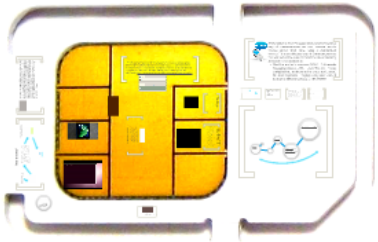
SMS fuzzing - SIM Toolkit Attack

Bogdan Alecu - http://www.m-sec.net



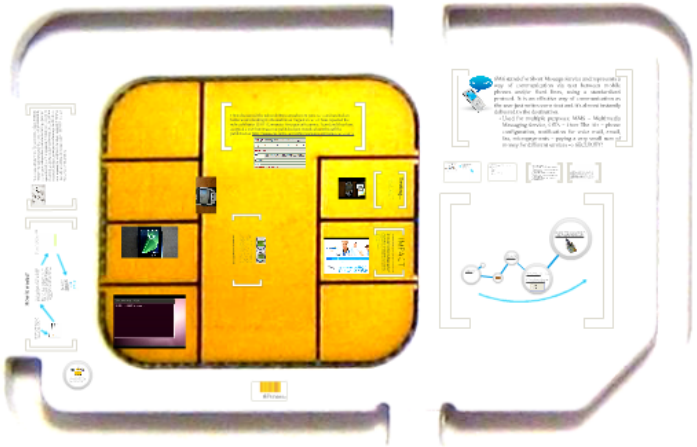
Push SIM from back to detach.

DEEPSEC Mobile

Get more security for your phone.

SMS fuzzing - SIM Toolkit Attack

Bogdan Alecu - http://www.m-sec.net



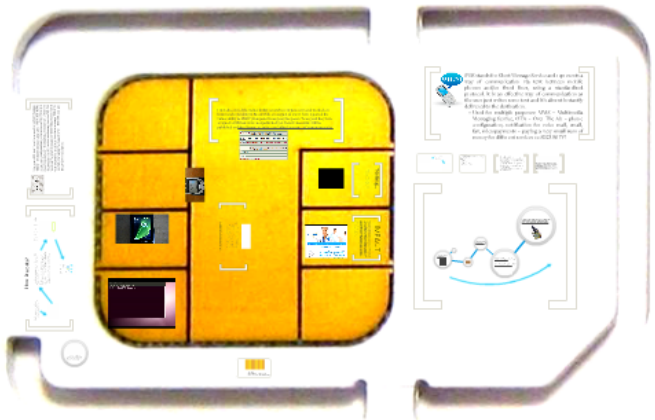
Push SIM from back to detach.

DEEPSEC Mobile

Get more security for your phone.

SMS fuzzing - SIM Toolkit Attack

Bogdan Alecu - http://www.m-sec.net

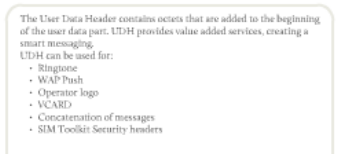


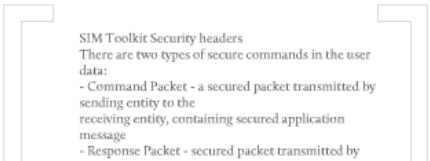
Push SIM from back to detach.

DEEPSEC Mobile

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.

- Used for multiple purposes: MMS – Multimedia Messaging Service, OTA – Over The Air – phone configuration, notification for voice mail, email, fax, micropayments – paying a very small sum of money for different services => SECURITY!

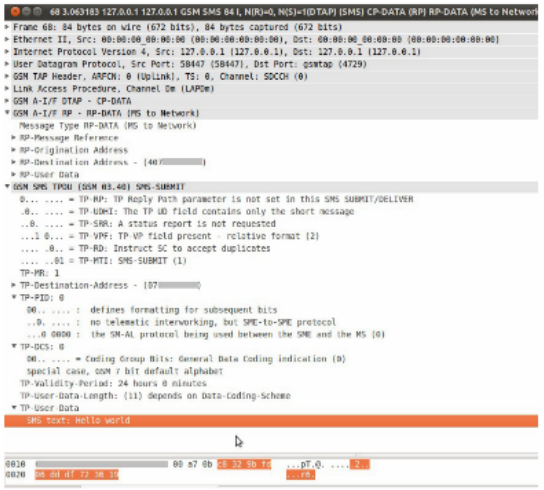

The User Data Header contains octets that are added to the beginning of the user data part. UDH provides value added services, creating a smart messaging.
UDH can be used for:
- Ringtone
- WAP Push
- Operator logo
- VCARD
- Concatenation of messages
- SIM Toolkit Security headers


SIM Toolkit Security headers
There are two types of secure commands in the user data:
- Command Packet - a secured packet transmitted by sending entity to the
receiving entity, containing secured application message
- Response Packet - secured packet transmitted by

“An active MS shall be able to receive a short message TPDU - Transfer protocol data unit - (SMS-DELIVER) at any time, independently of whether or not there is a speech or data call in progress. A report will always be returned to the SC; either confirming that the MS has received the short message, or informing the SC that it was impossible to deliver the short message TPDU to the MS, including the reason why.” ETSI TS 100 901 V7.5.0 (2001-12), page 13

Octet(s)	Description
00	Info about SMSC – here the length is 0, which means that the SMSC stored in the phone should be used.
01	First octet of the SMS-SUBMIT message. It indicates that there is no reply path, User Data Header, Status Report Request, Validity Period, Reject Duplicates. The message type is SMS-SUBMIT.
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	TP-PID, none specified
00	TP-DCS, none specified
0B	TP-User-Data-Length. Length of message = length of septets = 11
E8329BFD06DDDF723619	TP-User-Data. These octets represent the message "hello world".

In order to send this message trough AT commands via a GSM modem, the following steps should be performed:
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 >
0001000B914421436587F900000B
E8329BFD06DDDF723619



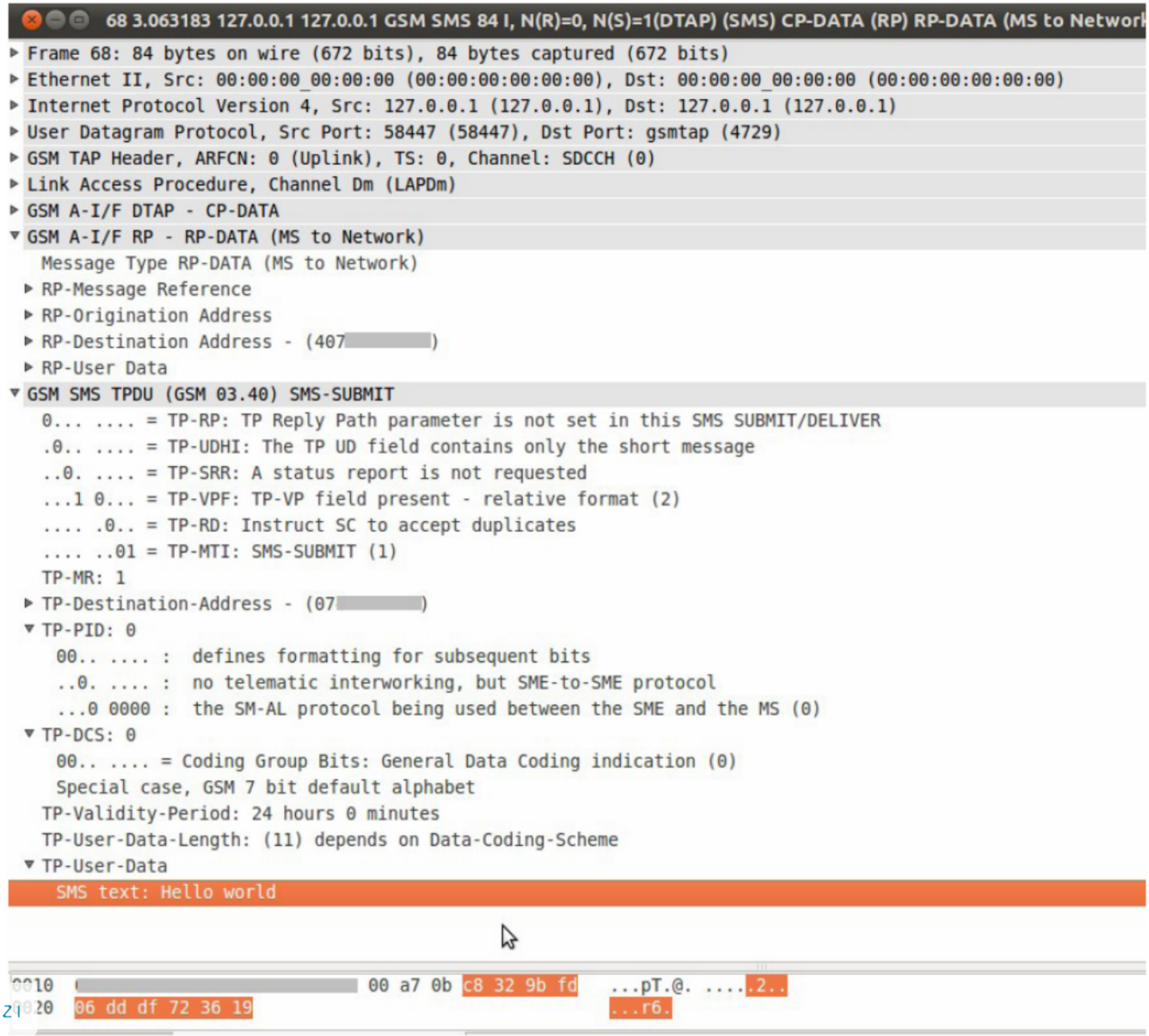
Octet(s)	Description
00	Info about SMSC – here the length is 0, which means that the SMSC stored in the phone should be used.
01	First octet of the SMS-SUBMIT message. It indicates that there is no reply path, User Data Header, Status Report Request, Validity Period, Reject Duplicates. The message type is SMS-SUBMIT.
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	TP-PID, none specified
00	TP-DCS, none specified
0B	TP-User-Data-Length. Length of message = length of septets = 11
E8329BFD06DDDF723619	TP-User-Data. These octets represent the message "hello world".

In order to send this message trough AT commands via a GSM modem, the following steps should be performed:

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 > 0001000B91442143658 7F900000B E8329BFD06DDDF723619


68 3.063183 127.0.0.1 127.0.0.1 GSM SMS 84 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network
Frame 68: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: 58447 (58447), Dst Port: gsmtap (4729)
GSM TAP Header, ARFCN: 0 (Uplink), TS: 0, Channel: SDCCH (0)
Link Access Procedure, Channel Dm (LAPDm)
GSM A-I/F DTAP - CP-DATA
GSM A-I/F RP - RP-DATA (MS to Network)
Message Type RP-DATA (MS to Network)
RP-Message Reference
RP-Origination Address
RP-Destination Address - (407
RP-User Data
GSM SMS TPDU (GSM 03.40) SMS-SUBMIT
0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
.0.. .... = TP-UDHI: The TP UD field contains only the short message
..0. .... = TP-SRR: A status report is not requested
...1 0... = TP-VPF: TP-VP field present - relative format (2)
.... .0.. = TP-RD: Instruct SC to accept duplicates
.... ..01 = TP-MTI: SMS-SUBMIT (1)
TP-MR: 1
TP-Destination-Address - (07
TP-PID: 0
00.. .... : defines formatting for subsequent bits
..0. .... : no telematic interworking, but SME-to-SME protocol
...0 0000 : the SM-AL protocol being used between the SME and the MS (0)
TP-DCS: 0
00.. .... = Coding Group Bits: General Data Coding indication (0)
Special case, GSM 7 bit default alphabet
TP-Validity-Period: 24 hours 0 minutes
TP-User-Data-Length: (11) depends on Data-Coding-Scheme
TP-User-Data
SMS text: Hello world
0010 00 a7 0b c8 32 9b fd ...pT.@. ....2..
0020 06 dd df 72 36 19 ...r6.

The User Data Header contains octets that are added to the beginning of the user data part. UDH provides value added services, creating a smart messaging.
UDH can be used for:

- Ringtone
- WAP Push
- Operator logo
- VCARD
- Concatenation of messages
- SIM Toolkit Security headers

SIM Toolkit Security headers

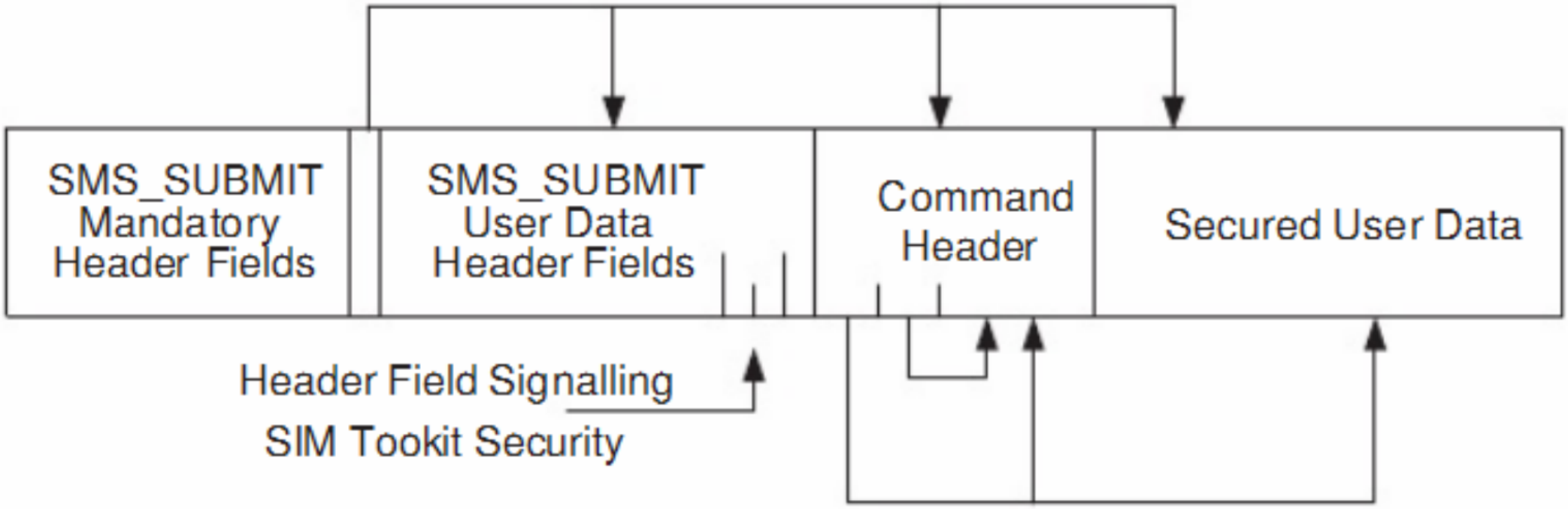
There are two types of secure commands in the user data:

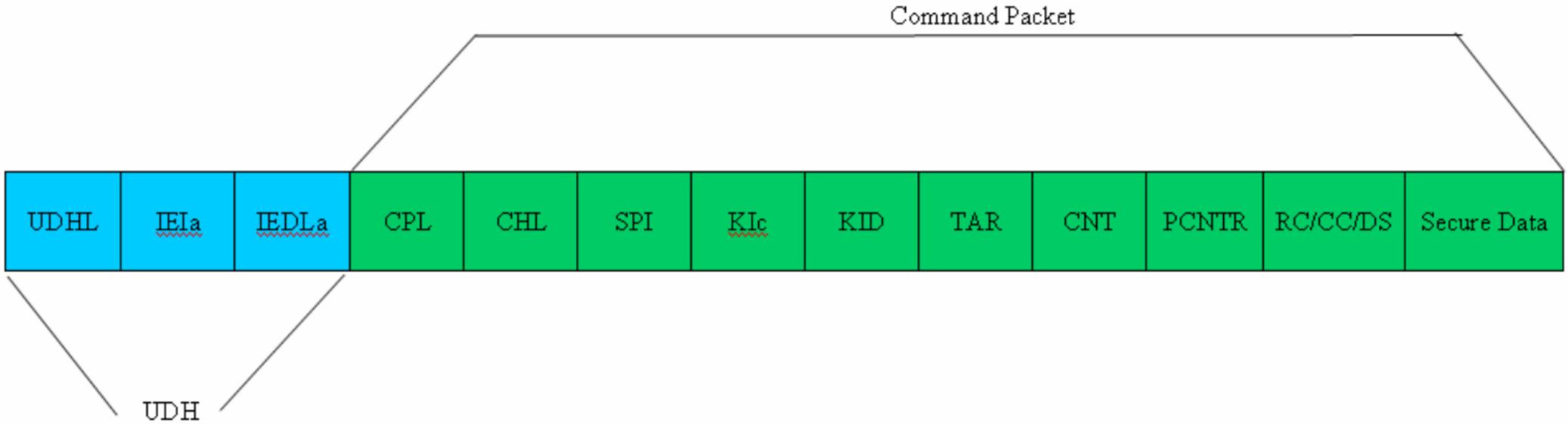
- Command Packet - a secured packet transmitted by sending entity to the receiving entity, containing secured application message
- Response Packet - secured packet transmitted by receiving entity to the sending entity, containing secured response and possibly application data

n the SIM

quence Integrity counter

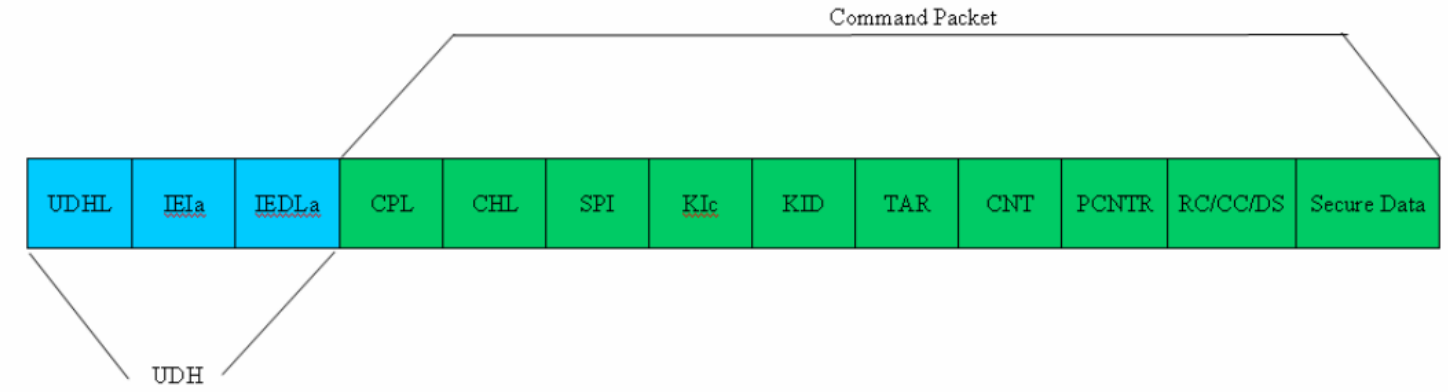
umber of padding octets used for ciphering at t



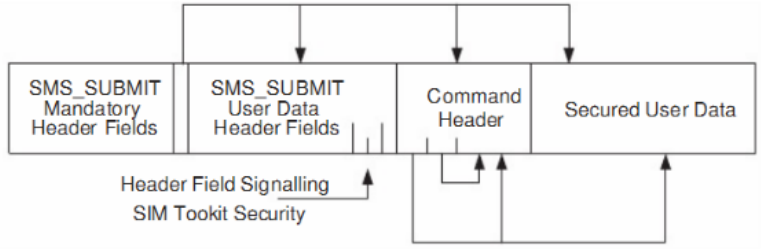


ength (CPL) – shall indicate the number of octets from and including the Command
the end of the Secured Data, including any padding octets required for ciphering.
ength (CHL) – the number of octets from and including the SPI to the end of the

ndicator (SPI) – defines the security level applied to the input and output message
ifier (KIc) – Key and algorithm Identifier for ciphering



Command Packet Length (CPL) – shall indicate the number of octets from and including the Command Header Identifier to the end of the Secured Data, including any padding octets required for ciphering.
Command Header Length (CHL) – the number of octets from and including the SPI to the end of the RC/CC/DS
Security Parameter Indicator (SPI) – defines the security level applied to the input and output message
Ciphering Key Identifier (KIc) – Key and algorithm Identifier for ciphering
Key Identifier (KID) – Key and algorithm Identifier for Redundancy Check (RC) / Cryptographic Checksum (CC) / Digital Signature (DS)
Toolkit Application Reference (TAR) – is part of the 23.048 header that identifies and triggers the Over The Air (OTA) feature, which is an application on the SIM
Counter (CNTR) – Replay detection and Sequence Integrity counter
Padding counter (PCNTR) – indicates the number of padding octets used for ciphering at the end of the secured data

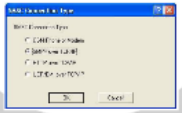


TOOLS USED

Gemalto GemPC Twin reader for accessing the SIM
SIMinfo Python script for reading the SIM files
https://gsm.tsaitgaist.info/doku.php?id=siminfo

Wireshark developement release 1.6.0.rc2 compiled and patched with GSMTAP and SIMCARD in order to decode GSM traffic and SIM access. Instructions on how to patch it can be found at
http://lists.osmocom.org/trac/wiki/rc1_gsmtap

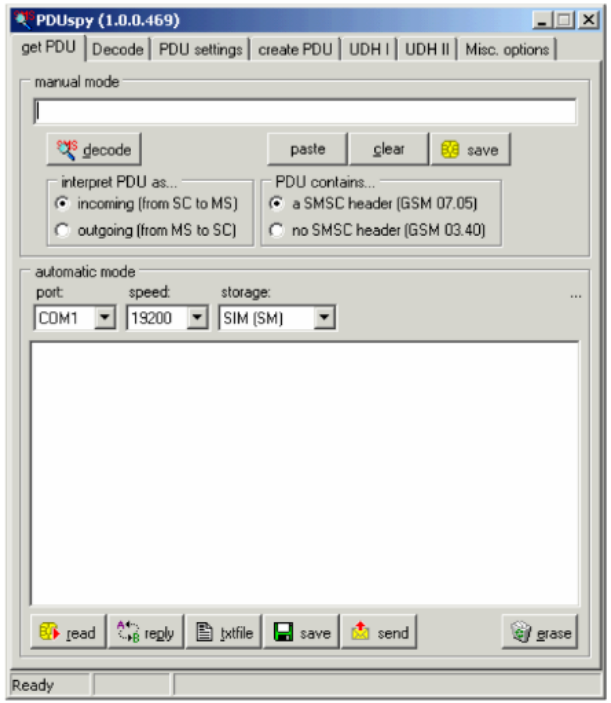
NowSMS Gateway for an easy way of sending messages and connection to an SMS provider by SMPP - http://www.nowsms.com/download-free-trial

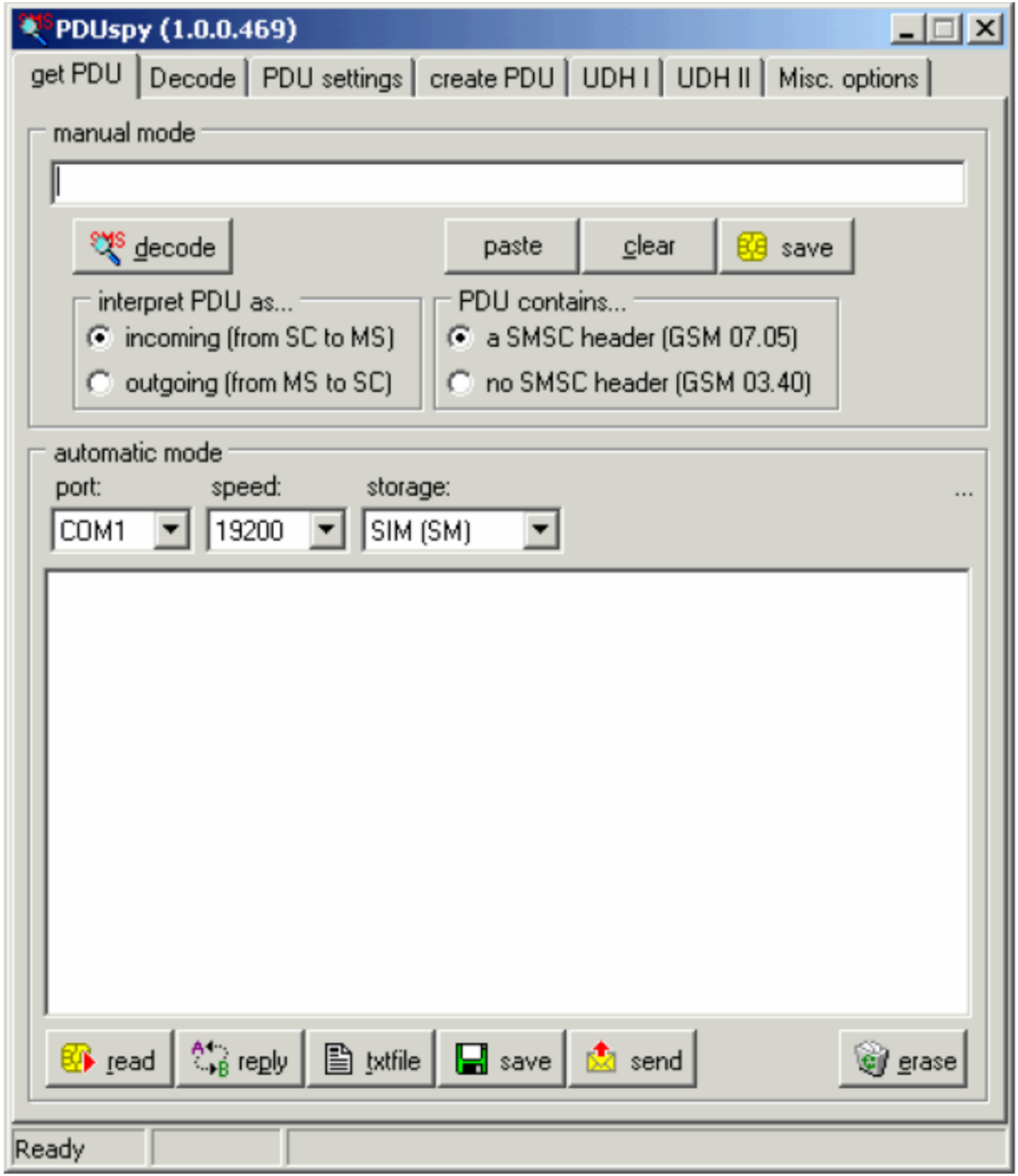


TOOLS USED

TOOLS USED

PDUspy – for better understating the incoming message and building my own crafted message (available at http://www.nobbi.com/pduspy.html)




PDUspy (1.0.0.469)
get PDU
Decode
PDU settings
create PDU
UDH I
UDH II
Misc. options
manual mode
decode
paste
clear
save
interpret PDU as...
incoming (from SC to MS)
outgoing (from MS to SC)
PDU contains...
a SMSC header (GSM 07.05)
no SMSC header (GSM 03.40)
automatic mode
port:
speed:
storage:
COM1
19200
SIM (SM)
read
reply
txtfile
save
send
erase
Ready

Nokia 3310 with F-BUS USB cable – I bought the cable on E-Bay

dct3tap command line utility (Linux) to capture the GSM Um and SIM-ME interfaces from a Nokia DCT3 phone (eg. 3310) and forward via GSMTAP to the Wireshark protocol analyzer. This tool has been created by Duncan Salerno and is available on http://bb.osmocom.org/trac/wiki/dct3-gsmtap

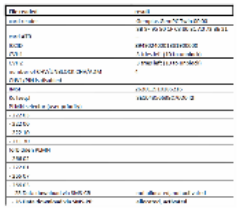
Wireshark development release 1.6.0.rc2 compiled and patched with GSMTAP and SIMCARD in order to decode GSM traffic and SIM access. Instructions on how to patch it can be found at http://bb.osmocom.org/trac/wiki/dct3-gsmtap

NowSMS Gateway for an easy way of sending messages and connection to an SMS provider by SMPP - http://www.nowsms.com/download-free-trial

Gemalto GemPC Twin reader for accessing the SIM
SIMinfo Python script for reading the SIM files
https://gsm.tsaitgaist.info/doku.php?id=siminfo

How it works?

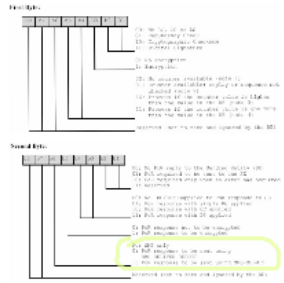
First of all, it is important that the SIM to have the service "data download via SMS Point-to-Point allocated and active. Also the SIM must have a SIM Toolkit Application on it in order to work.



The type of message sent is addressed directly to the SIM, by setting the PID to 0x7F,corresponding to USIM Data Download, as you will see below. Also the DCS has to be a class 2 message type. According to GSM 11.14 here is what happens when these are set:

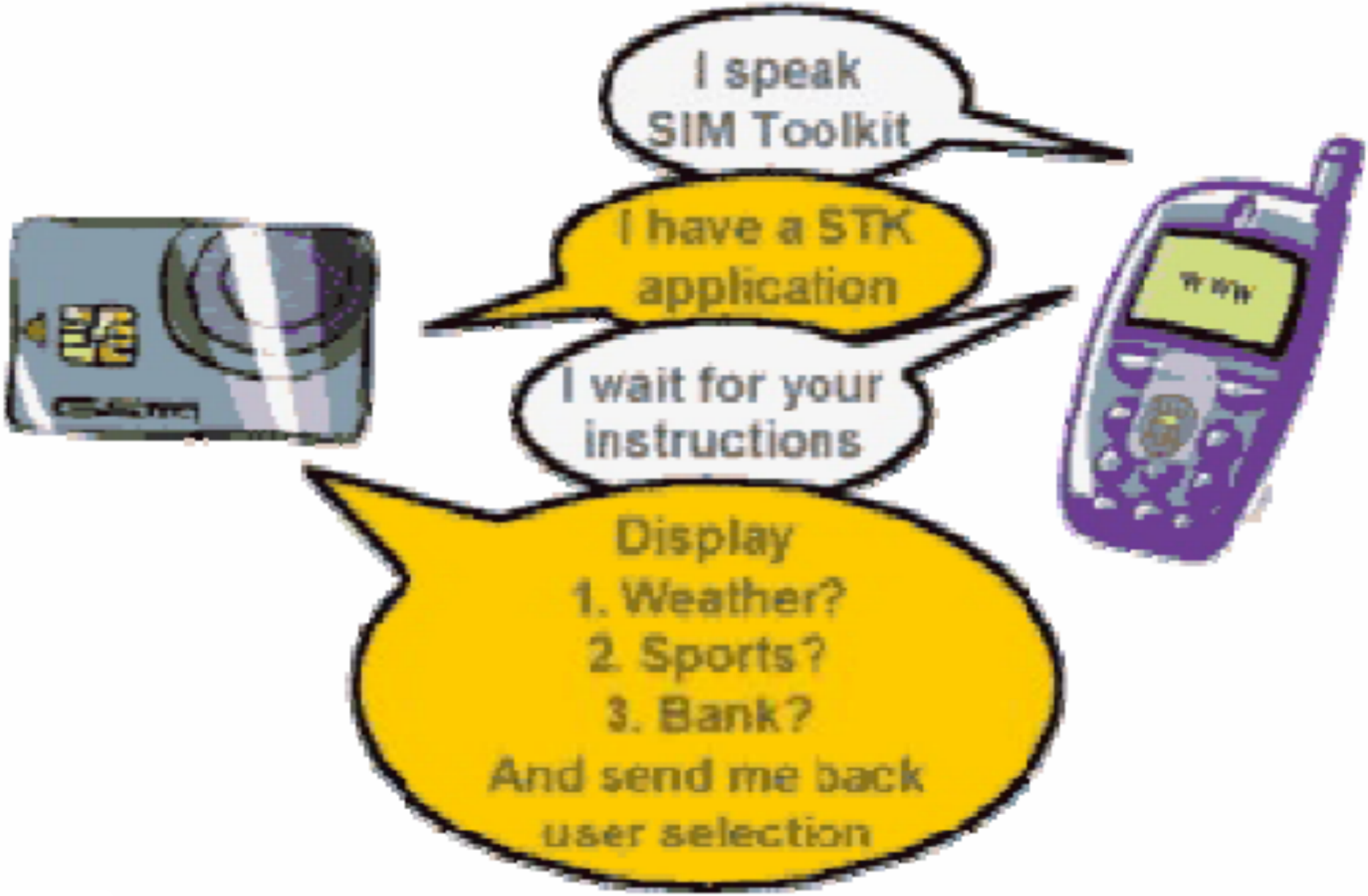
If the service "data download via SMS Point-to-point" is allocated and activated in the SIM Service Table, then the ME shall follow the procedure below:
- When the ME receives a Short Message with protocol identifier = SIM data download, and data coding scheme = class 2 message, then the ME shall pass the message transparently to the SIM using the ENVELOPE (SMS-PP DOWNLOAD) command.
- The ME shall not display the message, or alert the user of a short message waiting. In other words, the phone will not display anything and the user will not be aware of this attack.

Let's have a look at the secure command SMS header. One of its components is the Security Parameter Indicator (SPI). SPI is 2 octets long and it has the following structure:



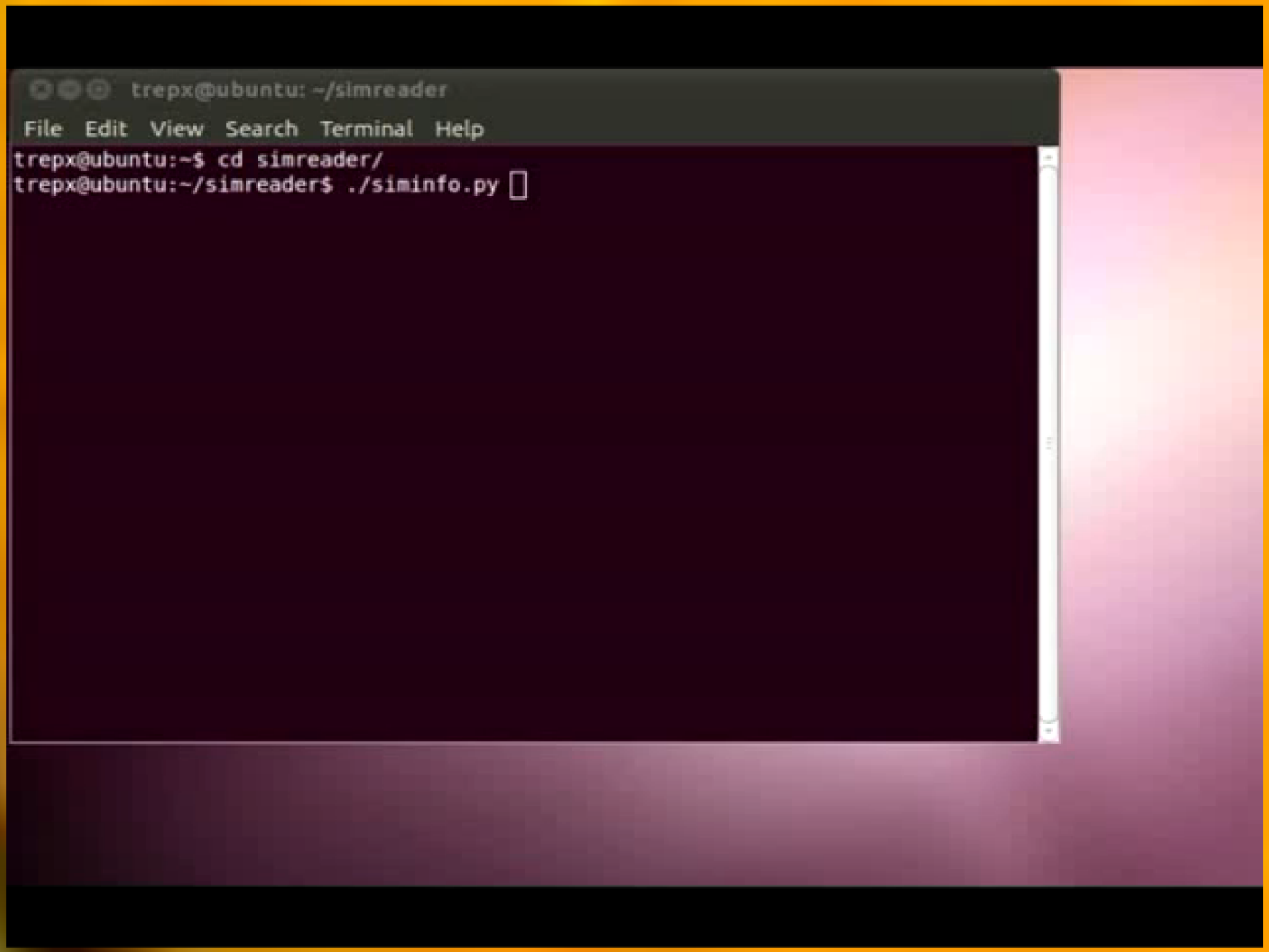
First of all, it is important that the SIM to have the service “data download via SMS Point-to-Point allocated and active. Also the SIM must have a SIM Toolkit Application on it in order to work.

SIM Application Toolkit provides Value Added Services for the mobile operators. Basically is a set of commands written on the SIM card which helps the card to communicate with the mobile device, making it possible to initiate commands independently of the network or handset.


I speak
SIM Toolkit
I have a STK
application
I wait for your
instructions
Display
1. Weather?
2. Sports?
3. Bank?
And send me back
user selection

SIM Application Toolkit provides Value Added Services for the mobile operators. Basically is a set of commands written on the SIM card which helps the card to communicate with the mobile device, making it possible to initiate commands independently of the network or handset.

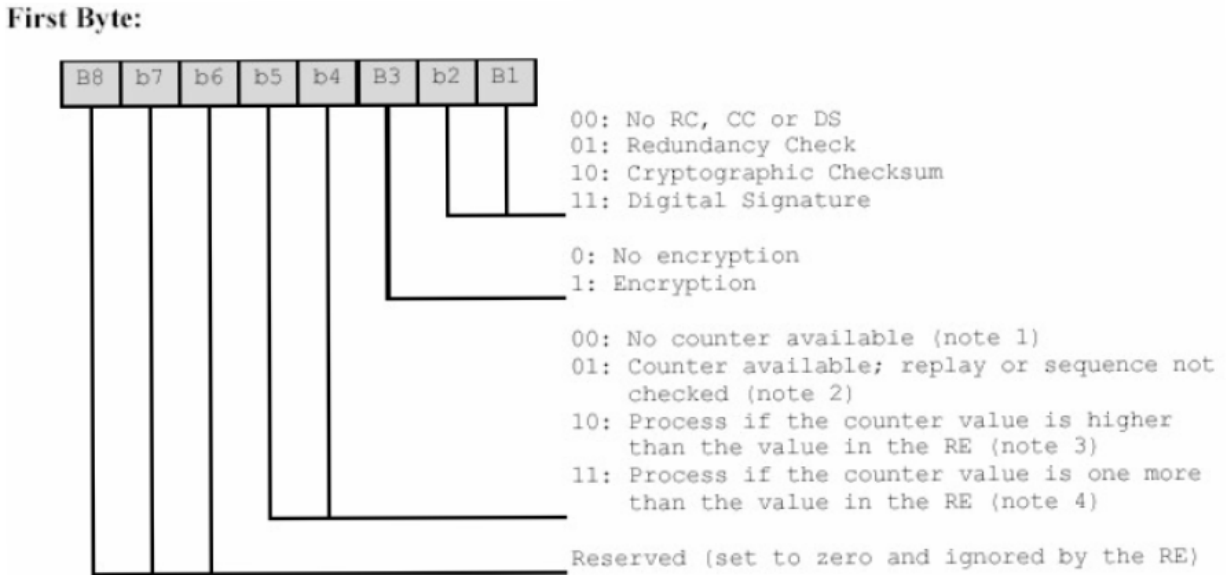
File readed	result
card reader	Gemplus GemPC Twin 00 00
card ATR	3B 9F 95 80 1F C3 80 31 A0 73 BE 21 ...
ICCID	8949024000138190000O
CVH1	3 tries left (10 to unblock)
CVH2	3 tries left (10 to unblock)
number of CHV/UNBLOCK CHV/ADM	4
CHV1/PIN is disabled	
IMSI	262011910185216
Kc [seq.]	3E104356638C70D0 [2]
PLMN selector (user priority)	
- 222 03	
- 222 06	
- 222 10	
- 211 30	
forbidden PLMN	
- 266 02	
- 222 01	
- 266 07	
- 266 03	
- 25 Data download via SMS-CB	not allocated, not activated
- 26 Data download via SMS-PP	**allocated, activated**


trepx@ubuntu: ~/simreader
File Edit View Search Terminal Help
trepx@ubuntu:~$ cd simreader/
trepx@ubuntu:~/simreader$ ./siminfo.py

The type of message sent is addressed directly to the SIM, by setting the PID to 0x7F,corresponding to USIM Data Download, as you will see below. Also the DCS has to be a class 2 message type. According to GSM 11.14 here is what happens when these are set:

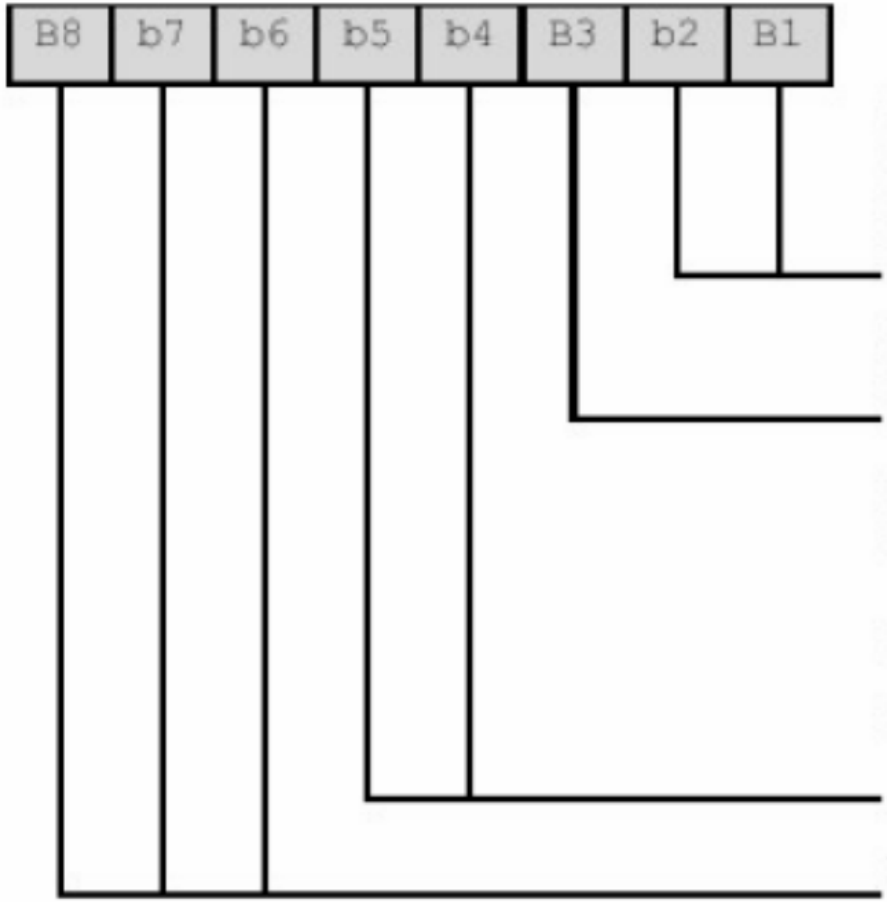
If the service "data download via SMS Point-to-point" is allocated and activated in the SIM Service Table, then the ME shall follow the procedure below:
- When the ME receives a Short Message with protocol identifier = SIM data download, and data coding scheme = class 2 message, then the ME shall pass the message transparently to the SIM using the ENVELOPE (SMS-PP DOWNLOAD) command.
- The ME shall not display the message, or alert the user of a short message waiting. In other words, the phone will not display anything and the user will not be aware of this attack.

Let's have a look at the secure command SMS header. One of its components is the Security Parameter Indicator (SPI). SPI is 2 octets long and it has the following structure:



ets long and it has the following structure:

First Byte:



00: No RC, CC or DS
01: Redundancy Check
10: Cryptographic Checksum
11: Digital Signature

0: No encryption
1: Encryption

00: No counter available (note 1)
01: Counter available; replay or sequence not checked (note 2)
10: Process if the counter value is higher than the value in the RE (note 3)
11: Process if the counter value is one more than the value in the RE (note 4)

Reserved (set to zero and ignored by the RE)

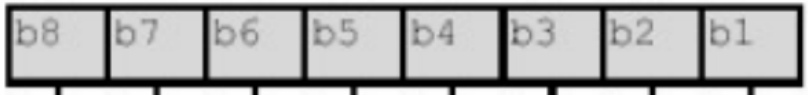
Second Byte:

00: No PoR reply to the Sending Entity (SE)

than the value in the RE (note 4)

Reserved (set to zero and ignored by the RE)

Second Byte:



00: No PoR reply to the Sending Entity (SE)
01: PoR required to be sent to the SE
10: PoR required only when an error has occurred
11: Reserved

00: No RC/CC/DSapplied to PoR response to SE
01: PoR response with simple RC applied
10: PoR response with CC applied
11: PoR response with DS applied

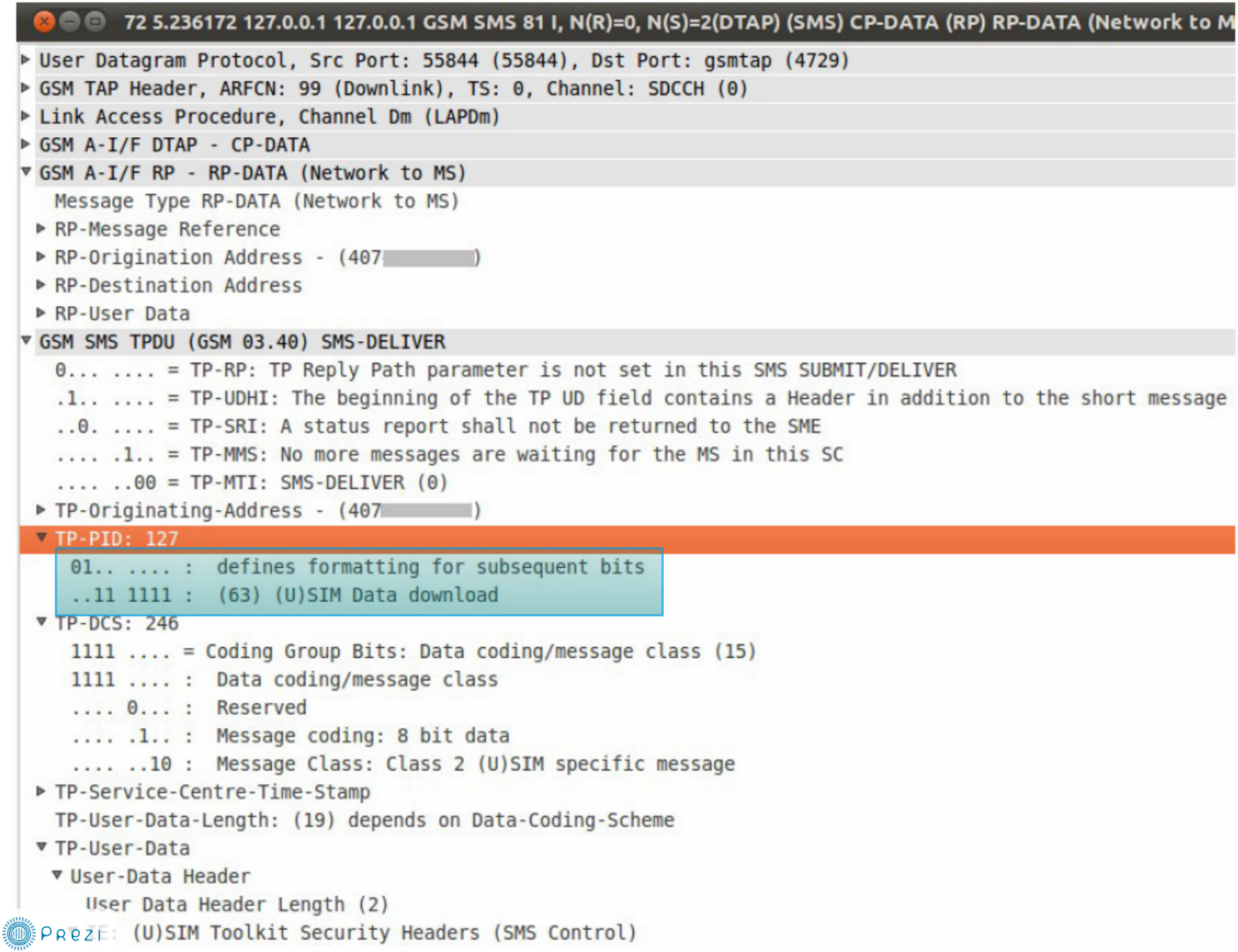
0: PoR response not to be encrypted
1: PoR response to be encrypted

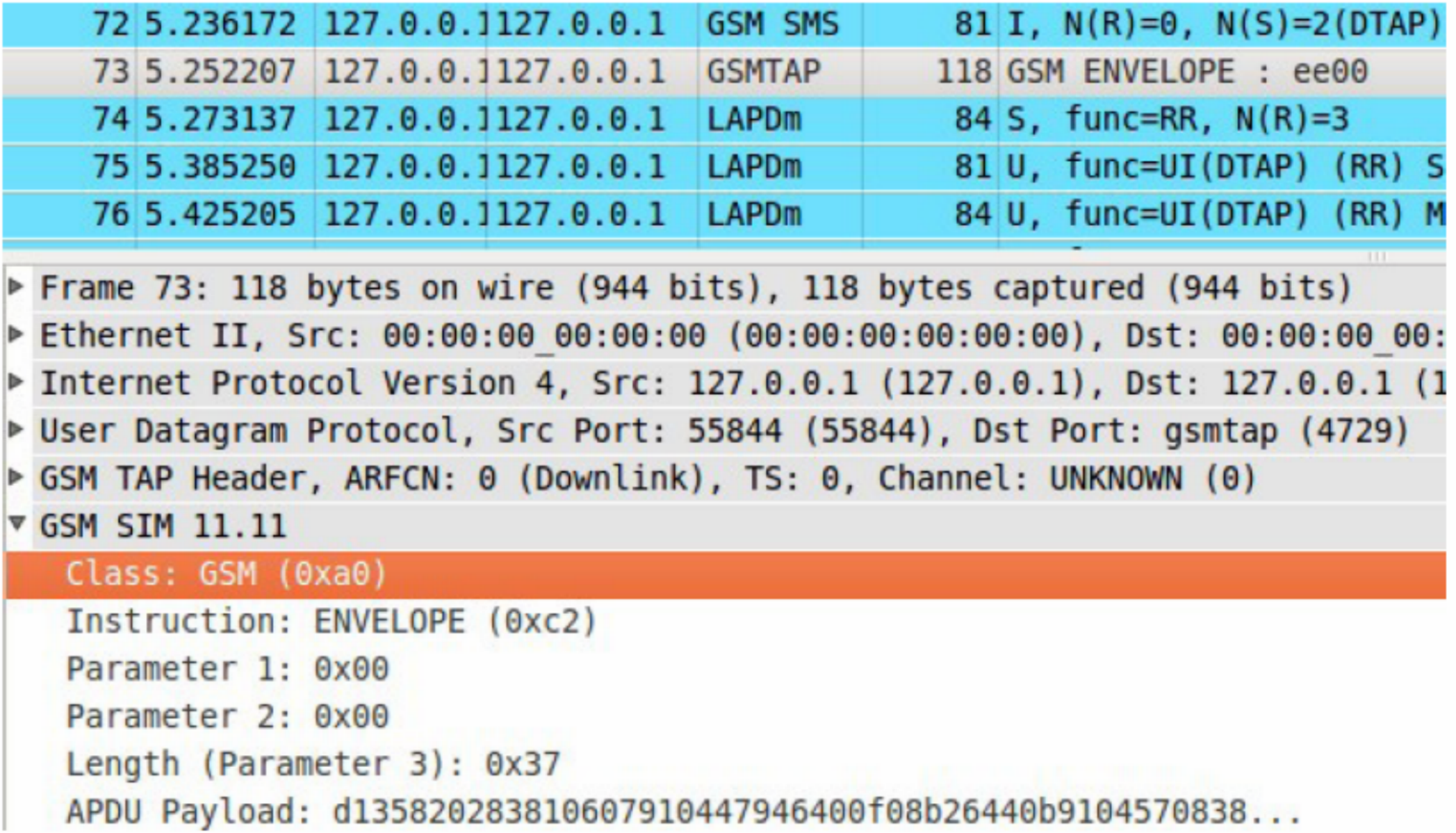
For SMS only
0: PoR response to be sent using SMS-DELIVER-REPORT
1: PoR response to be sent using SMS-SUBMIT

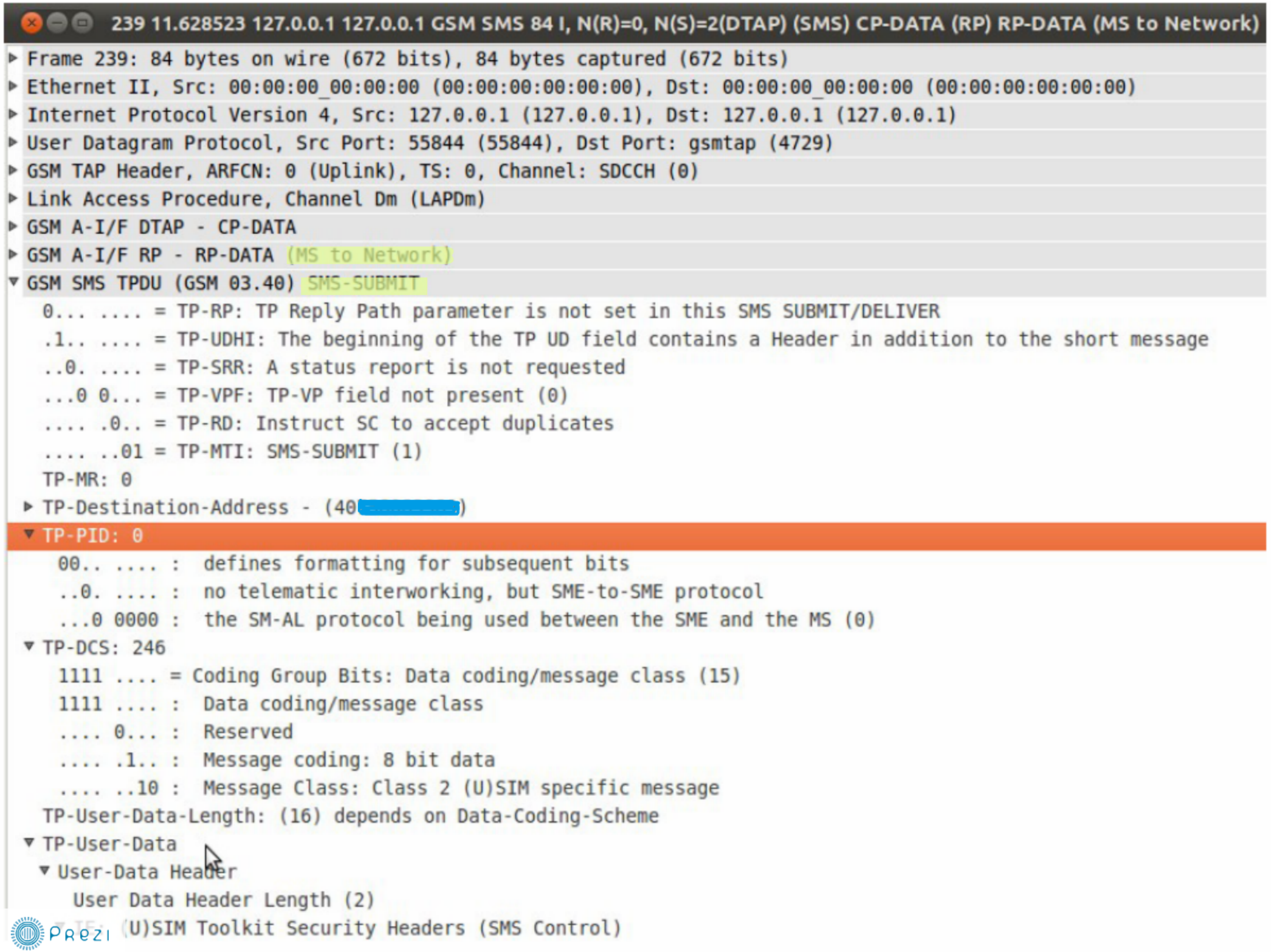
Reserved (set to zero and ignored by the RE)

The vulnerability is possible due to the second byte: here you can set how the proof of receipt (PoR) to be sent – via SMS-DELIVER-REPORT or SMS-SUBMIT. When is set to be on SMS-SUBMIT the phone will try to send back a reply to the originated sender.

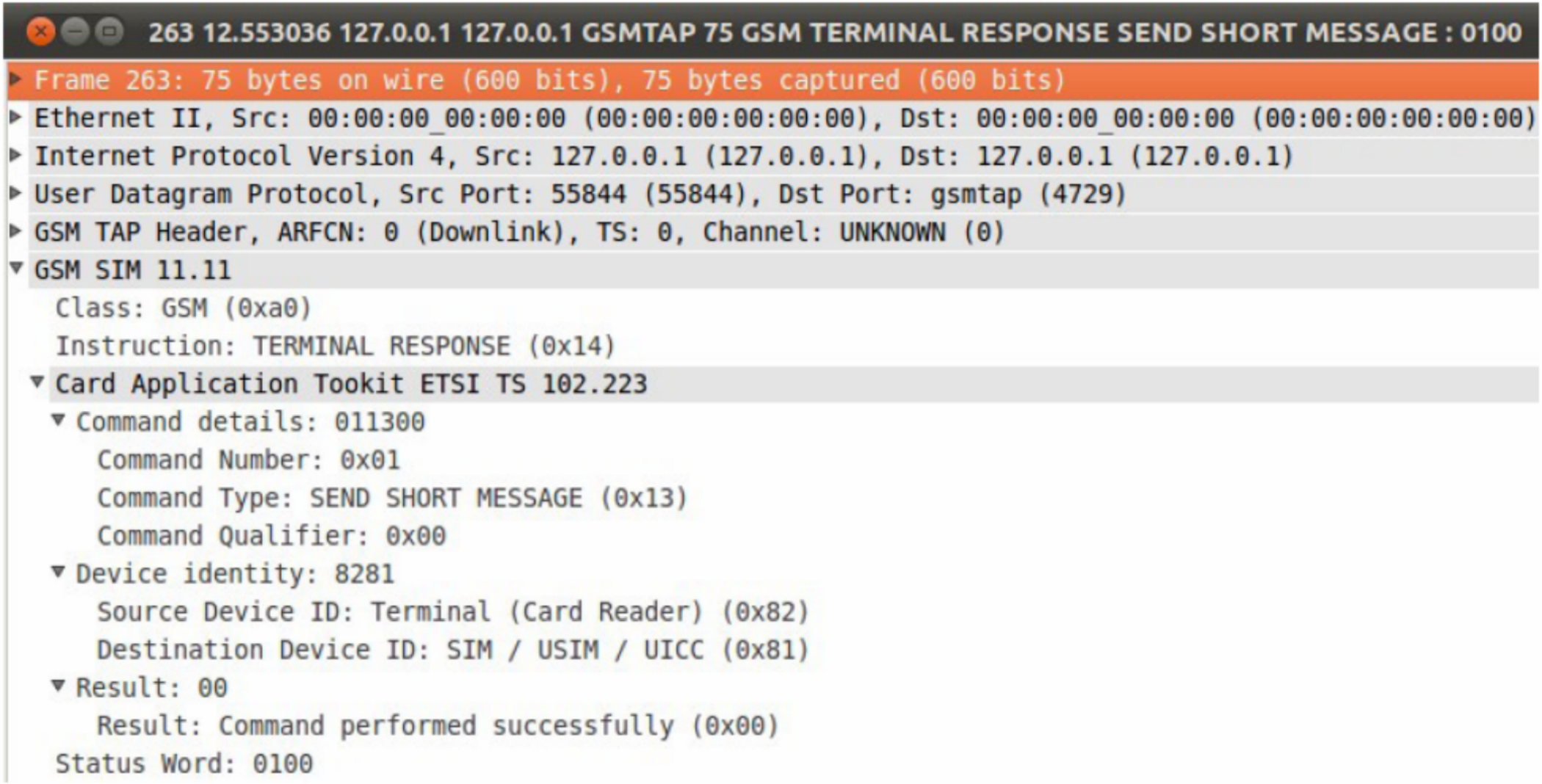
If we set it to acknowledge the receipt via DELIVER REPORT, the phone will report to the network the status of the message. Since we don't have valid entries for the KIc, KID,TAR, the result of the STK command is an error so the report will be an error. The sending SMSC then thinks that the phone hasn't received the message and it will try again to send the message, putting on hold any other future messages that are supposed to be delivered, until the initial message expires.

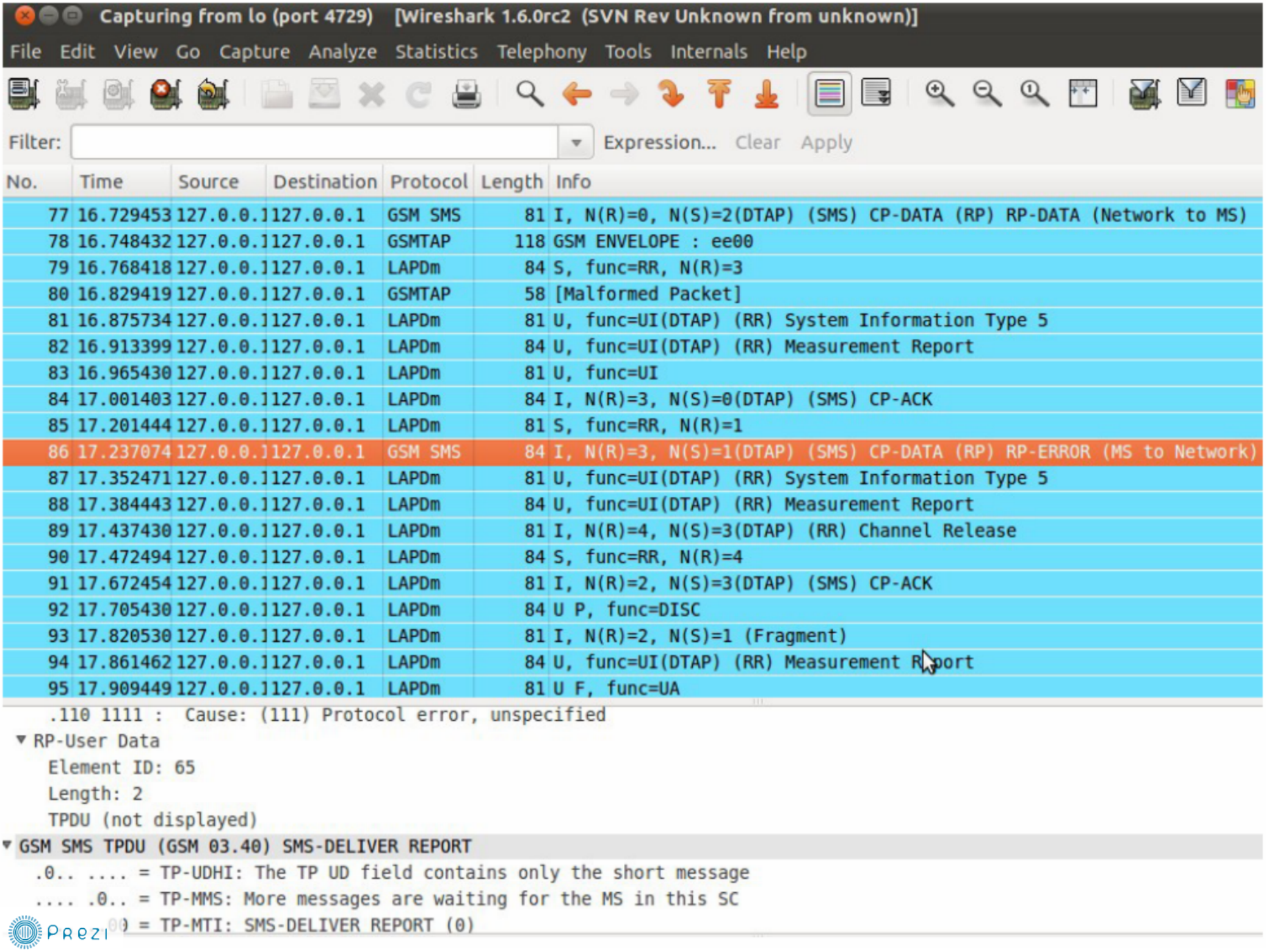

72 5.236172 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=2(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to M
User Datagram Protocol, Src Port: 55844 (55844), Dst Port: gsmtap (4729)
GSM TAP Header, ARFCN: 99 (Downlink), TS: 0, Channel: SDCCH (0)
Link Access Procedure, Channel Dm (LAPDm)
GSM A-I/F DTAP - CP-DATA
GSM A-I/F RP - RP-DATA (Network to MS)
Message Type RP-DATA (Network to MS)
RP-Message Reference
RP-Origination Address - (407
RP-Destination Address
RP-User Data
GSM SMS TPDU (GSM 03.40) SMS-DELIVER
0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
.1.. .... = TP-UDHI: The beginning of the TP UD field contains a Header in addition to the short message
..0. .... = TP-SRI: A status report shall not be returned to the SME
.... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
.... ..00 = TP-MTI: SMS-DELIVER (0)
TP-Originating-Address - (407
TP-PID: 127
01.. .... : defines formatting for subsequent bits
..11 1111 : (63) (U)SIM Data download
TP-DCS: 246
1111 .... = Coding Group Bits: Data coding/message class (15)
1111 .... : Data coding/message class
.... 0... : Reserved
.... .1.. : Message coding: 8 bit data
.... ..10 : Message Class: Class 2 (U)SIM specific message
TP-Service-Centre-Time-Stamp
TP-User-Data-Length: (19) depends on Data-Coding-Scheme
TP-User-Data
User-Data Header
User Data Header Length (2)
(U)SIM Toolkit Security Headers (SMS Control)


72 5.236172 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=2(DTAP)
73 5.252207 127.0.0.1 127.0.0.1 GSMTAP 118 GSM ENVELOPE : ee00
74 5.273137 127.0.0.1 127.0.0.1 LAPDm 84 S, func=RR, N(R)=3
75 5.385250 127.0.0.1 127.0.0.1 LAPDm 81 U, func=UI(DTAP) (RR) S
76 5.425205 127.0.0.1 127.0.0.1 LAPDm 84 U, func=UI(DTAP) (RR) M
Frame 73: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (1
User Datagram Protocol, Src Port: 55844 (55844), Dst Port: gsmtap (4729)
GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: UNKNOWN (0)
GSM SIM 11.11
Class: GSM (0xa0)
Instruction: ENVELOPE (0xc2)
Parameter 1: 0x00
Parameter 2: 0x00
Length (Parameter 3): 0x37
APDU Payload: d135820283810607910447946400f08b26440b9104570838...


239 11.628523 127.0.0.1 127.0.0.1 GSM SMS 84 I, N(R)=0, N(S)=2(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
Frame 239: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: 55844 (55844), Dst Port: gsmtap (4729)
GSM TAP Header, ARFCN: 0 (Uplink), TS: 0, Channel: SDCCH (0)
Link Access Procedure, Channel Dm (LAPDm)
GSM A-I/F DTAP - CP-DATA
GSM A-I/F RP - RP-DATA (MS to Network)
GSM SMS TPDU (GSM 03.40) SMS-SUBMIT
0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
.1.. .... = TP-UDHI: The beginning of the TP UD field contains a Header in addition to the short message
..0. .... = TP-SRR: A status report is not requested
...0 0... = TP-VPF: TP-VP field not present (0)
.... .0.. = TP-RD: Instruct SC to accept duplicates
.... ..01 = TP-MTI: SMS-SUBMIT (1)
TP-MR: 0
TP-Destination-Address - (40
TP-PID: 0
00.. .... : defines formatting for subsequent bits
..0. .... : no telematic interworking, but SME-to-SME protocol
...0 0000 : the SM-AL protocol being used between the SME and the MS (0)
TP-DCS: 246
1111 .... = Coding Group Bits: Data coding/message class (15)
1111 .... : Data coding/message class
.... 0... : Reserved
.... .1.. : Message coding: 8 bit data
.... ..10 : Message Class: Class 2 (U)SIM specific message
TP-User-Data-Length: (16) depends on Data-Coding-Scheme
TP-User-Data
User-Data Header
User Data Header Length (2)
(U)SIM Toolkit Security Headers (SMS Control)


263 12.553036 127.0.0.1 127.0.0.1 GSMTAP 75 GSM TERMINAL RESPONSE SEND SHORT MESSAGE : 0100
264 12.573553 127.0.0.1 127.0.0.1 LAPDm 84 S, func=RR, N(R)=4
265 12.751533 127.0.0.1 127.0.0.1 GSMTAP 60 [Malformed Packet]
User Datagram Protocol, Src Port: 55844 (55844), Dst Port: gsmtap (4729)
GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: UNKNOWN (0)
GSM SIM 11.11
pturing from lo (port 4729) [Wireshark 1.6.0rc2 (SVN Rev Unknown from unknown)]

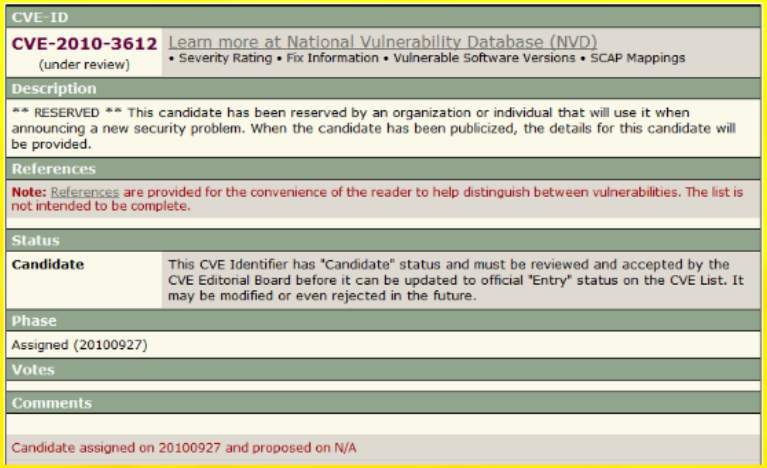

263 12.553036 127.0.0.1 127.0.0.1 GSMTAP 75 GSM TERMINAL RESPONSE SEND SHORT MESSAGE : 0100
Frame 263: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: 55844 (55844), Dst Port: gsmtap (4729)
GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: UNKNOWN (0)
GSM SIM 11.11
Class: GSM (0xa0)
Instruction: TERMINAL RESPONSE (0x14)
Card Application Tookit ETSI TS 102.223
Command details: 011300
Command Number: 0x01
Command Type: SEND SHORT MESSAGE (0x13)
Command Qualifier: 0x00
Device identity: 8281
Source Device ID: Terminal (Card Reader) (0x82)
Destination Device ID: SIM / USIM / UICC (0x81)
Result: 00
Result: Command performed successfully (0x00)
Status Word: 0100


Capturing from lo (port 4729) [Wireshark 1.6.0rc2 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length Info
77 16.729453 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=2(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
78 16.748432 127.0.0.1 127.0.0.1 GSMTAP 118 GSM ENVELOPE : ee00
79 16.768418 127.0.0.1 127.0.0.1 LAPDm 84 S, func=RR, N(R)=3
80 16.829419 127.0.0.1 127.0.0.1 GSMTAP 58 [Malformed Packet]
81 16.875734 127.0.0.1 127.0.0.1 LAPDm 81 U, func=UI(DTAP) (RR) System Information Type 5
82 16.913399 127.0.0.1 127.0.0.1 LAPDm 84 U, func=UI(DTAP) (RR) Measurement Report
83 16.965430 127.0.0.1 127.0.0.1 LAPDm 81 U, func=UI
84 17.001403 127.0.0.1 127.0.0.1 LAPDm 84 I, N(R)=3, N(S)=0(DTAP) (SMS) CP-ACK
85 17.201444 127.0.0.1 127.0.0.1 LAPDm 81 S, func=RR, N(R)=1
86 17.237074 127.0.0.1 127.0.0.1 GSM SMS 84 I, N(R)=3, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-ERROR (MS to Network)
87 17.352471 127.0.0.1 127.0.0.1 LAPDm 81 U, func=UI(DTAP) (RR) System Information Type 5
88 17.384443 127.0.0.1 127.0.0.1 LAPDm 84 U, func=UI(DTAP) (RR) Measurement Report
89 17.437430 127.0.0.1 127.0.0.1 LAPDm 81 I, N(R)=4, N(S)=3(DTAP) (RR) Channel Release
90 17.472494 127.0.0.1 127.0.0.1 LAPDm 84 S, func=RR, N(R)=4
91 17.672454 127.0.0.1 127.0.0.1 LAPDm 81 I, N(R)=2, N(S)=3(DTAP) (SMS) CP-ACK
92 17.705430 127.0.0.1 127.0.0.1 LAPDm 84 U P, func=DISC
93 17.820530 127.0.0.1 127.0.0.1 LAPDm 81 I, N(R)=2, N(S)=1 (Fragment)
94 17.861462 127.0.0.1 127.0.0.1 LAPDm 84 U, func=UI(DTAP) (RR) Measurement Report
95 17.909449 127.0.0.1 127.0.0.1 LAPDm 81 U F, func=UA
.110 1111 : Cause: (111) Protocol error, unspecified
RP-User Data
Element ID: 65
Length: 2
TPDU (not displayed)
GSM SMS TPDU (GSM 03.40) SMS-DELIVER REPORT
.0.. .... = TP-UDHI: The TP UD field contains only the short message
.... .0.. = TP-MMS: More messages are waiting for the MS in this SC
.... ..00 = TP-MTI: SMS-DELIVER REPORT (0)


14:11
orange
14:11
Tue 01 Nov.
Menu
Contacts
SAMSUNG


NOKIA
Vodafone RO
Silent
Menu

I first discovered the vulnerability somewhere in June 2010 and worked on better understanding it. Meanwhile on August 26 2010 I have reported the vulnerability to CERT (Computer Emergency Response Team) and they have assigned a CVE but it was not published yet. Details about this will be published on http://www.cve.mitre.org/cgibin/cvename.cgi?name=2010-3612.



CVE-ID

CVE-2010-3612 (under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20100927)

Votes

Comments

Candidate assigned on 20100927 and proposed on N/A

http://www.cve.mitre.org/cgibin/

CVE-ID	
CVE-2010-3612 (under review)	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Status	
Candidate	This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20100927)

Votes

Comments

Candidate assigned on 20100927 and proposed on N/A

Testing...

- The vulnerability has been tested on multiple phones: Nokia 2330, 3310, 6310, N97 ; Samsung i900, Galaxy S, Galaxy S2; iPhone; HTC with Windows Mobile 6.5, with Android; Blackberry
- Some of the phones show that a message is being sent, while others don't
- Sometimes the SIM tries to send 3 or 4 times the message

Testing...

- The vulnerability has been tested on multiple phones: Nokia 2330, 3310, 6310, N97 ; Samsung i900, Galaxy S, Galaxy S2; iPhone; HTC with Windows Mobile 6.5, with Android; Blackberry

Testing...

- The vulnerability has been tested on multiple phones: Nokia 2330, 3310, 6310, N97 ; Samsung i900, Galaxy S, Galaxy S2; iPhone; HTC with Windows Mobile 6.5, with Android; Blackberry
- Some of the phones show that a message is being sent, while others don't
- Sometimes the SIM tries to send 3 or 4 times the message

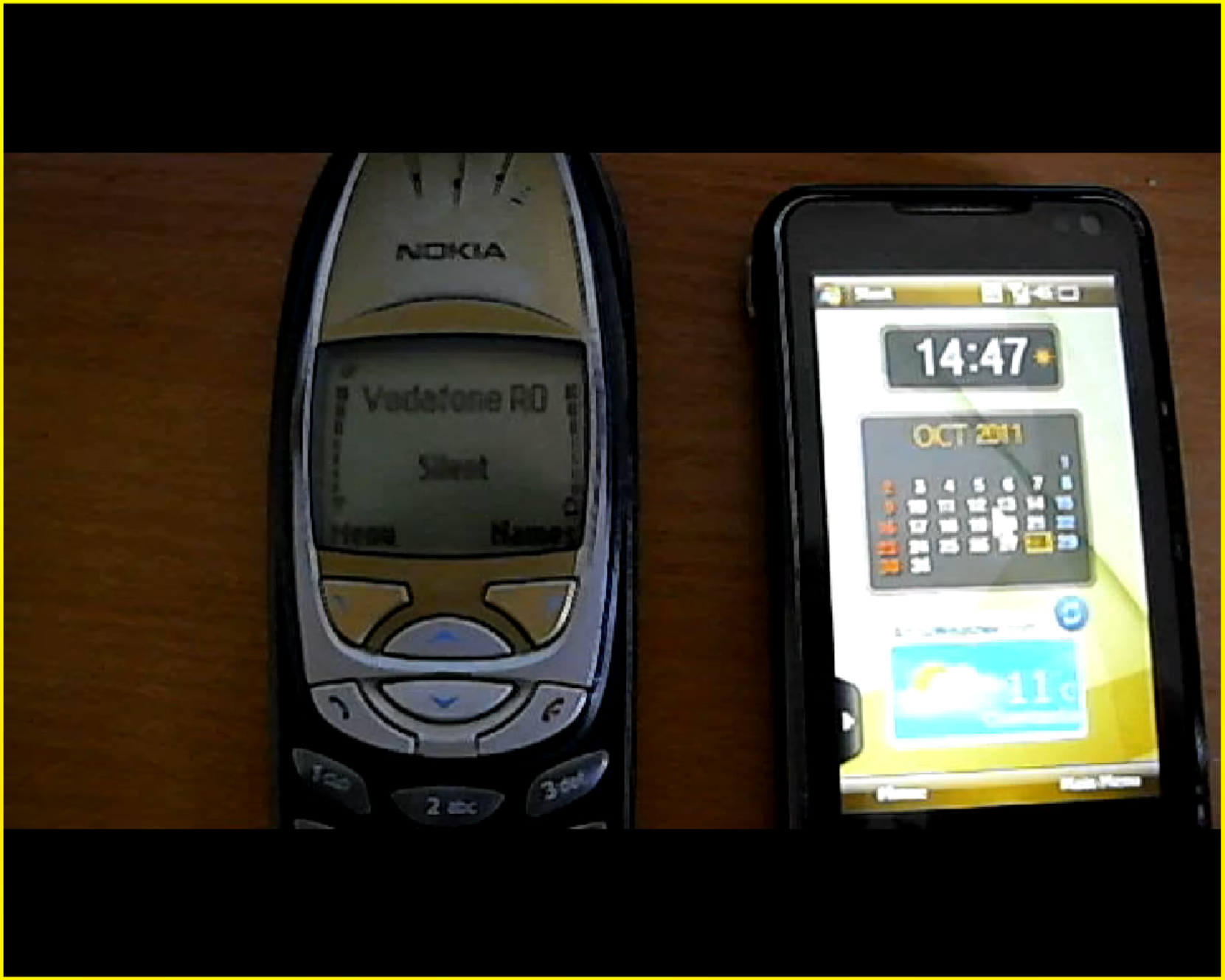
IMPACT

- The attack works independent of the phone or GSM network
- When sending the message between different networks or the same network it doesn't have such a great financial impact.
- There are bulk SMS providers that allow you to change the identity of the sender -> think about premium rate numbers

* The issue is that not all forward correctly the APDU packets to all or some mobile operators. During my research, after contacting about 10 different providers I found two that correctly forwarded the messages to the destination networks tested

- # There are bulk SMS provider identity of the sender -> thin

* The issue is that not all forward correctly the APDU packets to all or some mobile operators. During my research, after contacting about 10 different providers I found two that correctly forwarded the messages to the destination networks tested


NOKIA
Vodafone RO
Silent
14:47
OCT 2011


CallMed
Medicul tău,
la un telefon distanță
PLAY
Home
Services
News
FAQ
Partners
Contact
Forum
Menu
Home
Find a doctor
Request medical record
Log application CallMed
Register by SMS
Services
How do I use CallMed 1363?
Call in 1363 . After the voice message unique identifier type of doctor and the call is directed to it.
The price is 0.95 euro / min + VAT (1.18 euro / min, VAT included), the first minute is
What is CallMed?
CallMed telephone counseling service is designed to facilitate communication between physicians and their patients.
For any health problem, patients can seek medical advice before programming even for a

How to protect from such attacks?

- Mobile operators could filter command messages that are not coming from themselves. Even if it's a network protection, users not being protected if not all of the operators implement such security
- Some mobile devices have the option to ask the user about SIM actions. If the option is set, when the phone will try to send the message it will ask to allow this
- Use a SIM card that has the service "data download via SMS Point-to-point" deactivated or one that doesn't have any Toolkit Application on it
- Use a Nokia DCT3 phone and stay always connected with the F-BUS cable and Wireshark opened (hard to make it always)

How to protect from such attacks?

- Mobile operators could filter command messages that are not coming from themselves. Even if it's a network protection, users not being protected if not all of the operators implement such security
- Some mobile devices have the option to ask the user about SIM actions. If the option is set, when the phone will try to send the message it will ask to allow this
- Use a SIM card that has the service "data download via SMS Point-to-point" deactivated or one that doesn't have any Toolkit Application on it
- Use a Nokia DCT3 phone and stay always connected with the F-BUS cable and Wireshark opened (hard to make it always)

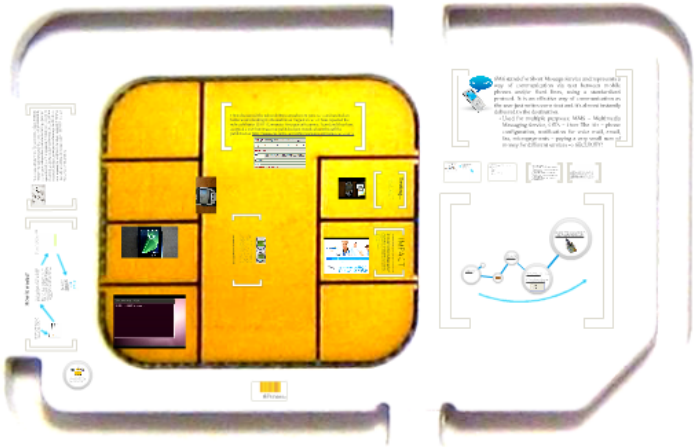
Some mobile devices have the option to ask the user about SIM actions. If the option is set, when the phone will try to send the message it will ask to allow this

- Use a SIM card that has the service "data download via SMS Poi point" deactivated or one that doesn't have any Toolkit Applicat it
- Use a Nokia DCT3 phone and stay always connected with the F cable and Wireshark opened (hard to make it always)

- Tobias Engel
- All the people that developed Osmocom
- All who agreed to let me play with their mobile

SMS fuzzing - SIM Toolkit Attack

Bogdan Alecu - http://www.m-sec.net



Push SIM from back to detach.

DEEPSEC Mobile

Get more security for your phone.