BUSINESS LOGIC FLAWS IN MOBILE OPERATORS SERVICES

BOGDAN ALECU

ABOUT ME

- Independent security researcher
- Sysadmin
- 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

GOALS

- SIM Toolkit: what is it, how can we exploit it
- Understanding of business logic flaws in mobile operators services
- What you should do in order to protect from these attacks

TOPICS

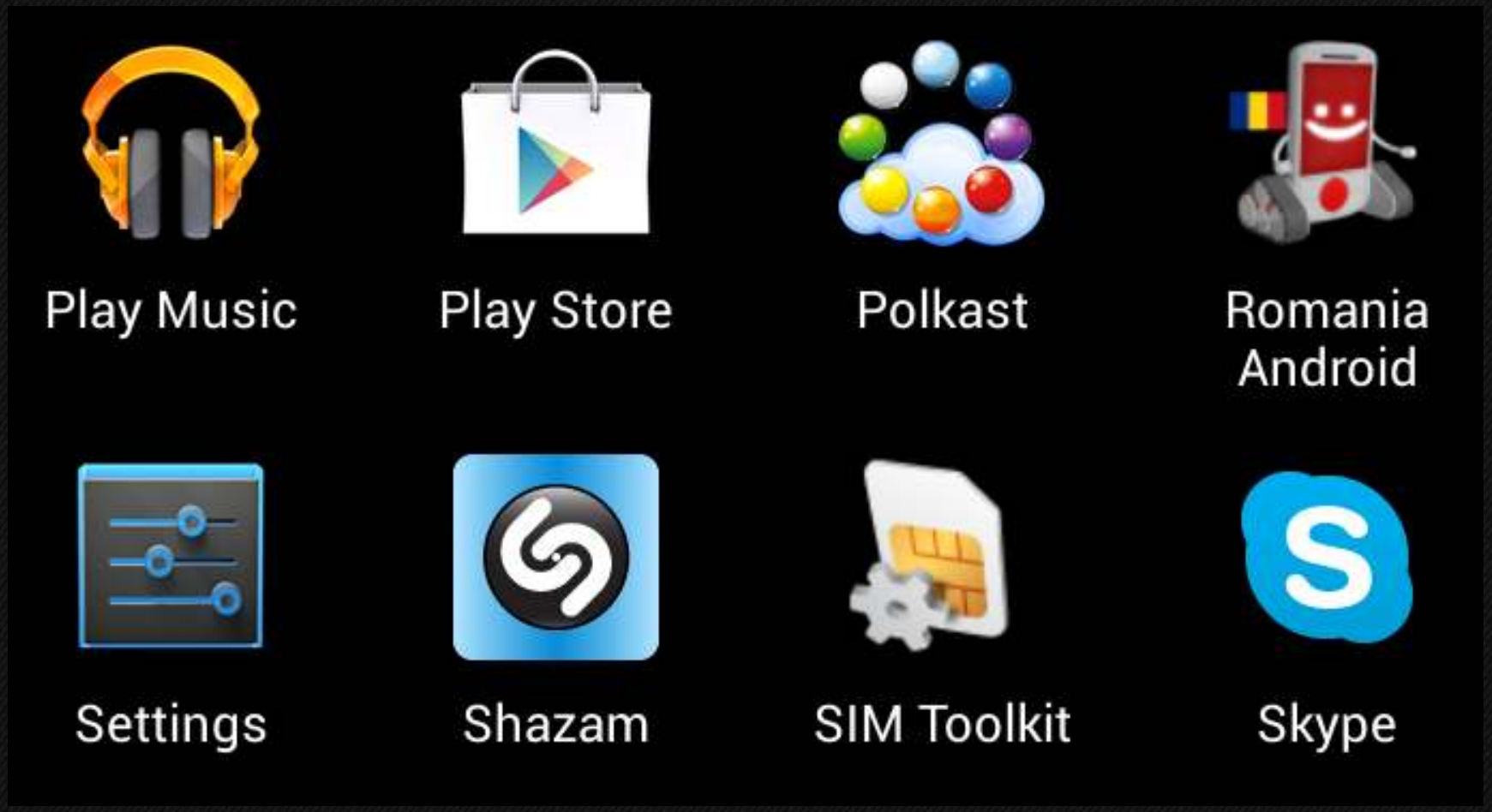
1. SIM TOOLKIT
2. HTTP HEADERS
3. DATA TRAFFIC VULNERABILITY
4. THE EXTRA DIGIT
5. SUMMARY

THE BUGGY WORLD

1 SIM TOOLKIT

BOGDAN ALECU

THE BUGGY WORLD

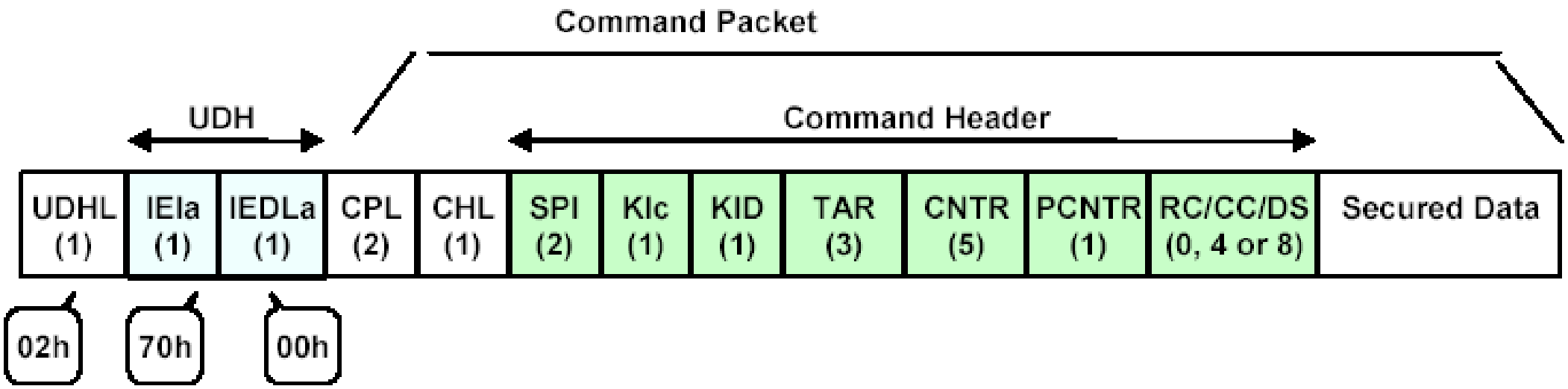


Example of SIM Toolkit icon on your mobile device

THE BUGGY WORLD

For sending Ringtones, operator logo, concatenated messages, SMS makes use of the User Data Header

THE BUGGY WORLD



ETSI TS 101 181 V8.9.0

BOGDAN ALECU

THE BUGGY WORLD

The type of message sent is addressed directly to the SIM, by setting the PID to 0x7F, corresponding to USIM Data Download and by setting DCS to F6

THE BUGGY WORLD

"

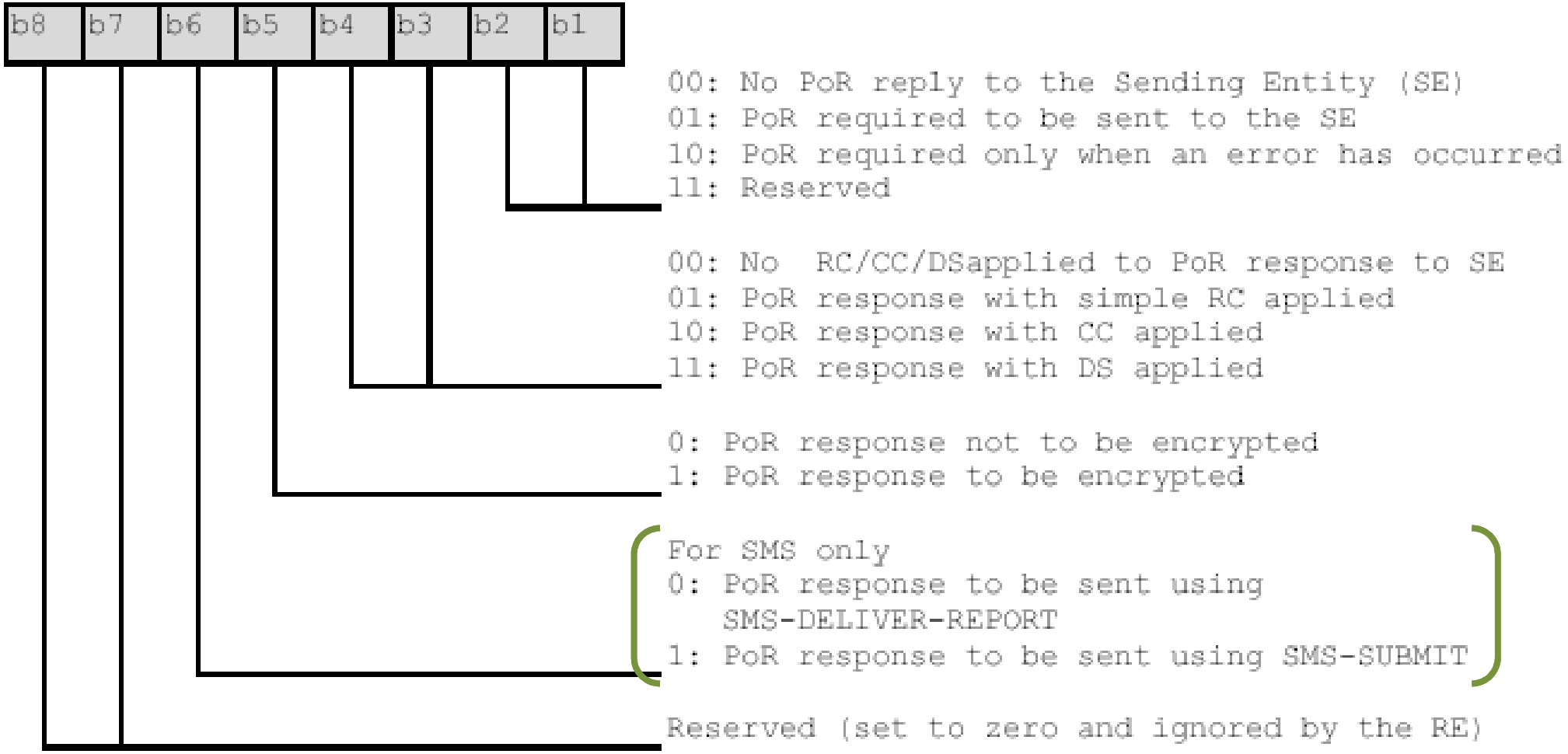
... then the ME shall pass the message transparently to the SIM
... shall not display the message, or alert the user of a short message waiting

ETSI GSM 11.14 "

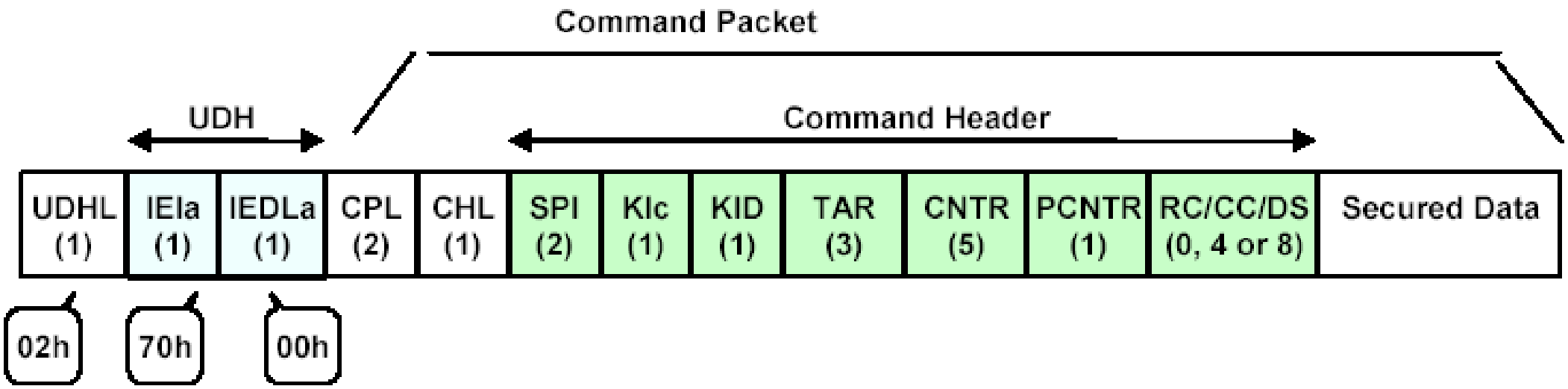
THE BUGGY WORLD

Second Byte:

Security Parameter Indicator

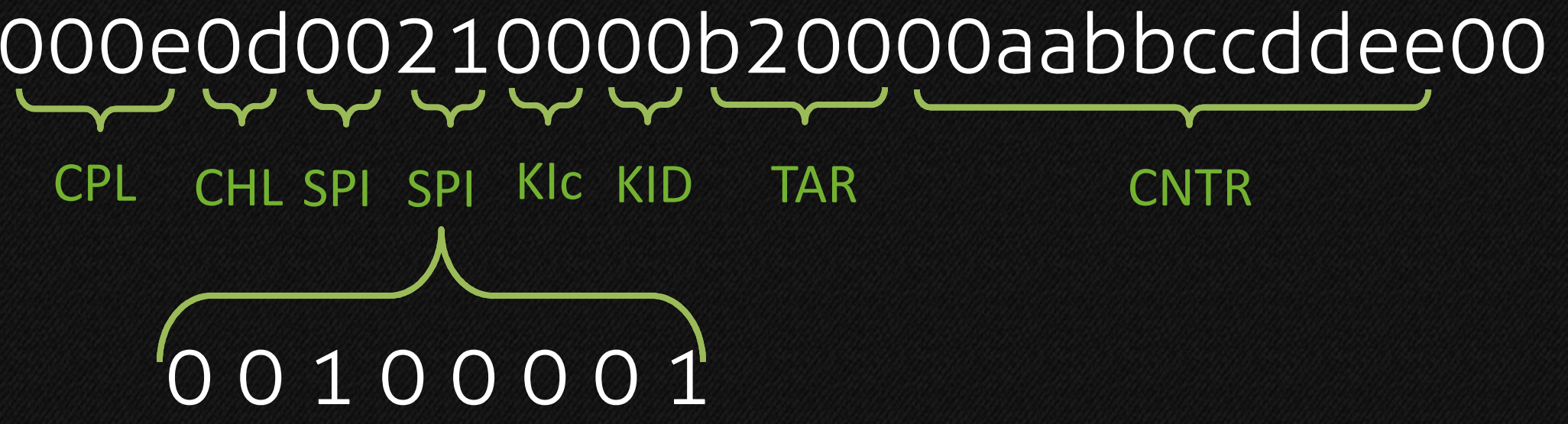


THE BUGGY WORLD



THE BUGGY WORLD

UDH (User Data Header): 027000
PID (Protocol ID): 7F
DCS (Data Coding Scheme): F6



THE BUGGY WORLD

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
```

THE BUGGY WORLD

- SIM card automatically replies to the sending number
- Nothing in Inbox, Outbox – only on your bill

THE BUGGY WORLD

LET'S SEE IT IN ACTION!

THE BUGGY WORLD

2 HTTP HEADERS

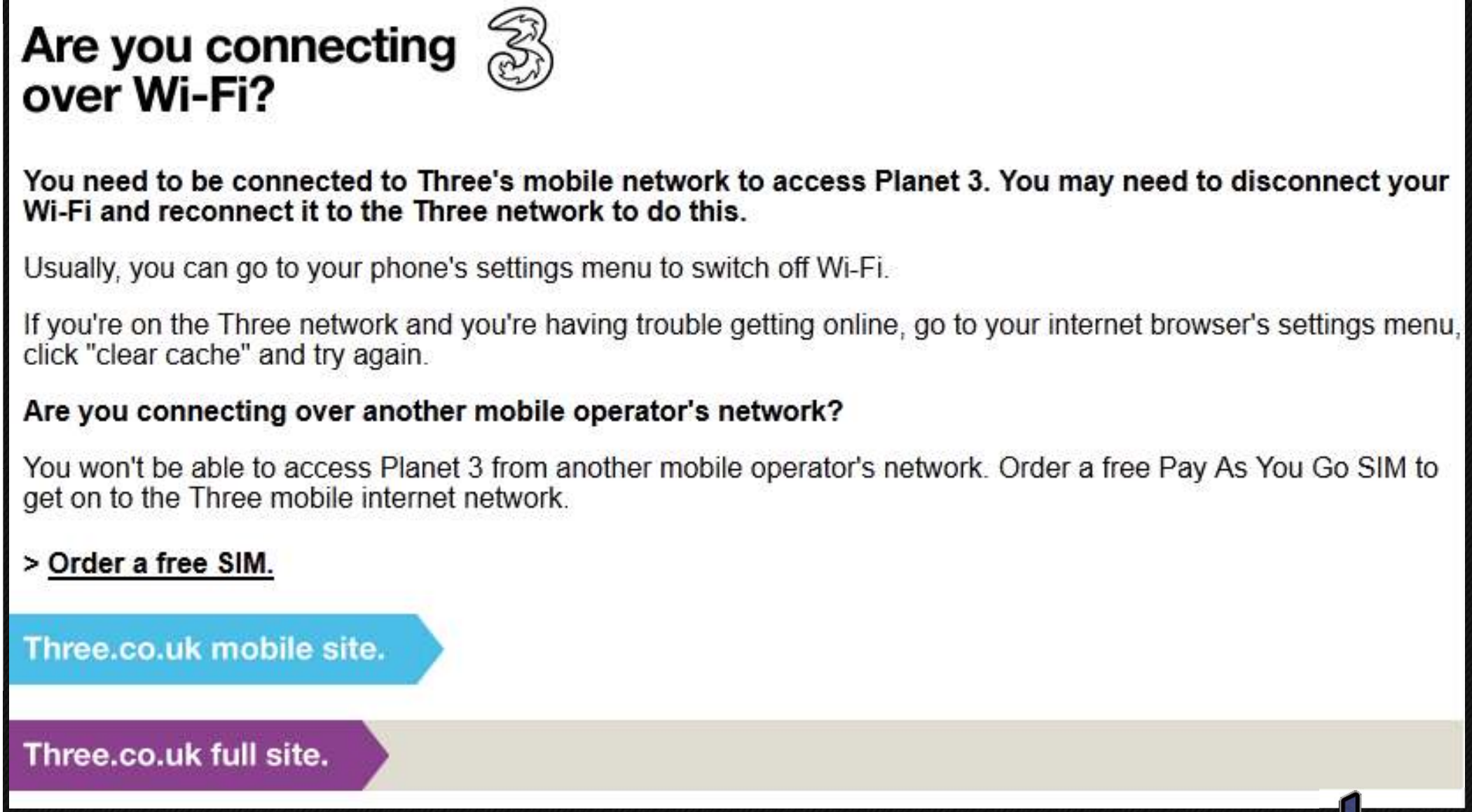
BOGDAN ALECU

THE BUGGY WORLD

Mobile operators have their own WAP / WEB page for customers:

- Balance check
- Money transfer
- Download music, videos, wallpapers
- Subscribe to services (eg. custom ringback tones)

THE BUGGY WORLD



Are you connecting over Wi-Fi?

You need to be connected to Three's mobile network to access Planet 3. You may need to disconnect your Wi-Fi and reconnect it to the Three network to do this.

Usually, you can go to your phone's settings menu to switch off Wi-Fi.

If you're on the Three network and you're having trouble getting online, go to your internet browser's settings menu, click "clear cache" and try again.

Are you connecting over another mobile operator's network?

You won't be able to access Planet 3 from another mobile operator's network. Order a free Pay As You Go SIM to get on to the Three mobile internet network.

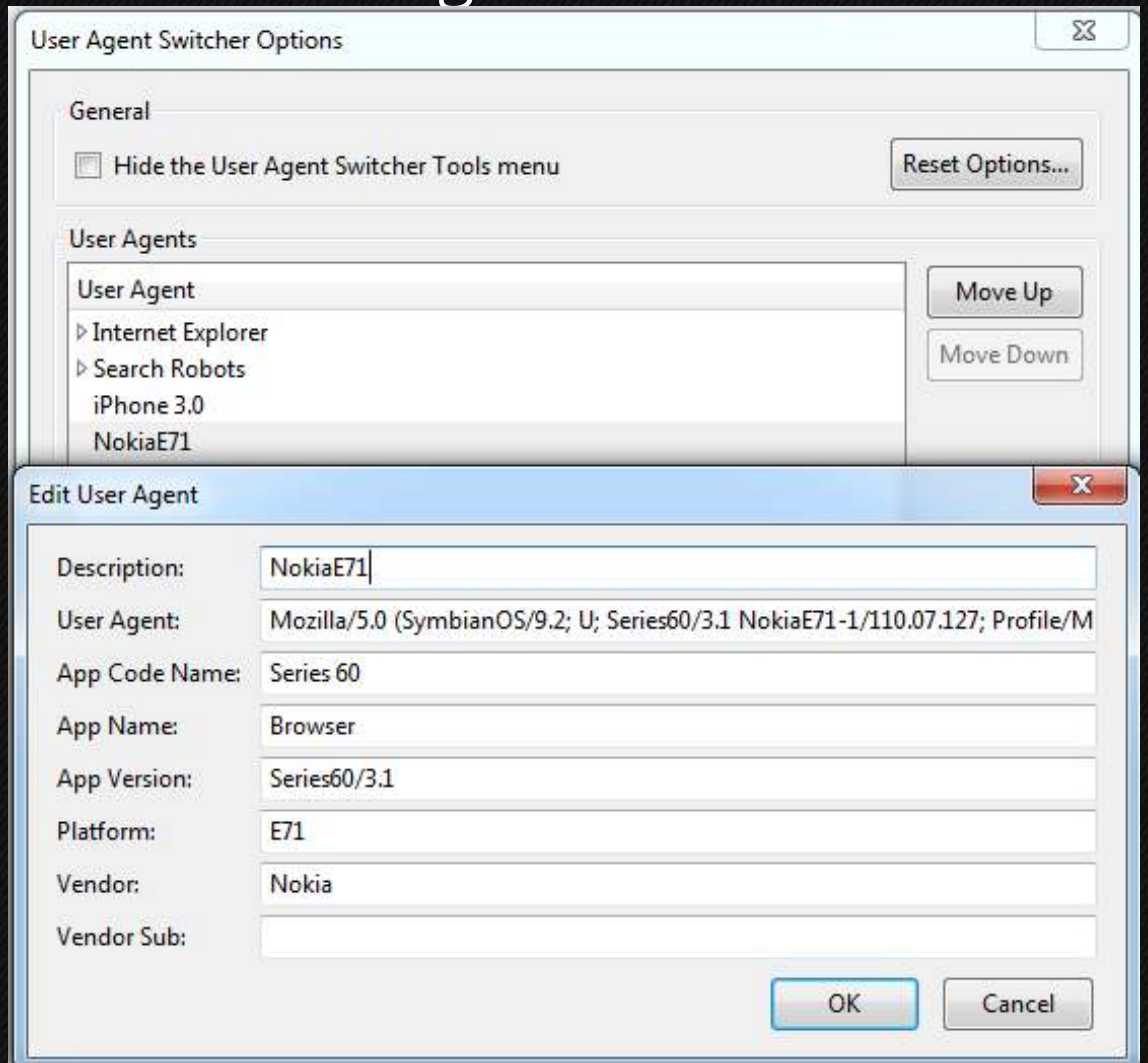
> Order a free SIM.

Three.co.uk mobile site.

Three.co.uk full site.

THE BUGGY WORLD

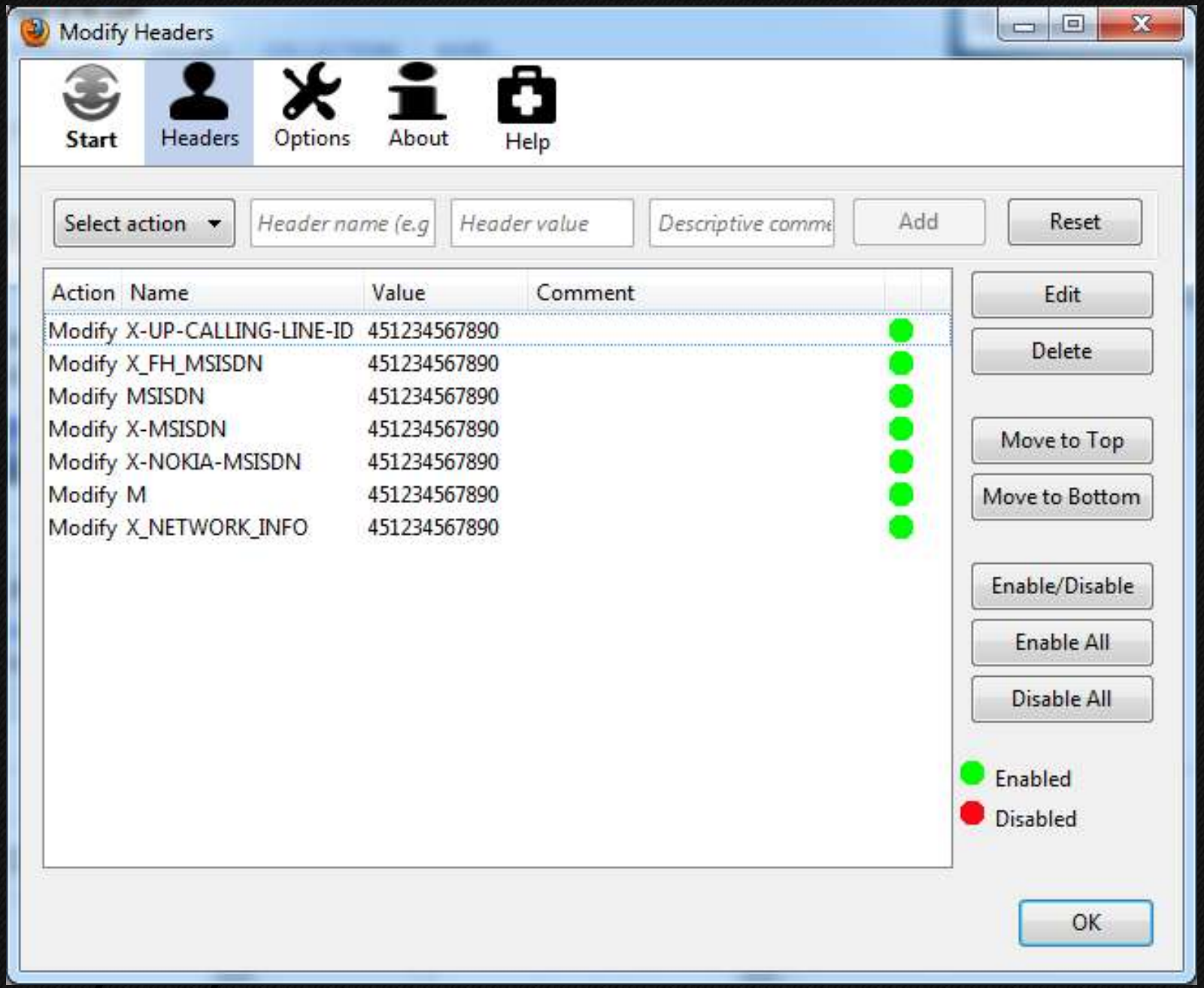
User Agent Switcher https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher/



THE BUGGY WORLD

- Operators know who to charge based on HTTP headers
- Sniff the traffic your phone does and look for the headers having mobile number
- "Privacy Leaks in Mobile Phone Internet Access" by Collin Mulliner

THE BUGGY WORLD



THE BUGGY WORLD

The old fashioned way of the attack

THE BUGGY WORLD

CSD (Circuit Switched Data)

- Think about it like dial-up
- Since it involves actually placing a phone call, it is exposed to the same vulnerabilities like a regular call

THE BUGGY WORLD

THE BUGGY WORLD

DEMO TIME!

THE BUGGY WORLD

3 Data traffic vulnerability

THE BUGGY WORLD

- What happens when you reach data limit?
- Have you ever tried to perform a DNS query?

THE BUGGY WORLD

But what if …

- you setup a VPN server listening on port 53 UDP (DNS port)
- connect to this server and route all the traffic

THE BUGGY WORLD

Internet traffic

Works also in Roaming!

THE BUGGY WORLD

4 The extra digit

BOGDAN ALECU

THE BUGGY WORLD

Do you have a flat-rate plan with unlimited minutes in the operator's network?

THE BUGGY WORLD

Do not try this at home!

- Take a ported number that was in your network
- Add two more digits to the end of the number
- Place the call
- You will be charged like calling in your network

THE BUGGY WORLD

Joi 03/01/2013	00:00:52	4	0581	Voce	NECUNOSCUT(-)	0.00	National/Intl
Joi 03/01/2013	00:00:43	4	05_P	Voce	150 minutes/SMS to all national destinations(00:01:00)	0.00	National/Intl

Legendă: ((P) Număr portat (transferat) in altă reţea,

THE BUGGY WORLD

If that does not work...

- try with one digit, all the digits
- divert all calls to that number, but add a digit at the end of it

5 Summary

SUMMARY

"Our technology does not allow unauthorized access. Occurrence of errors in billing regarding data traffic or voice is excluded."

BOGDAN AL

SUMMARY

- Test yourself and report the issues to your carrier
- Check if your carrier allows you to disable access to premium rate services

SUMMARY

- Filter SIM command messages
- Do not rely only on the caller ID
- Always authenticate, do not forget about privacy

THANK YOU

FOR YOUR ATTENTION

msecnet

www.m-sec.net

alecu@m-sec.net