Call me Maybe! – Establishing covert channels by abusing GSM AT Commands

Dr. Alfonso Muñoz (@mindcrypt) - Jorge Cuadrado (@Coke727)
Dr. Alfonso Muñoz - @mindcrypt
Head of Cybersecurity Lab –
- Expert Member / Criminal Use of Information Hiding (CUIng) Initiative (Europol European Cybercrime Centre -EC3)
- Speaker in hacking conferences (Deepsec, HackInTheBox, VirtusBulletin, 8.8, RootedCon, STIC CCN-CERT, ...)
- CISA (Certified Information Systems Auditor), CEHv8 (Certified Ethical Hacker), CHFIv8 (Computer Hacking Forensic Investigator), CES (Certified Encryption Specialist) and OSCP (Offensive Security Certified Professional)
- +60 academic publications (IEEE, ACM, JCR, hacking conferences...), books and computer security tools. He has also worked in advanced projects with European Organisms, public bodies and multinational companies (global 500)

www.linkedin.com/in/alfonsomunoz & http://alfonsocv.com & alfonso@criptored.com

Jorge Cuadrado @coke727
Security Researcher –

Jorge has a Bsc. in Computer Science by the University of Valladolid (UVa) and Masters in Cyber security by the University Carlos III of Madrid (UC3M). He is currently working in a cybersecurity and innovation laboratory as a researcher.

www.linkedin.com/in/jorgecuadradosaez & jorgecuadradosaez@gmail.com

Call me Maybe! – Establishing covert channels by abusing GSM AT Commands
Disclaimer
Phreaking

Phreaking is a slang term coined to describe the activity of a culture of people who study, experiment with, or explore telecommunication systems, such as equipment and systems connected to public telephone networks. The term phreak is a sensational spelling of the word freak with the ph-from phone, and may also refer to the use of audio frequencies to manipulate a phone system. Phreak, phreaker, or phone phreak are names used for and by individuals who participate in phreaking...

https://en.wikipedia.org/wiki/Phreaking
Secrets of the Little Blue Box

A way to trick the telephone company.

The Blue Box isいっぱい!

In the late 1960s, a group of 15 telephone engineers at Bell Labs, led by Martin Cooper, started working on a new project. They were tasked with creating a mobile phone that could make calls without the need for a landline. The project was code-named “Project 900,” and the team worked tirelessly to make it a reality.

The goal was to create a device that could be used to make calls from anywhere, and the team succeeded. In 1973, they unveiled the first mobile phone, which was a bulky and expensive device that could only make calls within a limited area.

Today, mobile phones are ubiquitous and are an essential part of our daily lives. However, it’s important to remember the history of this technology and the people who worked so hard to make it possible.


https://www.thingiverse.com/thing:2630646/#files
The beginning
Mobile phone: Golden nugget!

Edward Snowden reveals how Government can hack into YOUR smartphone and see EVERYTHING

https://www.tjoe.org/pub/direct-radio-introspection


WikiLeaks #Vault7 confirms CIA can effectively bypass Signal + Telegram + WhatsApp + Confide encryption

wikileaks.org/cia7p1

https://www.journalism.co.uk/2017/03/27/glyphone-recognizing-speech-from-gyroscope-signals/


https://www.tjoe.org/pub/direct-radio-introspection
Another kind of attacks are to the software that manage radio communications:

“Every mobile phone runs two operating systems; the one you interact with (like Android or IOS), and the one that controls the radio hardware. This second OS is ancient, creaking, and wildly insecure...”

Researchers can attack mobile phones via spoofed SMS messages

Phones that support MMS on GSM networks are vulnerable to new SMS spoofing attacks, researchers say at Black Hat.


DeepSec 2010: All your baseband are belong to us by Ralf Philipp Weinmann - https://www.youtube.com/watch?v=fQqv0v14KKY

Baseband vulnerability could mean undetectable, unblockable attacks on mobile phones

https://boingboing.net/2016/07/20/baseband-vulnerability-could-m.html

http://www.osnews.com/story/27416/The_second_operating_system_hiding_in_every_mobile_phone

The SMS of Death Mobile Phone Attack Explained

https://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html


Nearly 1 billion phones can be hacked with 1 text


Another kind of attacks are to the software that manage radio communications:

“Every mobile phone runs two operating systems; the one you interact with (like Android or IOS), and the one that controls the radio hardware. This second OS is ancient, creaking, and wildly insecure...”

https://boingboing.net/2016/07/20/baseband-vulnerability-could-m.html

http://www.osnews.com/story/27416/The_second_operating_system_hiding_in_every_mobile_phone

The SMS of Death Mobile Phone Attack Explained

https://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html

Nearly 1 billion phones can be hacked with 1 text

Secraphony...

Tron - Spring 1998

1998: TRONs CRYPTOFOON

http://tronland.org/
Homemade Phreaking – Making our own mobile phone

Yes, I am a criminal. My crime is that of curiosity  
(The Mentor - January 8, 1986)
http://phrack.org/issues/7/3.html
Homemade Phreaking – Making our own mobile phone

https://github.com/jorcuad/FreePhone/wiki
MÓDULO GSM SIM900

CONEXIÓN DIRECTA DE TODO LOS PINS ENTRE PANTALLA Y RPI3

HAPPY RELEASE DAY!

https://github.com/jorcuad/FreePhone/wiki
Covert Channel

In computer security, a **covert channel** is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. The term is defined as channels "not intended for information transfer at all, such as the service program's effect on system load," to distinguish it from legitimate channels that are subjected to access controls... (1973 by Lampson)
Telephone companies trust in the information sent by clients?
Antena GSM - Client attack
http://simcom.ee/modules/gsm-gprs/sim900/

Feature:

Chipset SIM900 - SIMCOM

Quad-Band 850 / 900 / 1800 / 1900 MHz - would work on GSM networks in all countries across the world.

Control via AT commands - Standard Commands: GSM 07.07 & 07.05 | Enhanced Commands: SIMCOM AT Commands.

The shield allows you to achieve SMS, MMS, GPRS and Audio via UART by sending AT commands

Embedded TCP/UDP stack

Speaker and Headphone jacks

Low power consumption - 1.5mA(sleep mode)

Industrial Temperature Range - -40°C to +85 °C
On 15 March 2006, the European Union adopted the Data Retention Directive, on "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC". It requires Member States to ensure that communications providers retain the necessary data as specified in the Directive for a period of between 6 months and 2 years in order to:

- Trace and identify the source of a communication;
- Trace and identify the destination of a communication;
- Identify the date, time, and duration of a communication;
- Identify the type of communication;
- Identify the communication device;
- Identify the location of mobile communication equipment.

The law of conservation of data on electronic communications and public communications networks (Law 25/2007 October DE18) states that service operators should maintain a prepaid SIM logbook stating the identity of the each customer. Data may be required by order of a judge, in order to detect, investigate and prosecute serious crimes...

… "It concluded that data retention was a valuable tool for ensuring criminal justice and public protection, but that it had achieved only limited harmonisation. There were serious concerns from service providers about the compliance costs and from civil society organisations who claim that mandatory data retention was an unacceptable infringement of the fundamental right to privacy and the protection of personal data..."
Telephone companies trust in the information sent by clients?
1 Introduction

1.1 Scope of the document

This document presents the AT Command Set for SIMCom SIM900 series cellular engine.

1.2 Related documents

The present document is based on the following standards:

[5] 3GPP 27.010: Terminal Equipment to Mobile Station (TE-MS) Multiplexer protocol

The AT Command set implemented by SIM900 is a combination of GSM07.05, GSM07.07 and ITU-T recommendation V.25ter and the AT commands developed by SIMCom.
Contents

1 Introduction ........................................... 15
   1.1 Scope of the document ......................... 15
   1.2 Related documents ............................. 15
   1.3 Conventions and abbreviations .......... 15
   1.4 AT Command system ......................... 15
       1.4.1 Basic syntax ...................... 16
       1.4.2 Parameter syntax ................. 16
       1.4.3 Extended syntax ................. 16
   1.5 Flow control .................................. 17
       1.5.1 Software flow control (XON/XOFF mode) ... 18
       1.5.2 Hardware flow control (RTS/CTS mode) .... 18

2 AT Commands According to V.25TER .......... 19
   2.1 Overview of AT Commands According to V.25TER .... 19
   2.2 Detailed Description of AT Commands According to V.25TER 20
       2.2.3.1 Answer an incoming call ........ 20
       2.2.3.3 Mobile Originated Call to Dial A Number ... 21
       2.2.4.1 ORIGIN to Local Originator in Memory ..... 23

3 AT Commands According to GSM07.07 ......... 46
   3.1 Overview of AT Command According to GSM07.07 .... 46
   3.2 Detailed Descriptions of AT Command According to GSM07.07 47
      3.2.1 AT+CADG Request Manufacturer Identification .... 47
      3.2.1 AT+CMGR Request TA Model Identification .... 49
      3.2.2 AT+CMGR Request TA Revision Identification of Software Release .... 49
      3.2.3 AT+CSQ Request Global Object Identification .... 49
      3.2.4 AT+CSS Request TA Serial Number Identification (IMEI) .... 49
      3.2.5 AT+CIF Set TE/TA Control Character Framing .... 49
      3.2.6 AT+CPG Set TE/TA Local Data Flow Control .... 49
      3.2.7 AT+CTI Set TA Fixed Local Rate .... 49
      3.2.8 AT+CVOC Disconnect Voice Call Only .... 49
      3.2.9 AT+CRF Select Remote Service Type .... 49
      3.2.10 AT+CC3 Call Waiting Number and Conditions Control .... 49
      3.2.11 AT+CC12 Call Waiting Control .... 49
      3.2.12 AT+CCN Request Remote KXN Service Parameter Identification .... 49
      3.2.13 AT+CCN Request Remote KXN Service Selection .... 49
      3.2.14 AT+CCN Request Remote KXN Service Parameter Identification (Identical with +OCSN) .... 49
      3.2.15 AT+CSCS Select TE Character Set .... 49

SIM900_ATCommands Manual_V1.11 6 2014.10.20

SIM900_ATCommands Manual_V1.11 7 2014.10.20
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.13 AT+CSTA</td>
<td>Select Type of Address</td>
<td>58</td>
</tr>
<tr>
<td>3.2.14 AT+CHLD</td>
<td>Call Hold and Mute</td>
<td>59</td>
</tr>
<tr>
<td>3.2.15 AT+CIIP</td>
<td>Request International Mobile Subscriber Identity</td>
<td>60</td>
</tr>
<tr>
<td>3.2.16 AT+CCCL</td>
<td>List Current Calls of MS</td>
<td>61</td>
</tr>
<tr>
<td>3.2.17 AT+CLCK</td>
<td>Facility Lock</td>
<td>62</td>
</tr>
<tr>
<td>3.2.18 AT+CLDP</td>
<td>Calling Line Identification Presentation</td>
<td>63</td>
</tr>
<tr>
<td>3.2.19 AT+CLLR</td>
<td>Calling Line Identification Restriction</td>
<td>64</td>
</tr>
<tr>
<td>3.2.20 AT+CMEE</td>
<td>Report Mobile Equipment Error</td>
<td>65</td>
</tr>
<tr>
<td>3.2.21 AT+COLP</td>
<td>Connected Line Identification Presentation</td>
<td>66</td>
</tr>
<tr>
<td>3.2.22 AT+COPS</td>
<td>Operator Selection</td>
<td>67</td>
</tr>
<tr>
<td>3.2.23 AT+CRAS</td>
<td>Phone Activity Status</td>
<td>68</td>
</tr>
<tr>
<td>3.2.24 AT+CPPR</td>
<td>Find Phonebook Entries</td>
<td>69</td>
</tr>
<tr>
<td>3.2.25 AT+CPPR</td>
<td>Read Current Phonebook Entries</td>
<td>70</td>
</tr>
<tr>
<td>3.2.26 AT+CPPS</td>
<td>Select Phonebook, Memory Storage</td>
<td>71</td>
</tr>
<tr>
<td>3.2.27 AT+CPPW</td>
<td>Write Phonebook Entry</td>
<td>72</td>
</tr>
<tr>
<td>3.2.28 AT+CPIN</td>
<td>Enter PIN</td>
<td>73</td>
</tr>
<tr>
<td>3.2.29 AT+CPWD</td>
<td>Change Password</td>
<td>74</td>
</tr>
<tr>
<td>3.2.30 AT+CR</td>
<td>Service Reporting Control</td>
<td>75</td>
</tr>
<tr>
<td>3.2.31 AT+CRTC</td>
<td>Set Cellular Result Codes for Incoming Call Indication</td>
<td>76</td>
</tr>
<tr>
<td>3.2.32 AT+CRSD</td>
<td>Network Registration</td>
<td>77</td>
</tr>
<tr>
<td>3.2.33 AT+CRST</td>
<td>Select Radio Link Protocol Parameters</td>
<td>78</td>
</tr>
<tr>
<td>3.2.34 AT+CRSM</td>
<td>Restricted Adj Access</td>
<td>79</td>
</tr>
<tr>
<td>3.2.35 AT+CRQ</td>
<td>Signal Quality Report</td>
<td>80</td>
</tr>
<tr>
<td>3.2.36 AT+CLASS</td>
<td>FAX: Select, Read or Test Service Class</td>
<td>81</td>
</tr>
<tr>
<td>3.2.37 AT+CM</td>
<td>FAX Report Manufactured ID</td>
<td>82</td>
</tr>
<tr>
<td>3.2.38 AT+CMF</td>
<td>FAX: Report Model ID</td>
<td>83</td>
</tr>
<tr>
<td>3.2.39 AT+CMR</td>
<td>FAX: Report Revision ID</td>
<td>84</td>
</tr>
<tr>
<td>3.2.40 AT+CT</td>
<td>Tone Duration</td>
<td>85</td>
</tr>
<tr>
<td>3.2.41 AT+CVT</td>
<td>DTMF and Tone Generation</td>
<td>86</td>
</tr>
<tr>
<td>3.2.42 AT+CMUX</td>
<td>Multiplex Control</td>
<td>87</td>
</tr>
<tr>
<td>3.2.43 AT+CNEM</td>
<td>Subscriber Number</td>
<td>88</td>
</tr>
<tr>
<td>3.2.44 AT+CPOL</td>
<td>Preferred Operator Line</td>
<td>89</td>
</tr>
<tr>
<td>3.2.45 AT+CRPN</td>
<td>Read Operator Name</td>
<td>90</td>
</tr>
<tr>
<td>3.2.46 AT+CTN</td>
<td>Set Phone Functionality</td>
<td>91</td>
</tr>
<tr>
<td>3.2.47 AT+CCLK</td>
<td>Clock</td>
<td>92</td>
</tr>
<tr>
<td>3.2.48 AT+CSIM</td>
<td>Generic SIM Access</td>
<td>93</td>
</tr>
<tr>
<td>3.2.49 AT+CLAM</td>
<td>Alert Sound Mode</td>
<td>94</td>
</tr>
<tr>
<td>3.2.50 AT+CLAS</td>
<td>Alert Sound Select</td>
<td>95</td>
</tr>
<tr>
<td>3.2.51 AT+CRSL</td>
<td>Ringer Sound Level</td>
<td>96</td>
</tr>
<tr>
<td>3.2.52 AT+DLVL</td>
<td>Loud Speaker Volume Level</td>
<td>97</td>
</tr>
<tr>
<td>3.2.53 AT+CMUT</td>
<td>Mute Control</td>
<td>98</td>
</tr>
<tr>
<td>3.2.54 AT+CPUC</td>
<td>Price Per Unit and Currency Table</td>
<td>99</td>
</tr>
<tr>
<td>3.2.55 AT+CCWE</td>
<td>Call Meter Maximum Event</td>
<td>100</td>
</tr>
<tr>
<td>3.2.56 AT+CBC</td>
<td>Battery Charge</td>
<td>101</td>
</tr>
</tbody>
</table>

5 AT Commands for SIM Application Toolkit

6 AT Commands for SIM Special for SIMCOM

126

6.1 Overview

6.2 Detailed Descriptions of Commands

6.3.1 AT+CSIM | Set SIM Application Toolkit

6.4 AT+CSIM | Set SIM Application Toolkit
Smart Machine Target Decision

6.2.5.2 A-TCELLLOK Set the List of APCR which Needs to be Locked 164
6.2.5.3 A-TELUGS Set the Time Period of New Light 164
6.2.5.4 A-CWOMADE Indicates If the Module Is Powered Off 165
6.2.5.5 A-CHIUZIERING Use the Baseline Signal in the Incoming Call Ring 166
6.2.5.6 A-CEXTISENTE Close or Open the Microphone 166
6.2.5.7 A-CSTSELIG Close the Set Light or Open it to Shining 167
6.2.5.8 A-CHRISTLE Set the White List 167
6.2.5.9 A-CSYSLACU Acceptable User Response Speed 167
6.2.5.10 A-CSTICAN Performing A Net Surveyor to Show All The Calls Information 168
6.2.5.11 A-CNIN Enable the Indication of GPRS States 169
6.2.5.12 A-CVIPFD Enable Keypad Indication 169
6.2.5.13 A-LCCIS Uplink Unsupplementary Service Date 170
6.2.5.14 A-CLSTICLOL Close or Open the Function of Lock Network 171
6.2.5.15 A-CNIPNPLMT Set MCC/MMSC List for Lock Network 172
6.2.5.16 A-CSTANLEVEL Set the Sound Level of Special AT Command 172

7 AT Commands for GPRS Support
7.1 Overview of AT Commands for GPRS Support 174
7.2 Detailed Descriptions of AT Commands for GPRS Support 174
7.2.1 A-TCOATT Attack or Detach From GPRS Service 174
7.2.2 A-CDONT Define PDP Context 175
7.2.3 A-CSDQIG Quality of Service Profile (Maximum Acceptable) 177
7.2.4 A-CSDQIQG Quality of Service Profile (Requested) 178
7.2.5 A-CGATT PDP Context Activation or Deactivation 179
7.2.6 A-CSUBDATA Enter Data State 180
7.2.7 A-CSCOPAR Show PDP Address 180
7.2.8 A-CCLASSS GPRS Mobile Station Class 181
7.2.9 A-CGRFFP Control Unacknowledged GPRS Data Reporting 183
7.2.10 A-CHGRFFP Network Registration Status 184
7.2.11 A-CMSGS Select Service for MO SMS Messages 185

8 AT Commands for TCPIP Application Toolkit 187
8.1 Overview 187
8.2 Detailed Descriptions of Commands 188
8.2.1 A-CHRES Start Up Multi-IP Connection 188
8.2.2 A-CHTPSTART Start Up TCP IP Connection 188
8.2.3 A-CHTPSEND Send Data Through TCP IP Connection 190
8.2.4 A-CHTPQAND Select Data Transmission Mode 192
8.2.5 A-CHTPQACK Query Previous Connection/Data Transmitting Status 193
8.2.6 A-CHTCPLOSE Close TCP IP Connection 194
8.2.7 A-CHTPDIS Connect TCP IP Data Control 194
8.2.8 A-CHTPSEND Set Local Port 195
8.2.9 A-CHTCPST Set Task and Set API USER NAME, PASSWORD 196
8.2.10 A-CHTCP Bring Up Windows Connection with GPRS /CSD 197

SIM080_ATCommands Manual_V1.11 10 2014.10.20
ATD/ATH – Call & hang up
AT+CLIP - Calling Line Identification Presentation
  (the command shows the caller’s metadata)
AT+CLIR - Calling Line Identification Restriction
AT+MORING - Show State of Mobile Originated Call
  (the command shows info when the phone tone sounds in the receiver)

AT+CEER - Extended Error Report
AT+VTS - DTMF tone generation
AT+EXUNSOL - Enable or Disable Proprietary Unsolicited Indications
AT+CLCC - List Current Calls of ME
AT+CRC - Set Cellular Result Codes for Incoming Call Indication
AT+COLP - Connected Line Identification Presentation
2.2.3 ATDU Mobile Originated Call to Dialed Number

**ATDU Mobile Originated Call to Dialed Number**

**Execution:**
- Command: ATDU=<value> where <value> is an integer command.

**Response:**
- This command can be used to set up outgoing voice, data or fax calls. It also serves to control supplementary services.
- Note: This command may be aborts generally by receiving an ATH command or a character during execution. The aborting is not possible during some states of connection establishment such as handshaking.
- If an error is related to ME functionality
  - +CME ERROR: <err>
- If no dial tone and (parameter setting ATX2 or ATX4)
  - NO DIALTONE
- If busy and (parameter setting ATX3 or ATX4)
  - BUSY
- If a connection cannot be established
  - NO CARRIER
- If the remote station does not answer
  - NO ANSWER
- If connection successful and non-voice call,
  - CONNECT=<text> TA switches to data mode.
  - Note: <text> output only if ATX-value parameter setting with the
  - <value>=>0

2.2.8 ATDH Disconnect Existing Connection

**ATDH Disconnect Existing Connection**

**Execution:**
- Command: ATDH=<value>

**Response:**
- Disconnect existing call by local TE from Command line and terminate call
  - OK
- Note: OK is issued after circuit 199(DCD) is turned off, if it was previously on.

**Parameter:**
- 0 Disconnect ALL calls on the channel the command is requested. All active or waiting calls, CS data calls, GPRS call of the channel will be disconnected.
  - 1 Disconnect all calls on ALL connected channels. All active or waiting calls, CS data calls, GPRS call will be disconnected. (close up of all calls of the ME)
  - 2 Disconnect all connected CS data call only on the channel the command is requested. (speech calls (active or waiting) or GPRS calls are not disconnected)
  - 3 Disconnect all connected GPRS calls only on the channel the command is requested (speech calls (active or waiting) or CS data calls are not disconnected.
  - 4 Disconnect all CS calls (either speech or data) but does not disconnect waiting call (either speech or data) on the channel the command is requested.
  - 5 Disconnect waiting call (either speech or data) but does not disconnect other active calls (either CS speech, CS data or GPRS) on the channel the command is requested. (rejection of incoming call)
### 3.2.18 AT+CLIP Calling Line Identification Presentation

#### AT+CLIP Calling Line Identification Presentation

**Test Command**

**AT+CLIP?**

**Response**

+CLIP: (list of supported a=a)

**OK**

**Parameter**

See Test Command

**Read Command**

**AT+CLIP?**

**Response**

+CLIP: "a=a; "

**OK**

If error is related to ME functionality:

+CME ERROR: <err>

**Parameters**

See Read Command

**Write Command**

**AT+CLIP=a=a**

TE enables or disables the presentation of the CLI at the TE. It has an effect on the execution of the supplementary service CLIP in the network.

**OK**

If error is related to ME functionality:

+CME ERROR: <err>

**Parameters**

See Write Command

---

### 3.2.19 AT+CLR Calling Line Identification Restriction

#### AT+CLR Calling Line Identification Restriction

**Test Command**

**AT+CLR?**

**Response**

+CLR: (list of supported a=a)

**OK**

**Parameter**

---

---

---
DEMO – Abusing GSM using covert channels with AT commands

Antenna Mobile Phone -> GSM Network -> Antenna Mobile Phone

Setup Tx
ATD#31#636666284
Sending: bit 1
ACK

Sending: bit 1

Setup Rx
Missed call
Hidden phone number

Received Call
ATD 636666284
Sending: bit 0

Received Call

AT+CHUP
(BUSY)

Missed call

Detail of protocol

Aihasd SIM900 GSM
Arduino
DEMO – Abusing GSM using covert channels with AT commands
Demo CovertChannel - HackInTheBox 2018, April 13, Amsterdam.
By Alfonso Muñoz (@mindcrypt) and Jorge Cuadrado (@coke727).

$dispositivo = 'RECEIVER'
$metodo_ocultacion = 'missed call & hidden number'
$mobile_number = '630XXXXX094'
Covert channel => Hidden capacity (Worst case)

Steganographic techniques considering only ONE SIM + ONE ANTENNA MOBILE PHONE

- Missed calls – Hidden phone number (8-10 bits/min)
- Duration of the call (aprox 10 bits/min)
- Return codes & network disconnection
- Mixing steganographic techniques (12 bits/min)

What means this?

Capacity/min = aprox 12 bits/min
→ 3 min = 1 IPv4 address | 3 min = TOR addr (URL shortener) | 3 min = GPS coord...

Capacity/hour = aprox 720 bits/hour
→ IPv4+ addr TOR + addr Bitcoin + GPS Coord + date/time + cryptographic pass + ...

Capacity/day = aprox 17.280 bits/day
Covert channel => Capacity + Delay + Stability

Stability

• No SIM ("registered" and "unregistered/anonymous" prepaid SIM) has been banned in the last 5 months (Spain) – 1 hour per day sending information (aprox 720 bits/hour per SIM)

• Example: Maximum Testing time - 2 uninterrupted days – Ej./ 34.560 missed calls – 34.560 bits (We stopped the test...)

Delay Vs Capacity Vs Invisibility → Amplification techniques

• Virtual phone numbers (Configuration by Internet but working in a 2G Scenario without Internet)
• Caller ID Spoofing & Internet Resources & Tricks (Working in a 2G & Internet Scenario)
Virtual phone numbers => Higher Capacity with = SIMs+Antenna

• Higher hiding capacity → More antennas, more SIM cards (*)

• Complement or alternative: Virtual phone numbers (free/anonymous and registered/paid)
Ejemplo – Abusando GSM usando canales ocultos con comandos AT + Números Virtuales

Emisor A

Virtual Number 0 (0000b)

Virtual Number 1 (0001b)

... Virtual Number 14 (1110b)

Virtual Number 15 (1111b)

Receptor B

Enviar 0001b, Llamar a Número 1

Llamada recibida del Número 1, decodificar 0001b

Ej/ 7*log₂(Virtual Numbers) bits/min → Ej/ 28 bits/min, 7 llamadas/min
Do The Impossible
See The Invisible
Row! Row!
Fight The Power!
Touch The Untouchable
Break The Unbreakable
Row! Row!
Fight The Power!
What You Gonna Do Is What You Wanna Do
Just Break The Rule, And You See The Truth…

Gurren_Laggann – Row Row Fight The Power
DEMO – Abusing GSM using covert channels with AT commands + Virtual Numbers
“Phreaking” by Internet & Caller ID Spoofing...

- **Services/Devices “with functionalities to call”**
  - Missed call / SMS “free” / IoT / Shodan ...

- **Caller ID Spoofing** (Spoofcard, CallerIdFaker, Spooftel...)
  - ...

- **Combination & Amplification**

Caller ID Spoofing (Phone Number): `<Country><City><Number>` 2+2+9 digits

Hiding capacity:

- $VR_{10,13} = 10^{13} \rightarrow \frac{13}{\log 2} = 43$ bits
- $VR_{10,9} = 10^9 \rightarrow \frac{9}{\log 2} = 29$ bits
**Demo: Covert channel – Caller ID Spoofing**

Alphabet: Capital letters, lowercase, numbers (64 car $\rightarrow 2^6 \rightarrow 6$ bits)

Shortened url from 3 to 5 char $\rightarrow 18$ to 30 bits (shortened url can have a lot of info)

Ej/ tiny.cc/A2bE $\rightarrow 24$ bits

To convert this code to binary $\rightarrow$ Binary to a phone number (emitter) $\rightarrow$ Call to the receiver $\rightarrow$ Apply inverse process
Demo: Covert channel – Caller ID Spoofing
Demo: Covert channel – Caller ID Spoofing
HackintheBox’s Blue Box System V1.0

Blue Box coded by @mindcrypt/@coke727

Dial tollfreenumber
Set a trunk and dial your number

Enter #:_________________
Call me Maybe! – Establishing covert channels by abusing GSM AT Commands

Dr. Alfonso Muñoz (@mindcrypt) - Jorge Cuadrado (@Coke727)