigation on security issues of Short Message Service (SMS) clients on mobile phones. We realized that firmware updates will not be available on a large scale and thus see filtering of SMS traffic as the only possible counter measure against large scale attacks based on SMS messages. This paper presents our ideas on filtering SMS features by the mobile network operators.

1. Introduction

We investigated the security of Short Message Service (SMS) client implementations – ME side SMS security. Analysis was done on a number of smartphones [10, 3] (iPhone/iOS, Android, Windows Mobile) in 2009 and in 2010 on devices produced by major feature phone manufacturers [12]. Analysis of feature phones was carried out on the five biggest manufacturers. These are Nokia, Samsung, Sony Ericsson, LG, and Motorola. In addition we also discovered bugs in phones made by Micromax (mostly sold and used in India) and HP/Palm.

Most of the bugs discovered by us lead the attacked phones to disconnect from the mobile phone network. In some instances attacked phones even rebooted. Further, calls in process would be interrupted. Some phones *switch off* if attacked multiple times in a row. Additionally, we accidentally bricked (destroyed) one phone during testing – but we did not further investigate this.

Furthermore, investigation of the vulnerabilities and the resulting attacks lead us to the discovery of attack amplification possibilities. This is observed when the targeted phone does not acknowledge the SMS message that it received from the network. The suppression of the acknowledgement can happen if the phone crashes or reboots before the acknowledgement is generated or sent back to the network. If the network (the SMSC) does not receive the acknowledgement it believes that the message was not delivered to the recipient. Therefore, the SMSC resends the message and thus crashes the phone again. This behavior repeats until the message is delivered or its life time expires.

The aim of this paper is provide the necessary information to allow mobile network operators to filter and block offending SMS messages without publishing the actual SMS message payloads that trigger bugs. The audience of this paper are people familiar with SMS messaging inside the mobile network operator.

2. SMS Vulnerabilities and Impact

We discovered bugs in the firmware of major mobile phone manufacturers. In this section we provide details on the vulnerabilities discovered by us and their impact to the phones. We further created a demonstration video [11] that shows the effect of the bugs on a number of feature phones. We notified the manufacturers and provided details on the vulnerabilities ahead of time in order to get firmware fixes started.

Below we briefly describe the bugs with their effect for each platform. For completeness we also included bugs that were found by others.

Nokia S40 Discovered in [12]. Attacked devices show the Nokia *white-screen-of-death* followed by a network disconnect and possible call interruption. The message receipt is not acknowledged to the network, repeated delivery attempts switches off the phone. The bug is tested on, but not limited to, the following devices: `6300, 6233, 6131 NFC, 3110c`.

Samsung Discovered in [12]. Attacked devices crash and completely reboot when the message is opened by the user. It further disables the ability to receive SMS messages permanently in addition the SMS and phone book application can no longer be started and used. The bug was named *Funkstille*. The bug was tested on following devices: `S5230, B5310`.

Sony Ericsson Discovered in [12]. The attacked phone crashes and completely reboots, in the process it is disconnected from the mobile phone network. Calls in process are interrupted. The message is not acknowledged to the network and thus the network continuously tries to retransmit the message. The bug was tested on the following phones: `W800i, W810i, W890i, Aino`.

LG Discovered in [12]. The device crashes and completely reboots. In process it is disconnected from the phone network. Calls in process are interrupted. An additional crash is triggered when the message is manually opened by the user at a later point in time. The bug was tested on: `GM360`

Motorola Discovered in [12]. The user interface crashes and restarts and in process disconnects the phone from the network. A call in process is interrupted. Further the inbox is filling up with non-deletable messages. The bug was tested on: `Razr, Rokr, SVLR L7`

Micromax Discovered in [12]. The phone UI crashes and restarts and in progress the phone disconnects form the network. Possibly ongoing calls are interrupted. The bug has been found and tested on the following device: `X114`.

Palm Discovered in [12] but not published. The GSM process crashes and disconnects the phone from the network. Possibly calls are interrupted. The message receipt is not acknowledged to network, additional operator spoofing possibility due to insufficient sender information displayed to the user. Bug discovered and tested on: `Palm Pre`.

iPhone Discovered in [3]. SMS crashed the CommCenter process (main communication hub of the iPhone). The iPhone disconnected from the network and an ongoing call is interrupted. Further we showed that arbitrary code execution is possible. A second bug allowed to lock the device by crashing SpringBoard (the iPhone app launcher). Both bugs are fixed in iOS 3.0.1. Also see CVE-2009-2204.

Android Discovered in [3]. The bug crashed the Android telephony stack *com.android.phone* and thus disconnected the phone from the network. If the SIM card is protected by a PIN the phone will stay disconnected until the PIN is entered by the user. The bug was fixed in 1.5 CRC1. Also see oCERT-2009-014.

Additionally to the issues discovered by us there have been more issues found by other researchers. Please note that this list might be incomplete.

Nokia S60 Discovered in [6]. The attacked phone no longer is able to receive SMS and MMS. The bug was called *Curse of Silence*.

Sony Ericsson / Nokia Discovered in [4]. The bug leads to crash and complete reboot, including disconnecting the phone from the network and possible call interruption. Devices: `Sony Z5 and Nokia 6110, 32xx, 33xx, 51xx, 61xx, 62xx, 7110, 82xx, 9110, 9210`.

Nokia 6210 Discovered in [13]. The bug caused either the SMS receiving handler to crash, phone locking up (requiring battery to be removed) or forced restart, thus interrupting calls, and disconnect from the network.
Another bug that lead to crashes has been found in [5]

Siemens 3568i Discovered in [14]. This bug causes the phone to switch itself off. It was not possible to deleted the offending SMS from the inbox.

3. Filtering

We propose protecting customers by filtering possible malicious SMS messages at or before the SMSC. Please note that this list is probably by no means complete and we see these filtering mechanisms from the perspective of our specific testing. It might not always be feasible from an operator perspective to apply exactly this kind of filtering. We would rather see manufacturers and operators pushing firmware updates to fix the bugs but since this is unlikely to happen on large scale, filtering is the only way to tackle the problem. Our filter suggestions are:

Flash/Class 0 during our testing it became clear that the flash SMS handling is a code path that got very few testing and is likely to be affected by parsing issues that are not present in the normal SMS application code. While this feature is specified in the spec we have seen very few phones (from our test phones only the Nokia 6303i, there are probably more, this needs further investigation) that allow the customer to send this type of message. Additionally, there often seem to be spoofing issues because the phone is assuming this type of message is originating from the operator. In a lot of cases the sender number is not displayed at all. Non-feature phone examples for this are the Palm Pre (notified vendor, fixed in future updates) and the Blackberry Curve (notified vendor). Either this type of message should be filtered completely or at least limited to messages originating from the mobile operator.

SIM toolkit messages should be limited to be originating from the operator. The security state of this SMS feature is currently very unclear to researchers and future research on this will happen. It should not be possible to send SIM commands from one phone to another. Additionally the SIM Data Download feature includes a field to indicate if a reply packet should be generated or not. This is sent in the form of an SMS (the customer will get charged for the reply). Due to spoofing possibilities by online bulk providers et. al it is possible to perform SMS DDoS Attacks [7] (Section 5.2.3) or drain money from a customer. Our testing also indicated that the practical usage of this field depends on operator SIM cards though.

Multipart Operators should perform additional sanity checks on UDH IEI 0x00/0x08 (multipart). This includes checking the current part number being less or equal to the overall number of parts and the number of parts being zero. Many phones seem to perform insufficient checking of these values. Similar problems probably exist for other UDH IEIs as well.

TP-PID This one byte identifier specifies [2] an excessive list of mostly legacy inter-workings. We believe that most of the encodings except 0x00 and 0x7f for TP-PID are unused these days. These values should be filtered and evaluated for their use in real networks. Most of these and especially reserved values hit ME code that is often not very well tested due to the lack of real-life use (see Sony Ericsson bug).

TP-DCS See **SIM Toolkit/Flash**. Filtering should be applied on values matching 00xx.... where xx is 10.

UDH Application Port Addressing Filtering applied to this kind of UDH should include MMS notifications, OTAP/FOTA and WAP-push messages. These types of messages should be limited to be originating from the operator. Besides a number of implementation flaws, there exist also design issues [8, 9] which can be exploited to e.g. hijack mobile phone data connections. Additionally, WAP-push message originators are not displayed properly on all phones (Samsung e.g. displays only WAP-push) so it might get abused for spoofing. To the best of our knowledge there are no cases in which such messages are sent from third parties.

UDH Special SMS Message Indication This type of message should never be sent from a third party or another ME and should be limited to be originating from the network operator. We did not observe any parsing issues or bugs related to this feature. However, for a user without technical knowledge about SMS it is impossible and very annoying to get rid of this message indication on the phone. Depending on the type of phone it can be very annoying.

Length fields Several bugs have been introduced in the past due to messages with malformed values for the various length fields present in SMS. A common example for this were malformed UDHL values. We suggest filters performing additional sanity checks to at least the length values specified in the general SMS structures [2].

3.1. Reassembly of Multipart Messages

In the case of SMS message concatenation, filtering becomes hard if only individual parts can be inspected. This is a known problem (TCP stream reassembly) in the area of IP packet filters and intrusion detection systems (IDS). Therefore, we suggest to install filtering software that is capable to inspect multiple messages that belong to the same multipart message. We acknowledge that this might cause some policy change between operators since messages once accepted for delivery might not be discarded due to contract agreements.

3.2. Discussion

We believe that filtering and/or content inspection is not always possible because of privacy restrictions in some countries. Therefore, we suggest that in some cases (e.g. TP-PID and TP-DCS) the mobile operator instead sets fields or specific bits to known good values. Because of the large number of possible combinations of the encodings, we further suggest that operators do not just filter problematic encodings discussed in [12]. Instead, operators should look into valid use cases of these features (that can be actually found in real world networks) and apply a white listing approach. Operators should pro actively work together on assessing these features and building up filter lists.

4. Homerouting

Mobile network operators should enable *SMS homerouting* in order to protect phones while roaming. This is described in [1].

5. SMS Retransmission

A SMS message that fails to be delivered to a mobile phone is retransmitted to the phone a number of times by the SMSC before the message is discarded. If a mobile phone crashes before it can send the acknowledgement that it received a specific SMS message the network believes the message was not transmitted. Thus the SMSC will try to retransmit the message. This retransmission can be abused by an attacker to amplify his attack.

We suggest to limit the number of retries in order to make it less attractive for an attacker. In addition we suggest to increase the interval between retries.

Acknowledgements

The authors would like to thank Tobias Engel for some helpful discussion on SMS security.

References

[1] 3GPP. TR 23.840 Study into routeing of MT-SMs via the HPLMN.

[2] 3rd Generation Partnership Project. 3GPP TS 23.040 - Technical realization of the Short Message Service (SMS). http://www.3gpp.org/ftp/Specs/html-info/23040.htm, September 2004.

[3] C. Miller, C. Mulliner. Fuzzing the Phone in your Phone. http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-SLIDES.pdf, August 2009.

[4] T. Engel. SMS and all its features. http://berlin.ccc.de/~tobias/smsfeatures/html/slide_15.html, December 2001.

[5] T. Engel. SMS and all its features. http://berlin.ccc.de/~tobias/smsfeatures/html/slide_13.html, December 2001.

[6] T. Engel. Remote SMS/MMS Denial of Service - "Curse Of Silence" for Nokia S60 phones. http://berlin.ccc.de/~tobias/cursesms.txt, December 2008.

[7] N. Golde. SMS Vulnerability Analysis on Feature Phones. Master's thesis, Berlin Institue of Technology, February 2011.

[8] Mobile Security Lab. Hijacking Mobile Data Connections, April 2009.

[9] Mobile Security Lab. Hijacking Mobile Data Connections 2.0, November 2009.

[10] C. Mulliner and C. Miller. Injecting SMS Messages into Smart Phones for Security Analysis. In *Proceedings of the 3rd USENIX Workshop on Offensive Technologies (WOOT)*, Montreal, Canada, August 2009.

[11] Nico Golde and Collin Mulliner. SMS-o-Death: Demo Video. http://www.youtube.com/watch?v=vseY9kFCkIc, December 2010.

[12] Nico Golde and Collin Mulliner. SMS-o-Death: from analyzing to attacking mobile phones on a large scale. http://www.mulliner.org/security/sms/smsodeath_mulliner_golde_cansecwest2011.pdf, March 2011.

[13] @stake, Inc. Nokia 6210 DoS SMS Issue. http://www.auscert.org.au/render.html?it=2795, February 2003.

[14] XFocus/benjurry. Siemens Mobie SMS Exceptional Character Vulnerability. http://seclists.org/bugtraq/2002/Jan/162, January 2002.