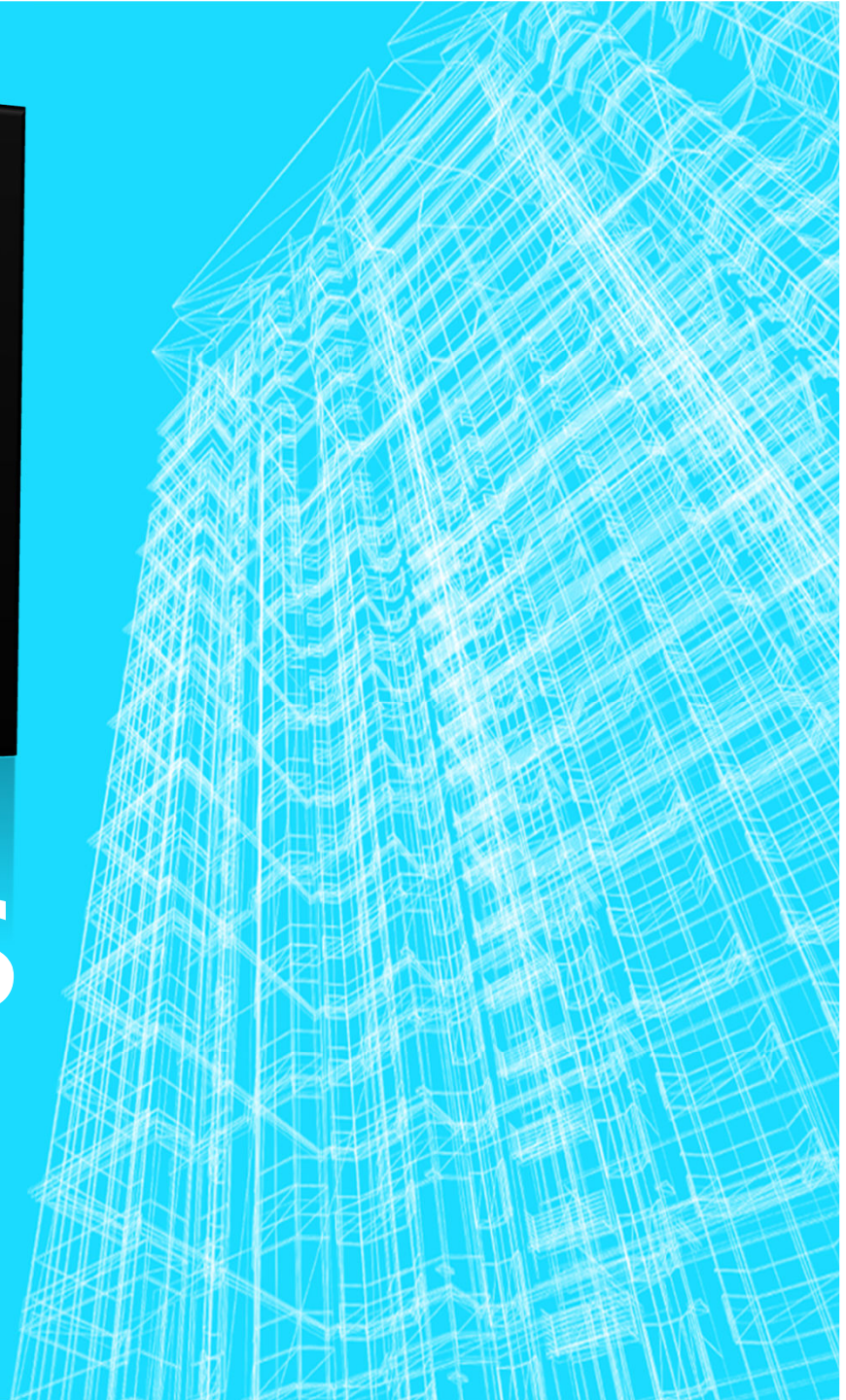




0c1ass2DOS

Bogdan ALECU
www.m-sec.net
[@msecnet](https://twitter.com/msecnet)





ABOUT...

- Independent security researcher
- Sysadmin @ Levi9
- Passionate about security, specially when it's related to mobile devices; started with NetMonitor (thanks Cosconor), continued with VoIP and finally GSM networks / mobile phones
- @msecnet / www.m-sec.net



TOPICS

- **SMS Intro**
- **Fun stuff with SMS**
- **Wrong implementation of SMS**
- **Can it be fixed?**
- **Conclusions**



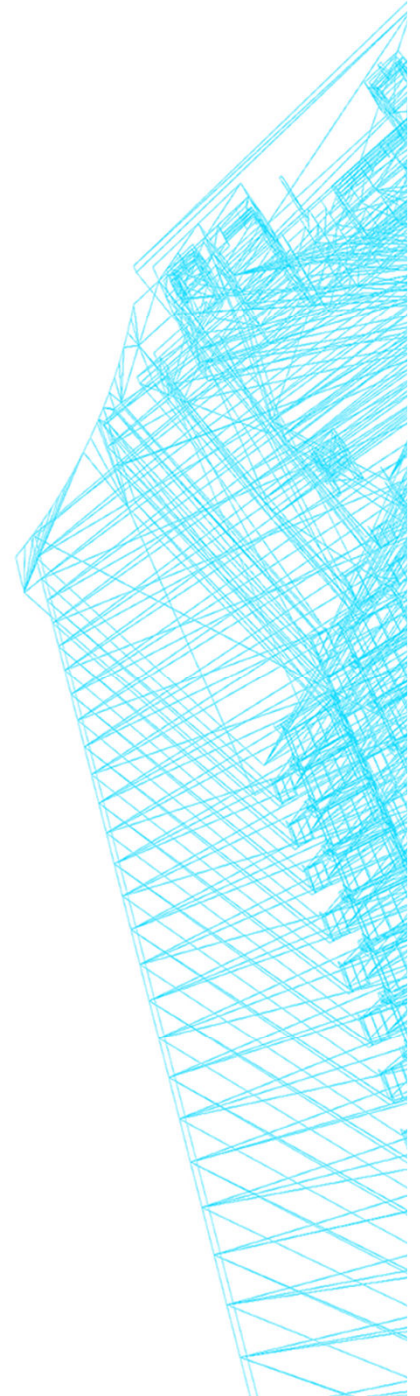
SMS INTRO

- SMS stands for Short Message Service and represents a way of communication via text between mobile phones and/or fixed lines, using a standardized protocol. It is an effective way of communication as the user just writes some text and it's almost instantly delivered to the destination.
- The provision of SMS makes use of a Service Center, which acts as a store and forward center for short messages

SMS INTRO

- Two different point-to-point services have been defined: mobile originated and mobile terminated
- An active MS shall be able to receive a short message TPDU - Transfer protocol data unit - (SMS-DELIVER) OR to submit a short message TPDU (SMS-SUBMIT) at any time ...

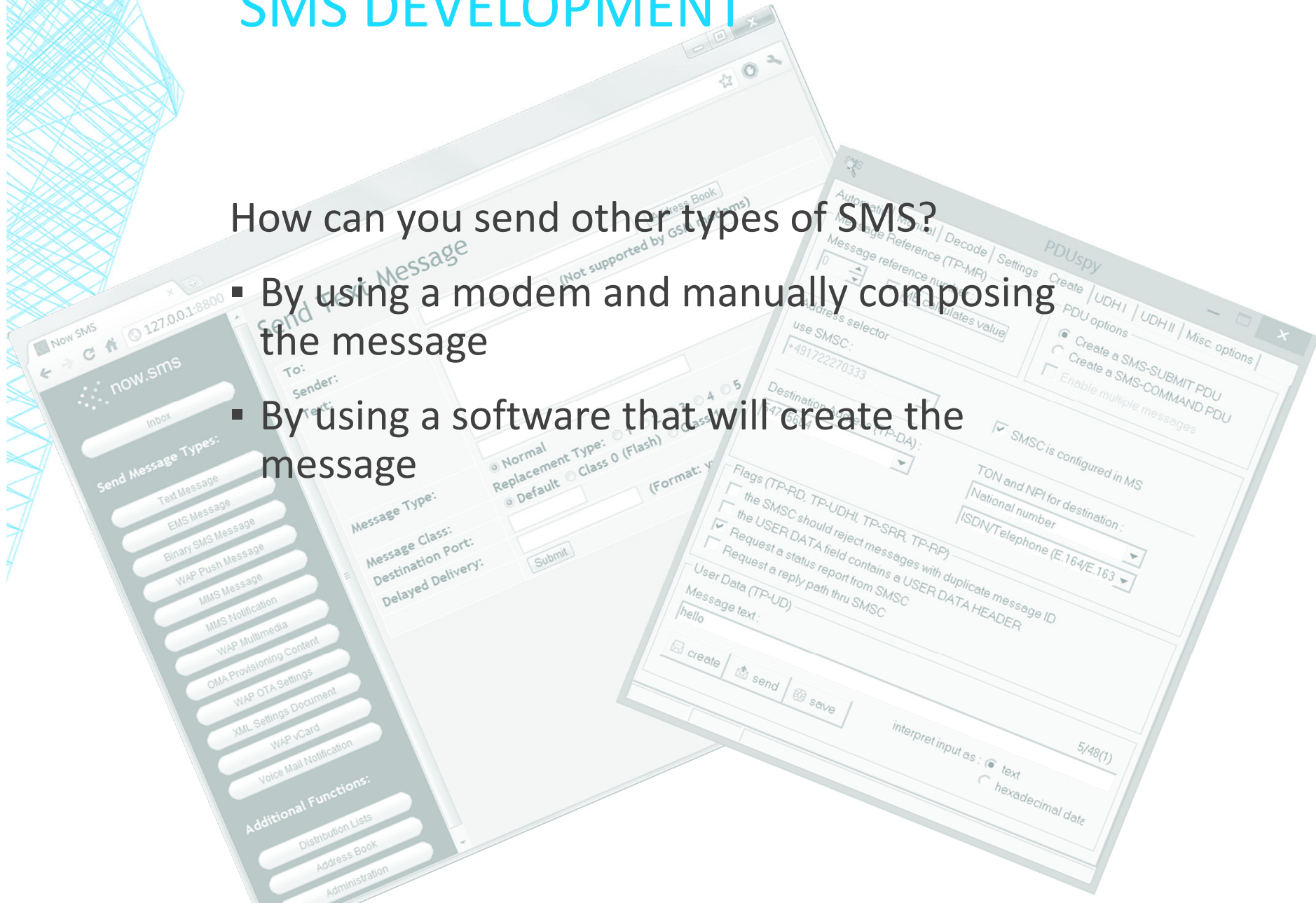
independently of whether or not there is a
speech or data call in progress



SMS DEVELOPMENT

How can you send other types of SMS?

- By using a modem and manually composing the message
- By using a software that will create the message



FUN STUFF WITH SMS

- Notifications

<http://mobiletidings.com/2009/07/08/voicemail-waiting-indication-sms/>

DCS:

0xC8 – turn on voicemail

0xC9 – turn on fax

0xCA – turn on email

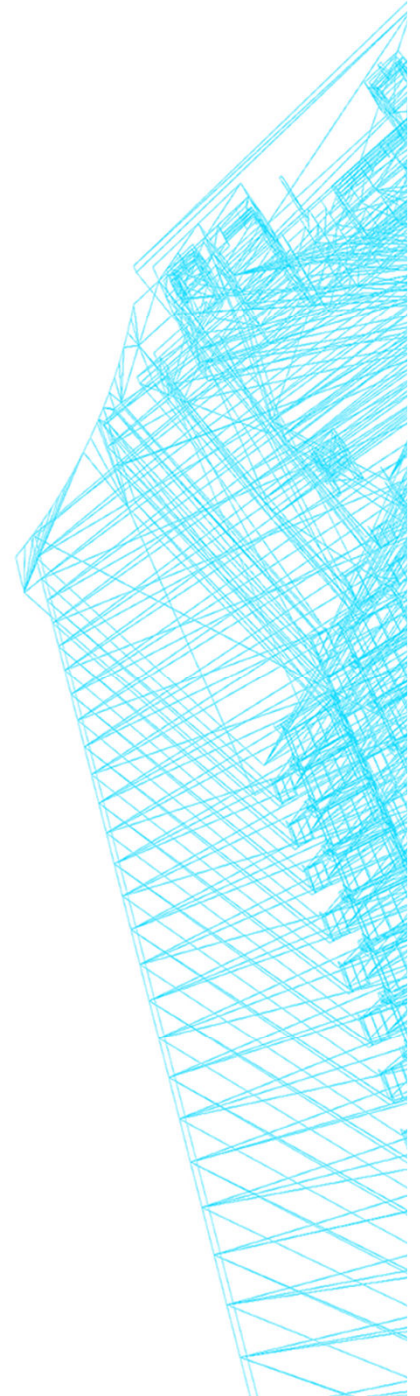
0xCB – turn on other message

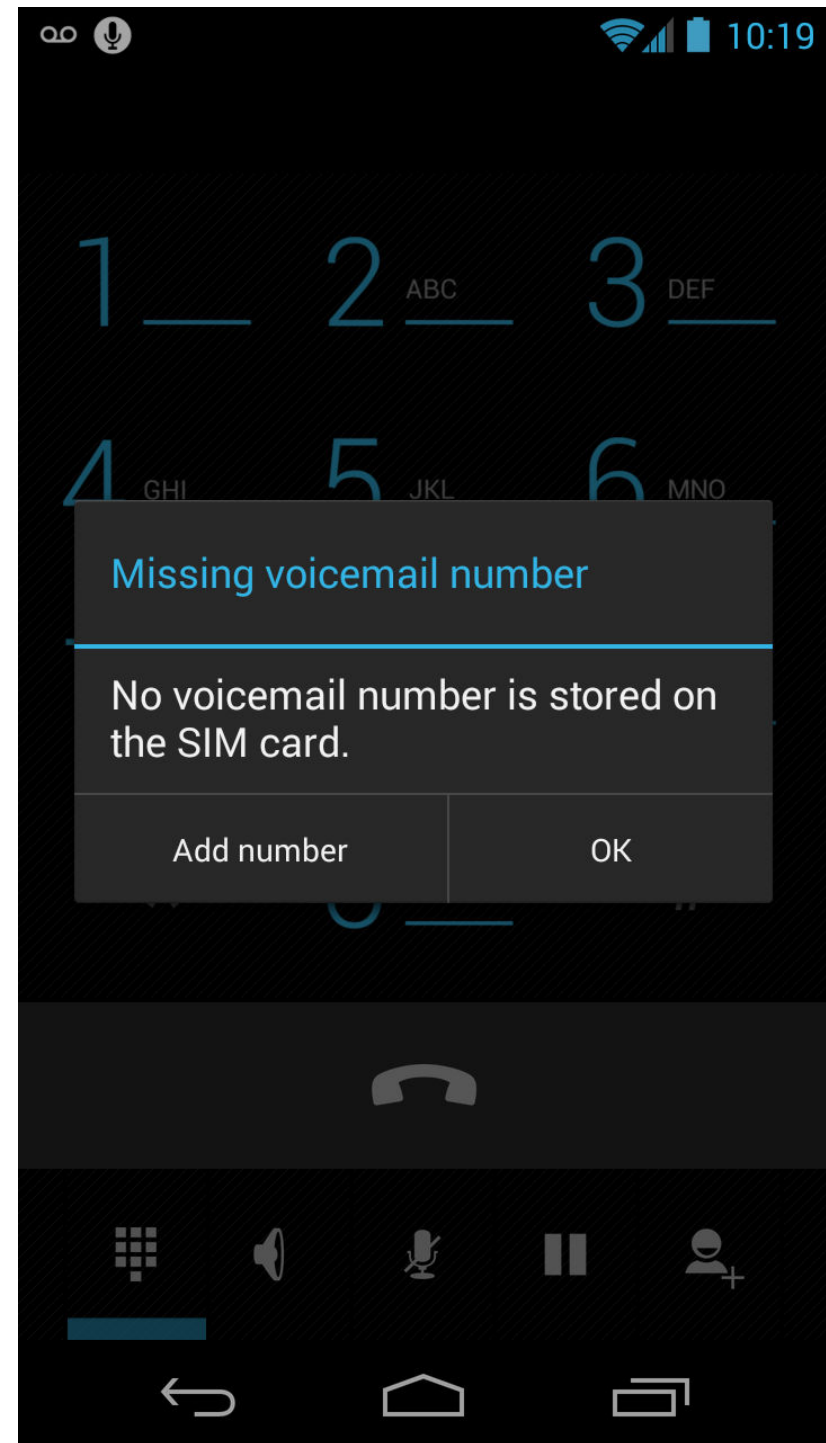
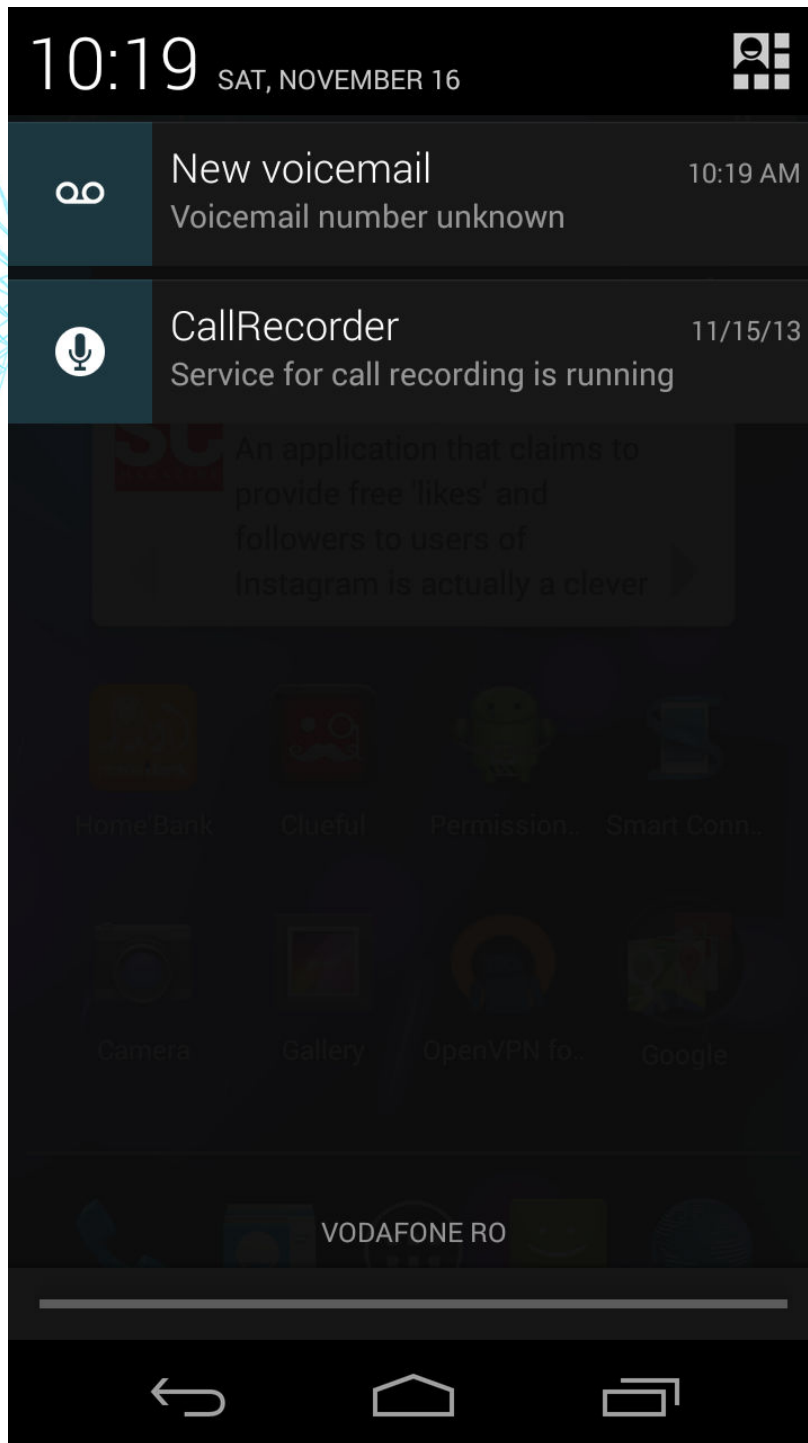
0xC0 – turn off voicemail

0xC1 – turn off fax

0xC2 – turn off email

0xC3 – turn off other message





FUN STUFF WITH SMS

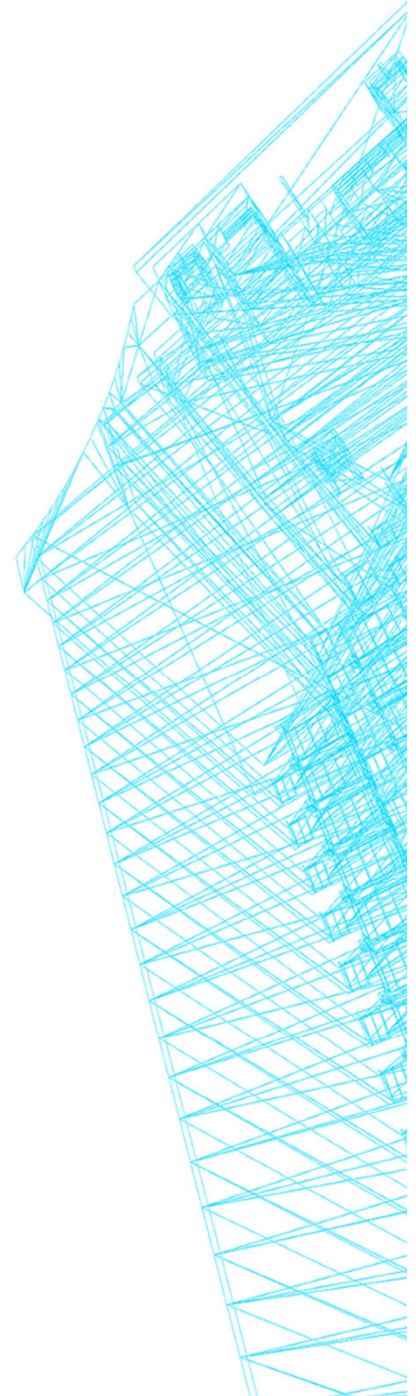
- “Silent” message

The receiving device must acknowledge receipt of the message (so you can get a delivery receipt), but the content of the message is to be discarded

Some carriers might restore it

PID: 0x40

DCS: 0xC0

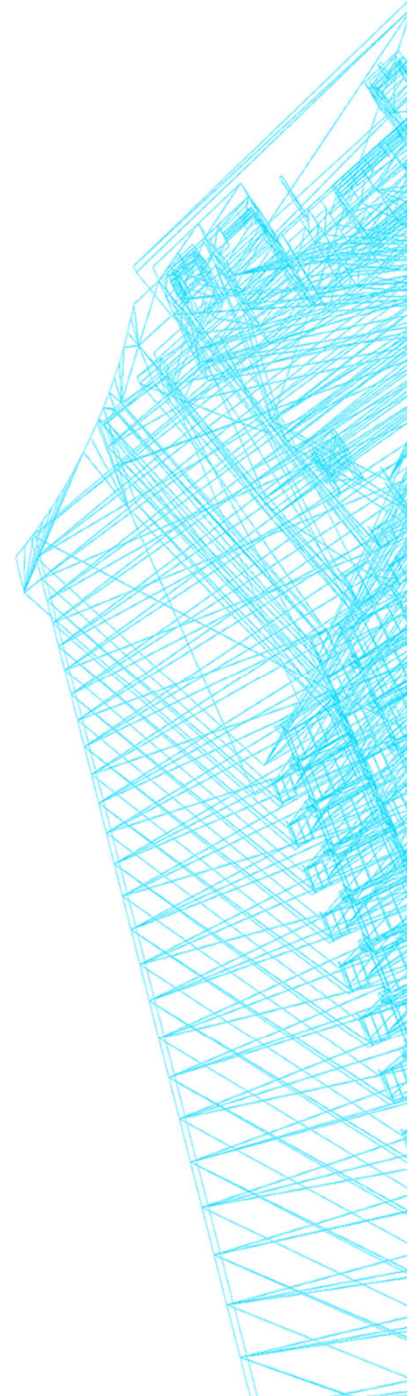


FUN STUFF WITH SMS

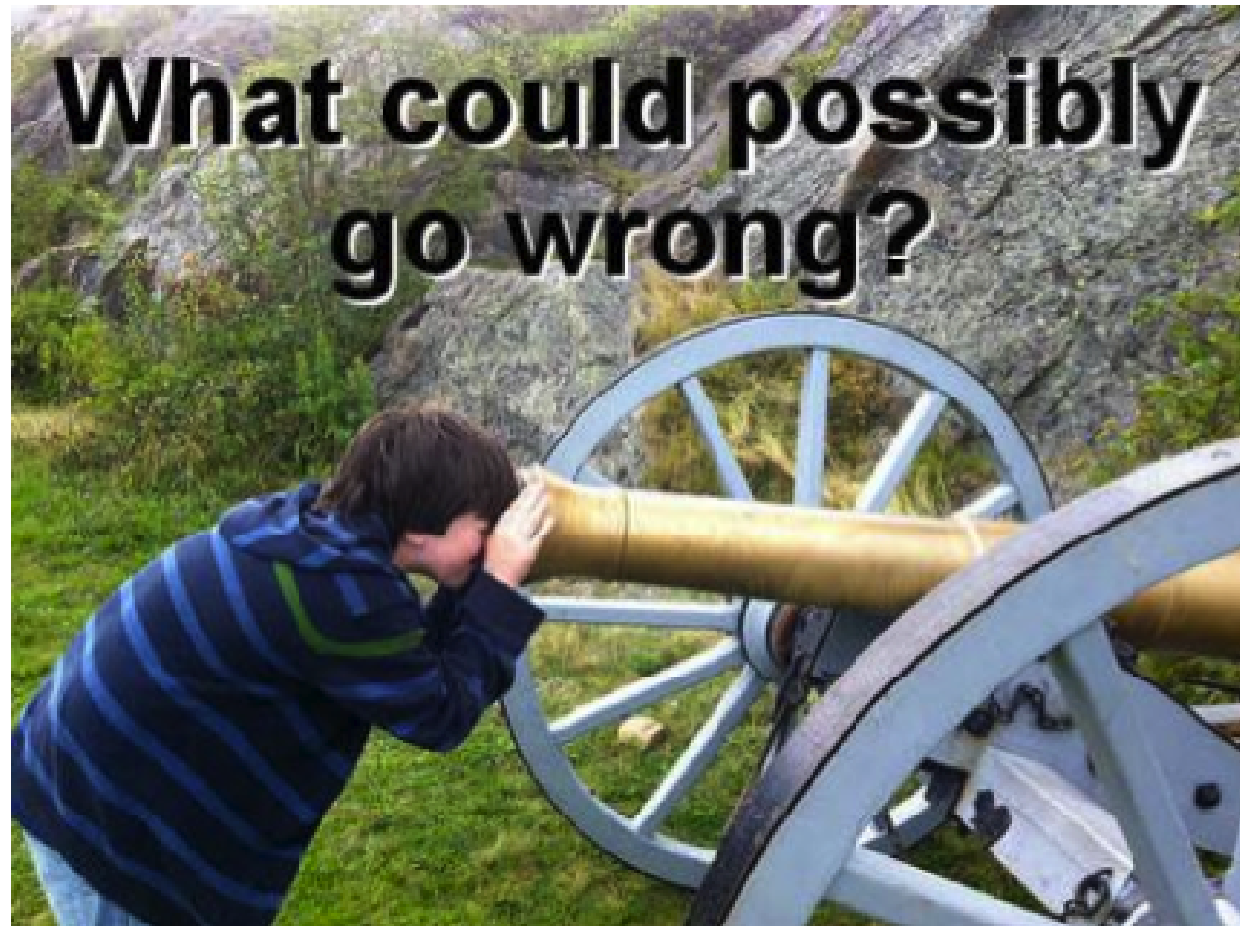
- Service Load (WAP Push)

PID: 0x00

DCS: 0x04 (binary encoding)



WHEN THINGS GO WRONG

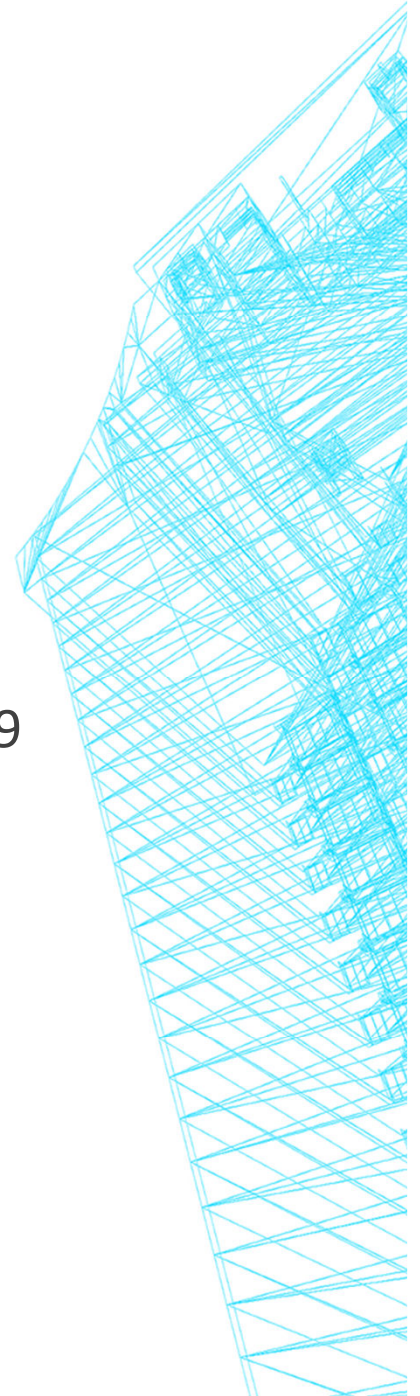


WHEN THINGS GO WRONG

Octets	Description
00	Info about SMSC – here the length is 0, which means that the SMSC stored on SIM should be used.
01	There is no reply path, User Data Header, Status Report Request, Validity Period
00	TP-Message-Reference. The "00" value here lets the phone set the message reference number itself
0B	Address-Length. Length of phone number (11)
91	Type-of-Address. Here it is the international format of the phone number
4421436587F9	The phone number in semi octets – 44123456789
00	PID, none specified
00	DCS, none specified
0B	User-Data-Length. Length of message = length of septets = 11
E8329BFD06DDDF723619	User-Data. These octets represent the message "hello world"

WHEN THINGS GO WRONG

- a) Set the modem in PDU mode: `AT+CMGF=0`
- b) Check if modem is able to process SMS: `AT+CSMS=0`
- c) Send the message: `AT+CMGS=23 >`
`0001000B914421436587F900000BE8329BFD06DDDF723619`

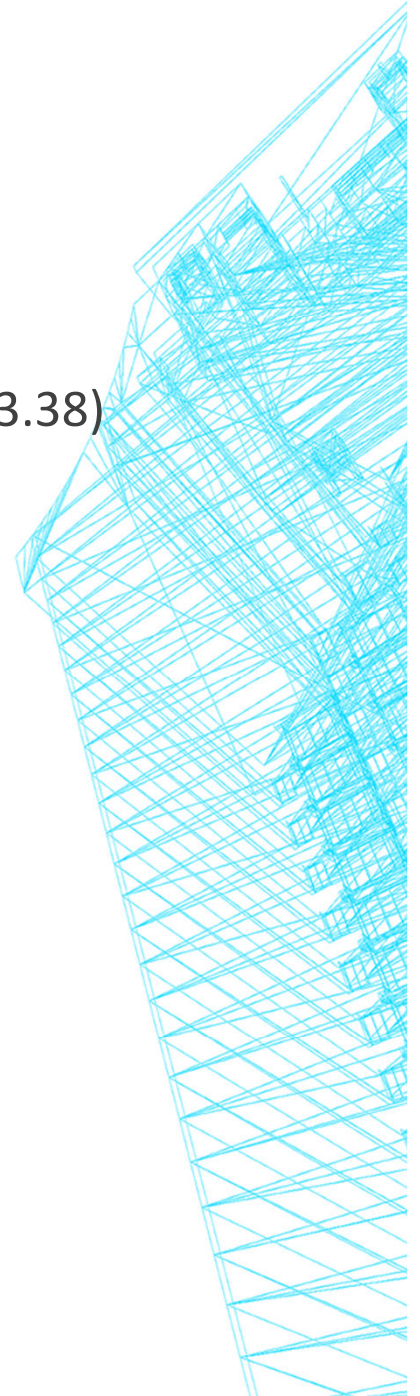


WHEN THINGS GO WRONG

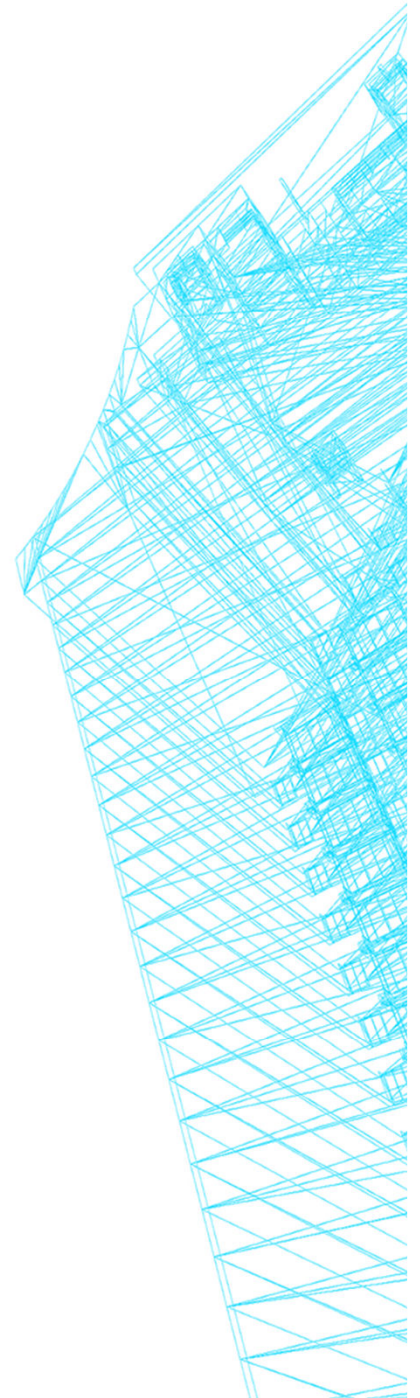
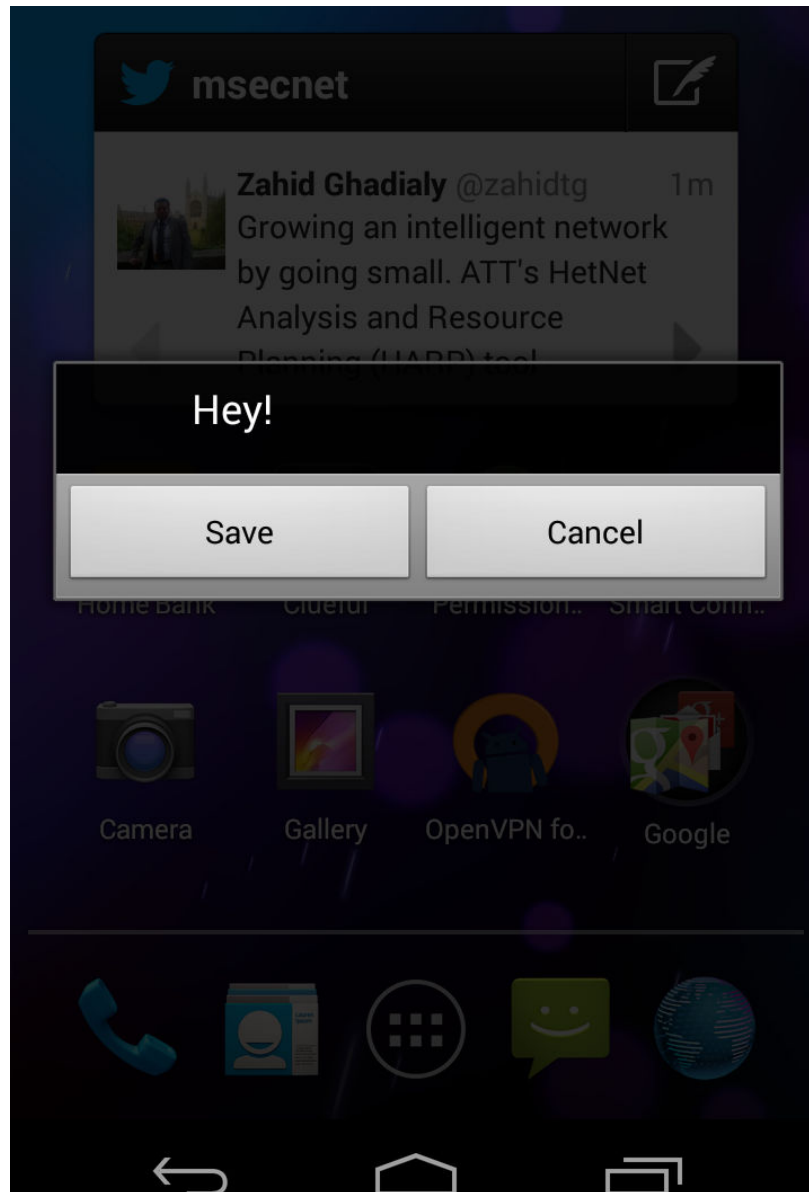
Class 0 /flash message defined in Data Coding Scheme (ETSI GSM 03.38)
DCS = 10 (hex)

When a mobile terminated message is class 0 and the MS has the capability of displaying short messages, the MS shall display the message immediately [...]

The message shall not be automatically stored in the SIM or ME

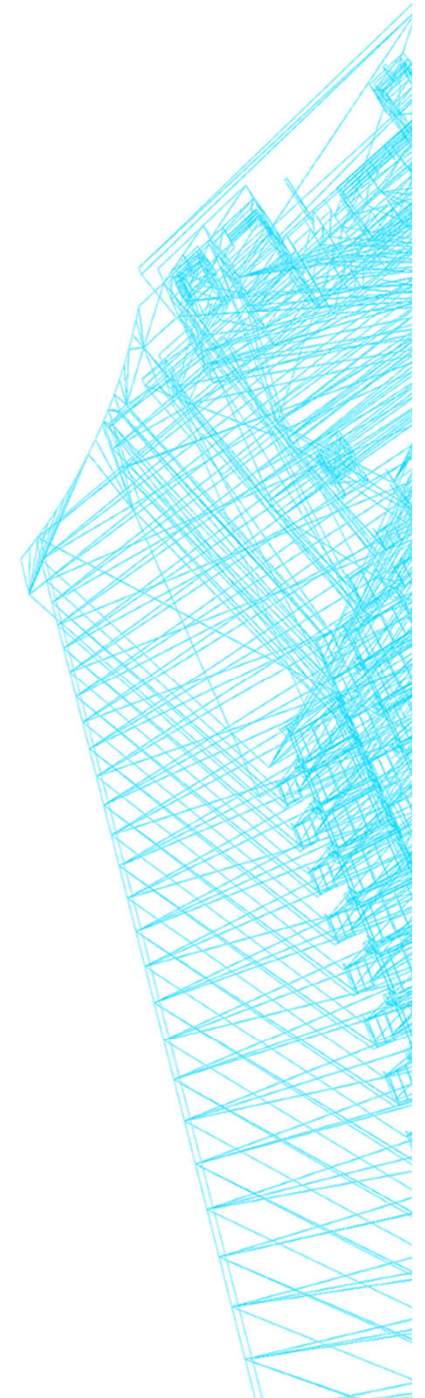
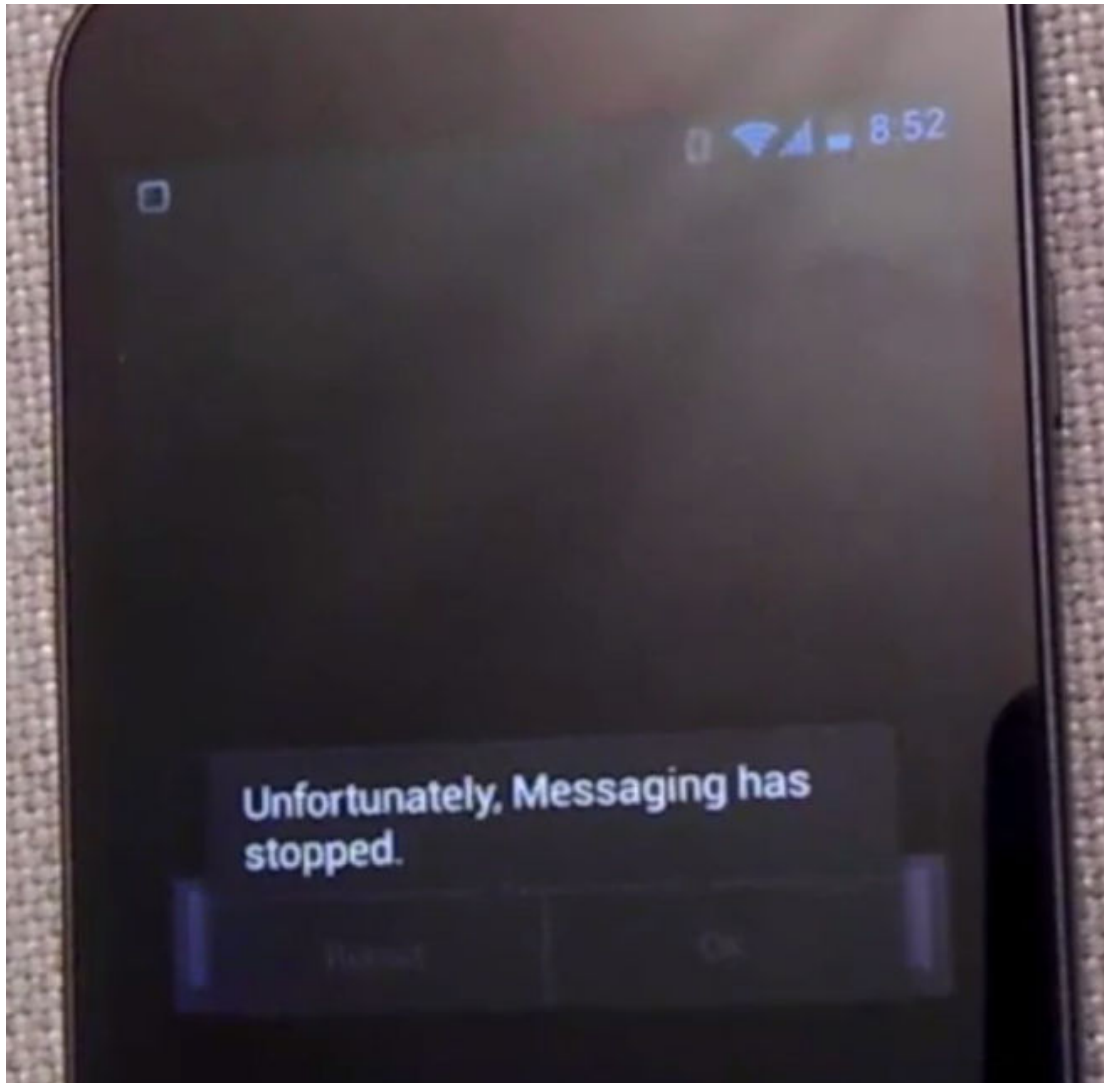


WHEN THINGS GO WRONG



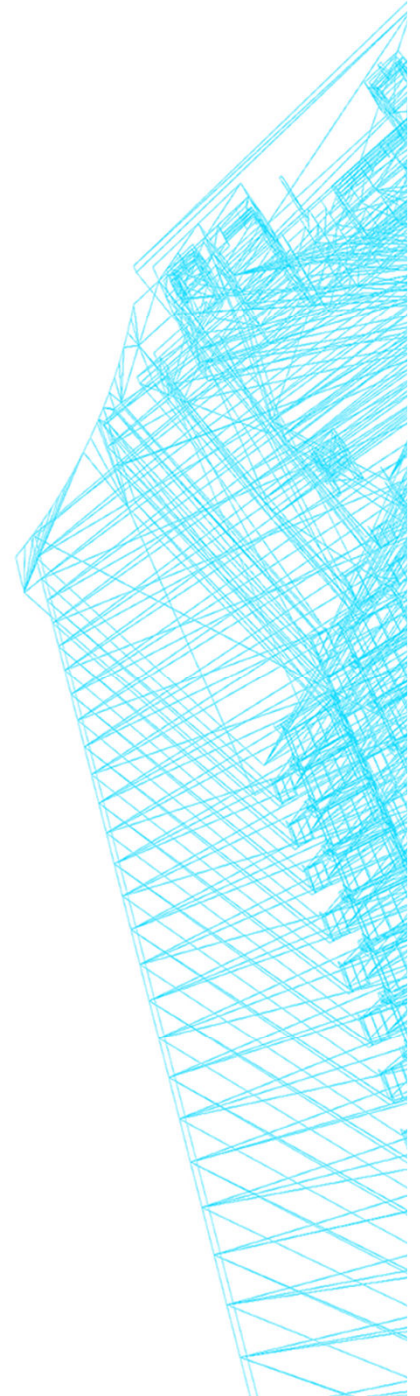
WHEN THINGS GO WRONG

Sending multiple class 0 messages



WHEN THINGS GO WRONG

Sending multiple class 0 messages

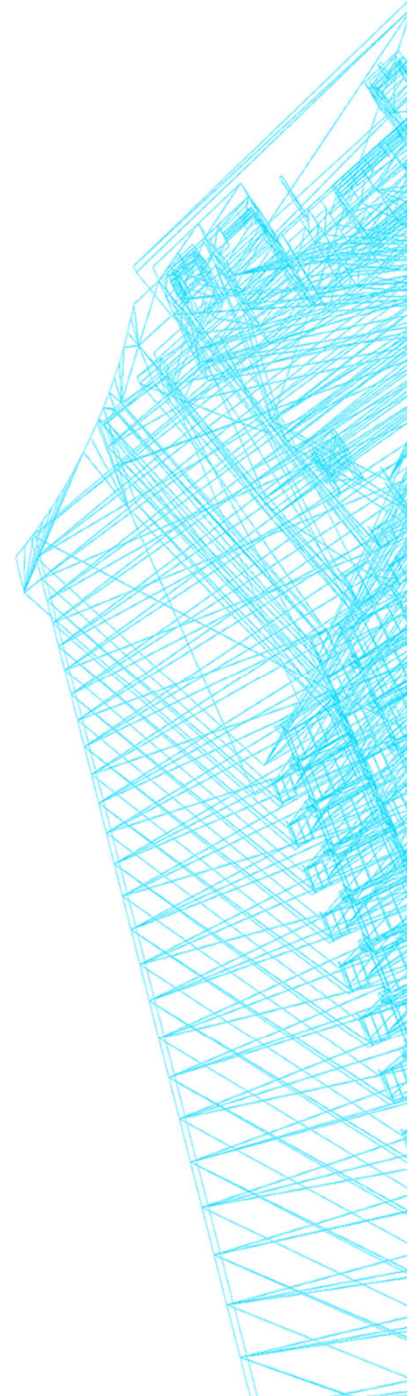


WHEN THINGS GO WRONG

PoC videos:

<https://vimeo.com/80539057>

<https://vimeo.com/69643571>



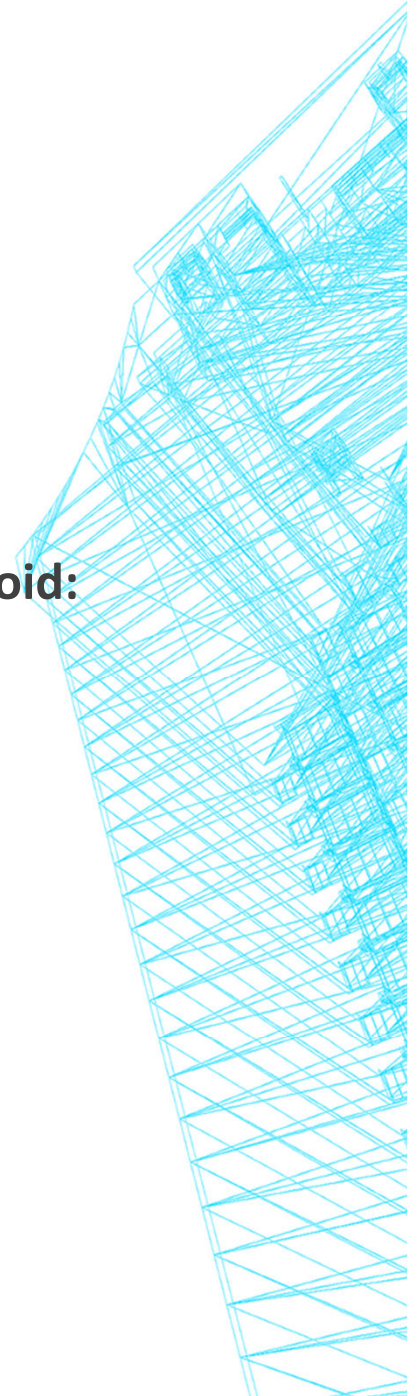
WHEN THINGS GO WRONG

Class 0 message Denial-of-Service

When sending over 30 messages to a Google device running Android:

- Messaging application stops
- Phone reboots
- Radio application restarts, but Internet no longer works

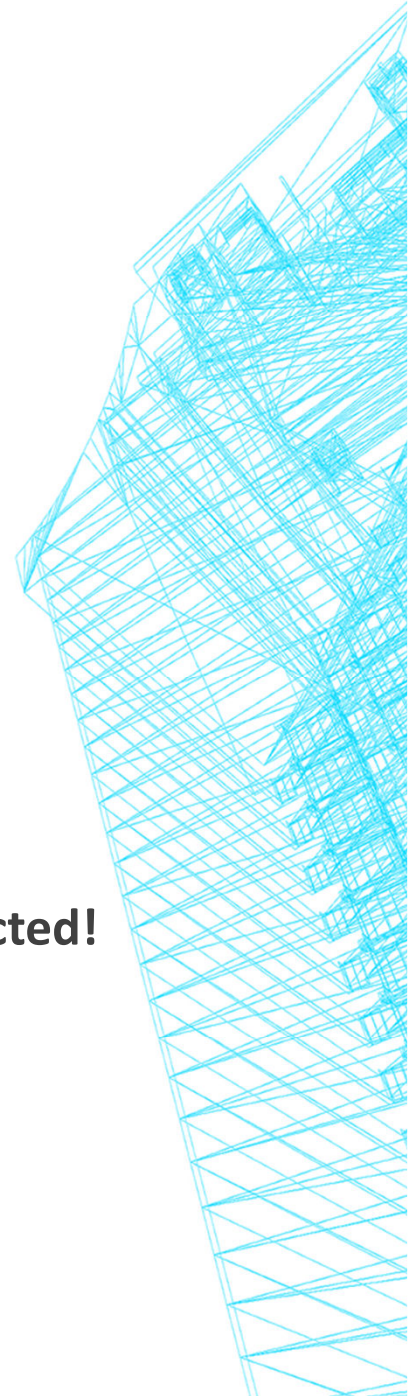
If SIM PIN protection is enabled -> no phone signal, no calls



WHEN THINGS GO WRONG

Class 0 message Denial-of-Service

- Reported to Google over 1 year ago
- Finally got a reply in July
- Still have no idea when / if this will be fixed
- Tested on Galaxy Nexus, Nexus 4 with Android 4.1-4.3
- **Google devices with Android 4.4 KitKat (Nexus 5) are also affected!**



FIX ME!



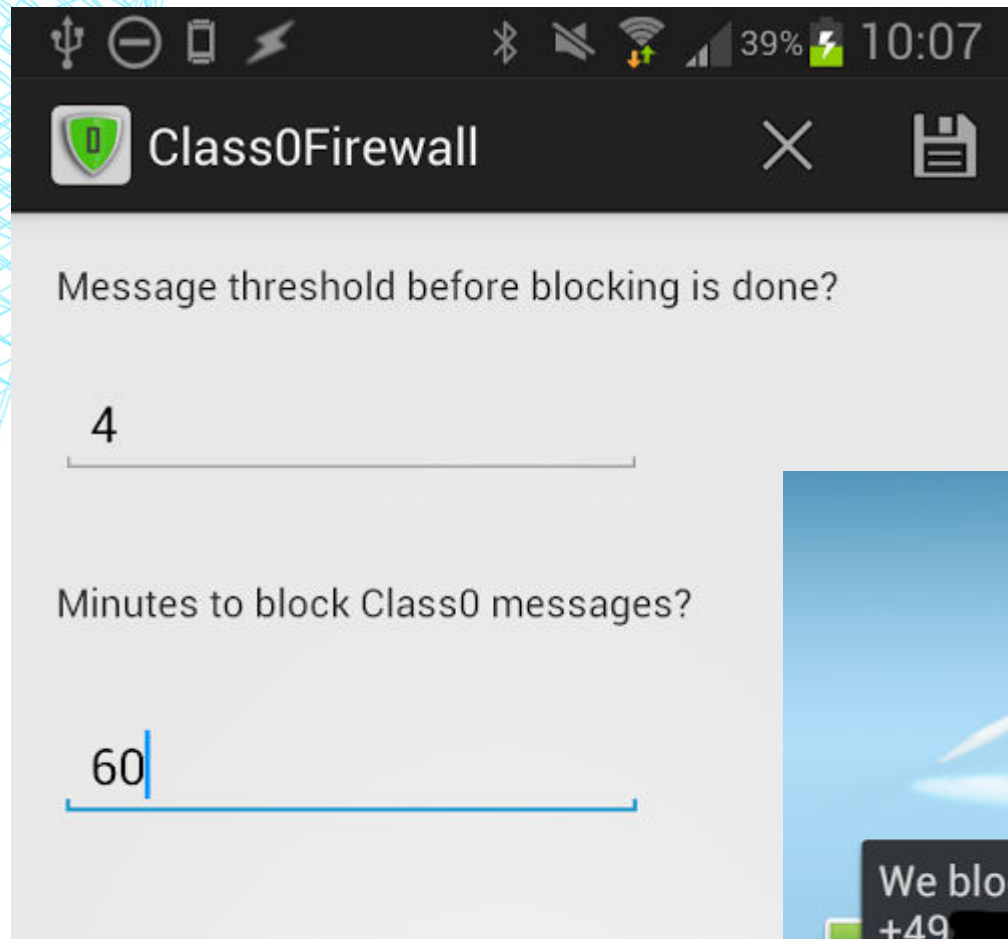


FIX ME!

- Class0Firewall application available in Google Play
- Thanks to Michael Mueller (@c0rnholio)
- You define the threshold, then Class0Firewall will block any incoming “flash” messages

<https://play.google.com/store/apps/details?id=com.silentservices.class0firewall>

FIX ME!



The screenshot shows the 'Class0Firewall' application window. The title bar includes a shield icon, the text 'Class0Firewall', a close button (X), and a save button (floppy disk). The main content area contains two settings: 'Message threshold before blocking is done?' with a value of '4' in a text field, and 'Minutes to block Class0 messages?' with a value of '60' in a text field.

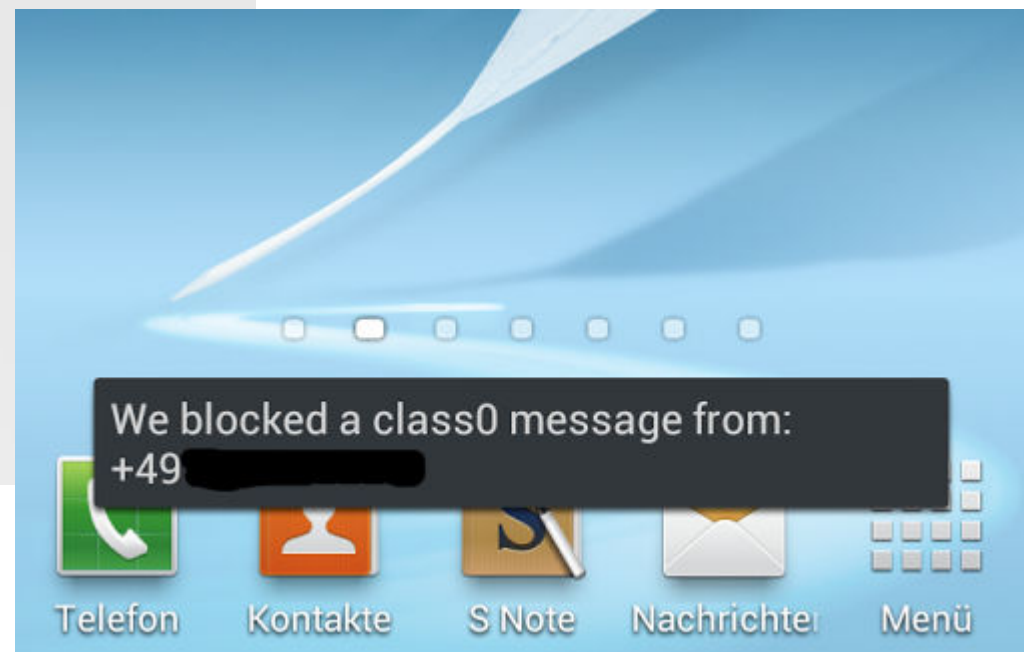
Class0Firewall

Message threshold before blocking is done?

4

Minutes to block Class0 messages?

60





CONCLUSIONS

- Be careful on how you implement SMS
- Check as many messages types as possible
- Sometimes it may not be the number of messages that causes the problem, but the type of message

Thank you!



msecnet



www.m-sec.net



alecu@m-sec.net