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
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
1. SIM TOOLKIT
2. HTTP HEADERS
3. DATA TRAFFIC VULNERABILITY
4. THE EXTRA DIGIT
5. SUMMARY
Example of SIM Toolkit icon on your mobile device
For sending Ringtones, operator logo, concatenated messages, SMS makes use of the User Data Header
ETSI TS 101 181 V8.9.0
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.
... 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
Second Byte:

<table>
<thead>
<tr>
<th>b8</th>
<th>b7</th>
<th>b6</th>
<th>b5</th>
<th>b4</th>
<th>b3</th>
<th>b2</th>
<th>b1</th>
</tr>
</thead>
</table>

Security Parameter Indicator

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/DS applied 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 BUGGY WORLD

Command Packet

UDH

Command Header

UDHL (1) IEl (1) IEDL (1) CPL (2) CHL (1) SPI (2) Klc (1) KID (1) TAR (3) CNTR (5) PCNTR (1) RC/CC/DS (0, 4 or 8) Secured Data

02h 70h 00h

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

000e0d00210000b20000aabbccddeee00

CPL  CHL  SPI  SPI  KIC  KID  TAR  CNTR

00100001

BOGDAN ALECU
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 Toolkit 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
• SIM card automatically replies to the sending number
• Nothing in Inbox, Outbox – only on your bill
LET’S SEE IT IN ACTION!
HTTP HEADERS
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)
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.
• 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
HTTP HEADERS

THE BUGGY WORLD
The old fashioned way of the attack

KIDS, I REMEMBER WHEN
WE HAD TO CALL THE INTERNET WITH OUR PHONES

9GAG.COM/GAG/4664592
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

DEMO TIME!

BOGDAN ALECU
3 Data traffic vulnerability
• What happens when you reach data limit?

• Have you ever tried to perform a DNS query?
But what if ... 

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

Works also in Roaming!
4 The extra digit
Do you have a flat-rate plan with unlimited minutes in the operator’s network?
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
<table>
<thead>
<tr>
<th>Data</th>
<th>Oră</th>
<th>Cod</th>
<th>Număr</th>
<th>Tip</th>
<th>Durată</th>
<th>Cost</th>
<th>Tip  Rezoluție</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/01/2013</td>
<td>00:00:52</td>
<td>4</td>
<td>0581</td>
<td>Voce</td>
<td>NECUNOSCUT(–)</td>
<td>0.00</td>
<td>National/Intl</td>
</tr>
<tr>
<td>03/01/2013</td>
<td>00:00:43</td>
<td>4</td>
<td>05_P</td>
<td>Voce</td>
<td>150 minutes/SMS to all national destinations (00:01:00)</td>
<td>0.00</td>
<td>National/Intl</td>
</tr>
</tbody>
</table>

Legendă: ((P)) Număr portat (transferat) în altă rețea.
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
Summary
“Our technology does not allow unauthorized access. Occurrence of errors in billing regarding data traffic or voice is excluded.”
SUMMARY

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

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