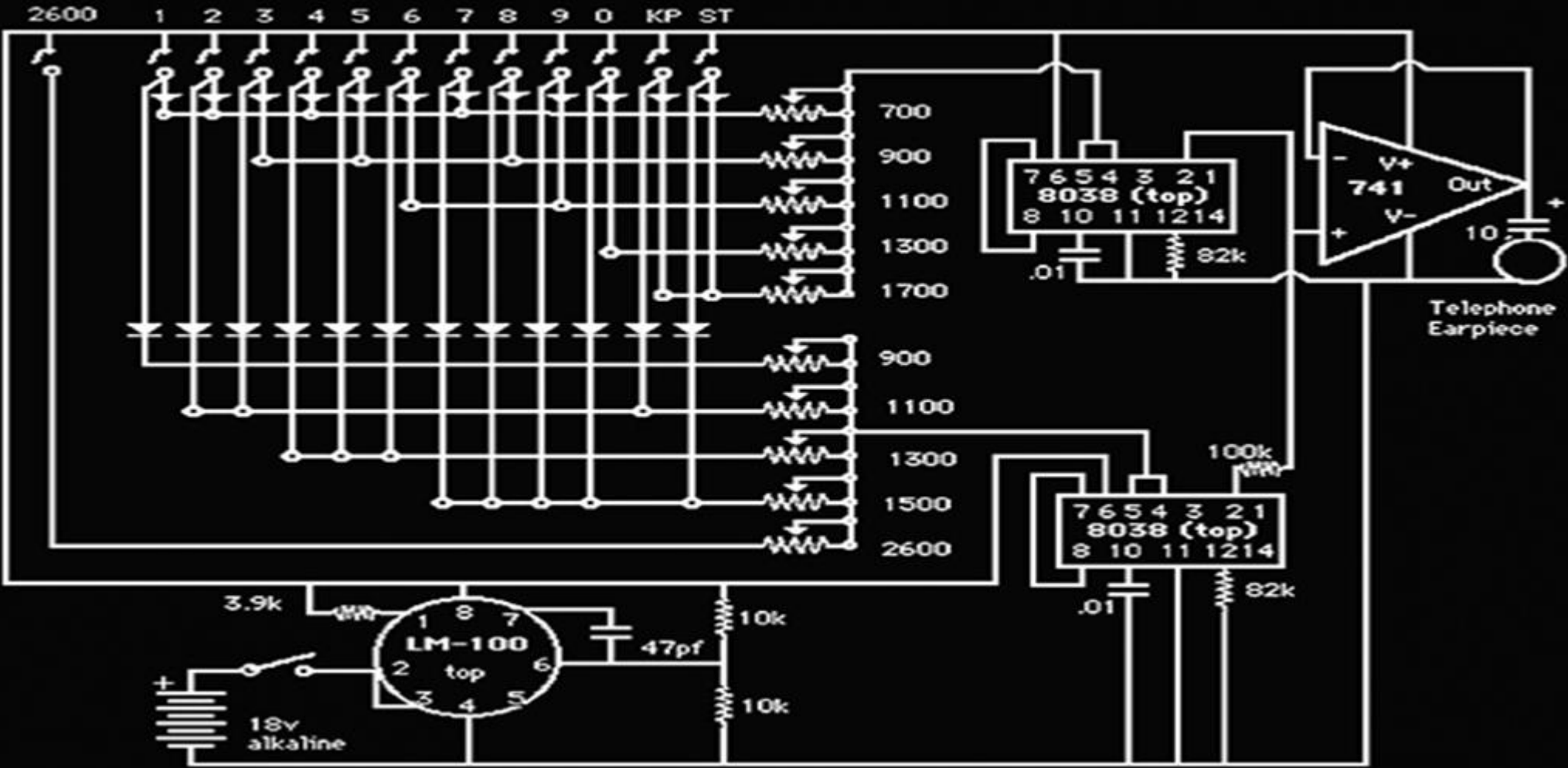
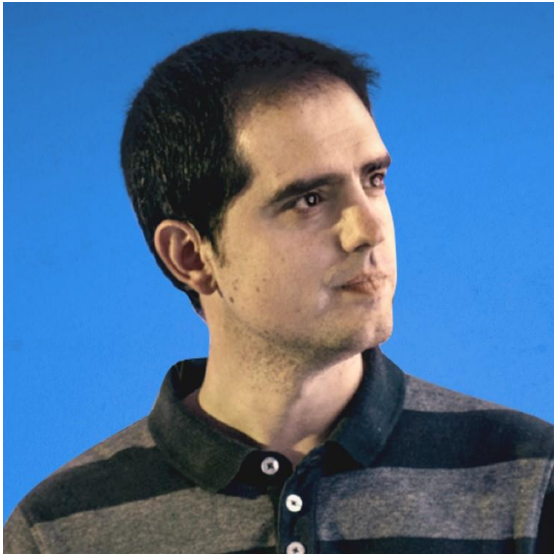


Call me Maybe! – Establishing covert channels by abusing GSM AT Commands



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/alfonsomuñoz & <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

2600

The Monthly Journal of the American Hacker



Volume 4, Number 6

June, 1987

\$2



Disclaimer

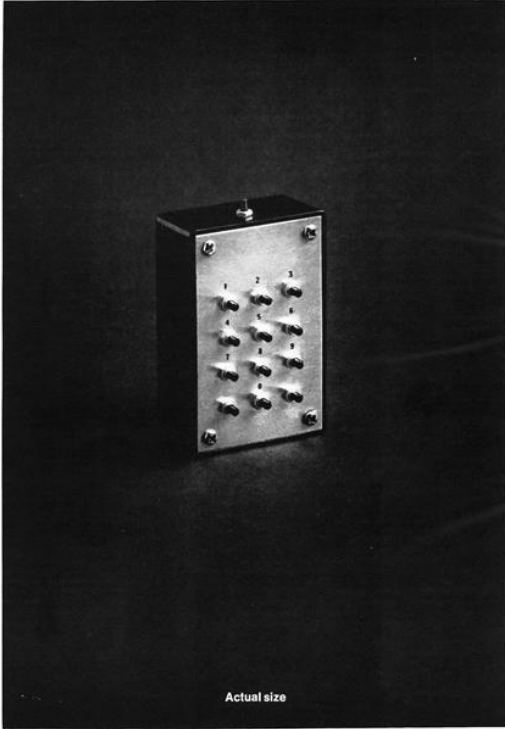


Phreaking

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

by Ron Rosenbaum

A story so incredible it may even make you feel sorry for the phone company

The Blue Box Is Introduced: Its Qualities Are Remarkable

I am in the extensively furnished living room of Al Gilbertson, the creator of the "blue box." Gilbertson is holding one of his shiny black-and-silver "blue boxes" comfortably in the palm of his hand, pointing out the thirteen little red push buttons sticking up from the console. He is dancing his fingers over the buttons, tapping out discordant beeping electronic jingles. He is trying to explain to me how his little blue box does nothing less than place the entire telephone system of the world, satellites, cables and all, at the service of the blue-box operator, free of charge.

"That's what it does. Essentially it gives you the power of a super operator. You seize a tandem with this top button," he presses the top button with his index finger and the blue box emits a high-pitched cheep, "and like that"—cheep goes the blue box again—"you control the phone company's long-distance switching systems from your cute little Princess phone or any old pay phone. And you've got anonymity. An operator has to operate from a definite location: the phone company knows where she is and what she's doing. But with your beeper box, once you hop onto a trunk, say from a Holiday Inn 800 (toll-free) number, they don't know where you are, or where you're coming from, they don't know how you slipped into their lines and peeped up in that 800 number. They don't even know anything illegal is going on. And you can obscure your origins through as many levels as you like. You can call next door by way of White Plains, then over to Liverpool by cable, and then back here by satellite. You can call yourself from one pay phone all the way around the world to a pay phone next to you. And you get your dime back too."

"And they can't trace the calls? They can't charge you?"

"Not if you do it the right way. But you'll find that the free-call thing isn't really as exciting at first as the feeling of power you get from having one of these babies in your hand. I've watched people when they first get hold of one of these things and start using it, and discover they can make connections, set up crisscross and zigzag switching patterns back and forth across the world. They hardly talk to the people they finally reach. They say hello and start thinking of what kind of call to make next. They go a little crazy." He looks down at the neat little package in his palm. His fingers are still dancing, tapping out beeper patterns.

"I think it's something to do with how small my models

"The real name has been changed.
Photographed by Ronald Barnett

are. There are lots of blue boxes around, but mine are the smallest and most sophisticated electronically. I wish I could show you the prototype we made for our big syndicate order."

He sighs. "We had this order for a thousand beeper boxes from a syndicate front man in Las Vegas. They use them to place bets coast to coast, keep lines open for hours, all of which can get expensive if you have to pay. The deal was a thousand blue boxes for \$500 apiece. Before then we retailed them for \$1,500 apiece, but \$200,000 in one lump was hard to turn down. We had a manufacturing deal worked out in the Philippines. Everything ready to go. Anyway, the model I had ready for limited mass production was small enough to fit inside a flip-top Marlboro box. It had flush touch panels for a keyboard, rather than these unsightly buttons sticking out. Looked just like a tiny portable radio. In fact, I had designed it with a tiny transistor receiver to get one AM channel, so in case the law became suspicious the owner could switch on the radio part, start snapping his fingers, and no one could tell anything illegal was going on. I thought of everything for this model—I had it lined with a band of thermite which could be ignited by radio signal from a tiny button transmitter on your belt, so it could be burned to ashes instantly in case of a bust. It was beautiful. A beautiful little machine. You should have seen the faces on these syndicate guys when they came back after trying it out. They'd hold it in their palm like they never wanted to let it go, and they'd say, 'I can't believe it. I can't believe it.' You probably won't believe it until you try it."

The Blue Box Is Tested: Certain Connections Are Made

About eleven o'clock two nights later Fraser Lacey has a blue box in the palm of his left hand and a phone in the palm of his right. He is standing inside a phone booth next to an isolated shut-down motel off Highway 1. I am standing outside the phone booth.

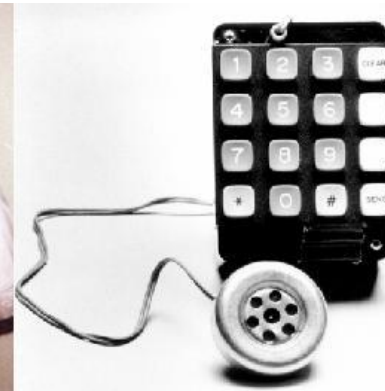
Fraser likes to show off his blue box for people. Until a few weeks ago when Pacific Telephone made a few arrests in his city, Fraser Lacey liked to bring his blue box** to parties. It never failed: a few cheeps from his device and Fraser became the center of attention at the very hippest of gatherings, playing phone tricks and doing request numbers for hours. He began to take

**The particular blue box, like most blue boxes, is not blue. Blue boxes have come to be called "blue boxes" rather than "blue boxes" to be blue or to distinguish them from "blue boxes" which have no device, usually a resistor in series, which, when plugged into some phone, allow all incoming calls to be made without charge to the caller.



<https://www.thingiverse.com/thing:2630646/#files>

<http://www.historyofphonephreaking.org/faq.php> & <http://explodingthephone.com>





The beginning



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



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

Mobile phone: Golden nugget!



<https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data>



WikiLeaks #Vault7 confirms CIA can effectively bypass Signal + Telegram + WhatsApp + Confide encryption
wikileaks.org/ciav7p1

RETWEETS 5,745 LIKES 4,565

6:29 AM - 7 Mar 2017

184 5.7K 4.6K



What is being hacked into?

Signalling System No 7 (SS7), which is called Common Channel Signalling System 7 (CCSS7) in the US or Common Channel Interoffice Signaling 7 (CCIS7) in the UK, is a system that connects one mobile phone network to another.

It was first developed in 1975 and has many variants. Most networks use protocols defined by the American National Standards Institute and the European Telecommunications Standards Institute.

What does SS7 normally do?

SS7 is a set of protocols allowing phone networks to exchange the information needed for passing calls and text messages between each other and to ensure correct billing. It also allows users on one network to roam on another, such as when travelling in a foreign country.

What can access to SS7 enable hackers to do?

Once they have access to the SS7 system, a hacker can essentially have access to the same amount of information and snooping capabilities as security services.

They can transparently forward calls, giving them the ability to record or listen in to them. They can also read SMS messages sent between phones, and track the location of a phone using the same system that the phone networks use to help keep a constant service available and deliver phone calls, texts and data.

<https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls>

<http://www.securitybydefault.com/2015/01/hacking-en-redes-ss7.html>

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

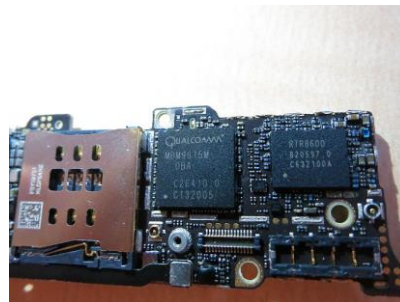
The SMS of Death Mobile Phone Attack Explained

<http://www.infosecisland.com/blogview/12656-The-SMS-of-Death-Mobile-Phone-Attack-Explained.html>

Nearly 1 billion phones can be hacked with 1 text

<http://fortune.com/2015/07/27/stagefright-android-vulnerability-text/>

Baseband vulnerability could mean undetectable, unblockable attacks on mobile phones



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

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

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.

<https://www.cnet.com/news/researchers-can-attack-mobile-phones-via-spoofed-sms-messages/>

Secraphony...

Chipcard
(with Keys)

2 x 40 LC Display

Menu
Buttons

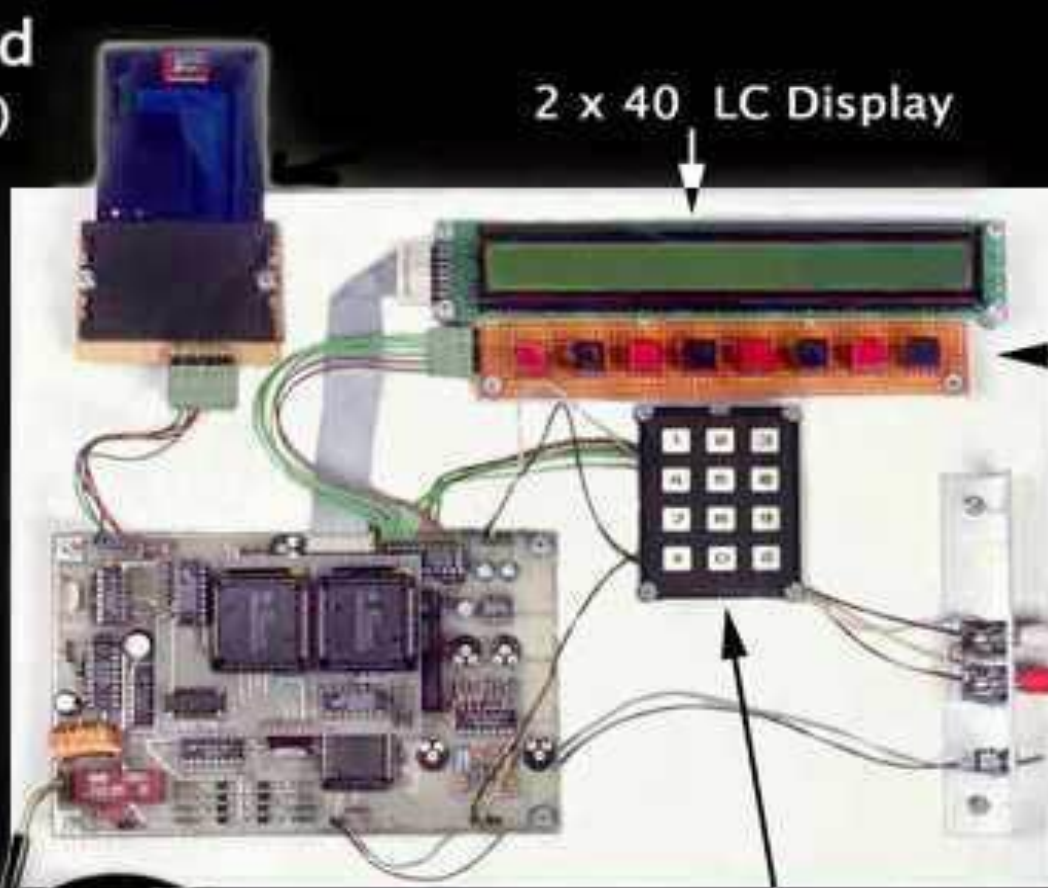
Headset

Dialblock

ISDN NTBA

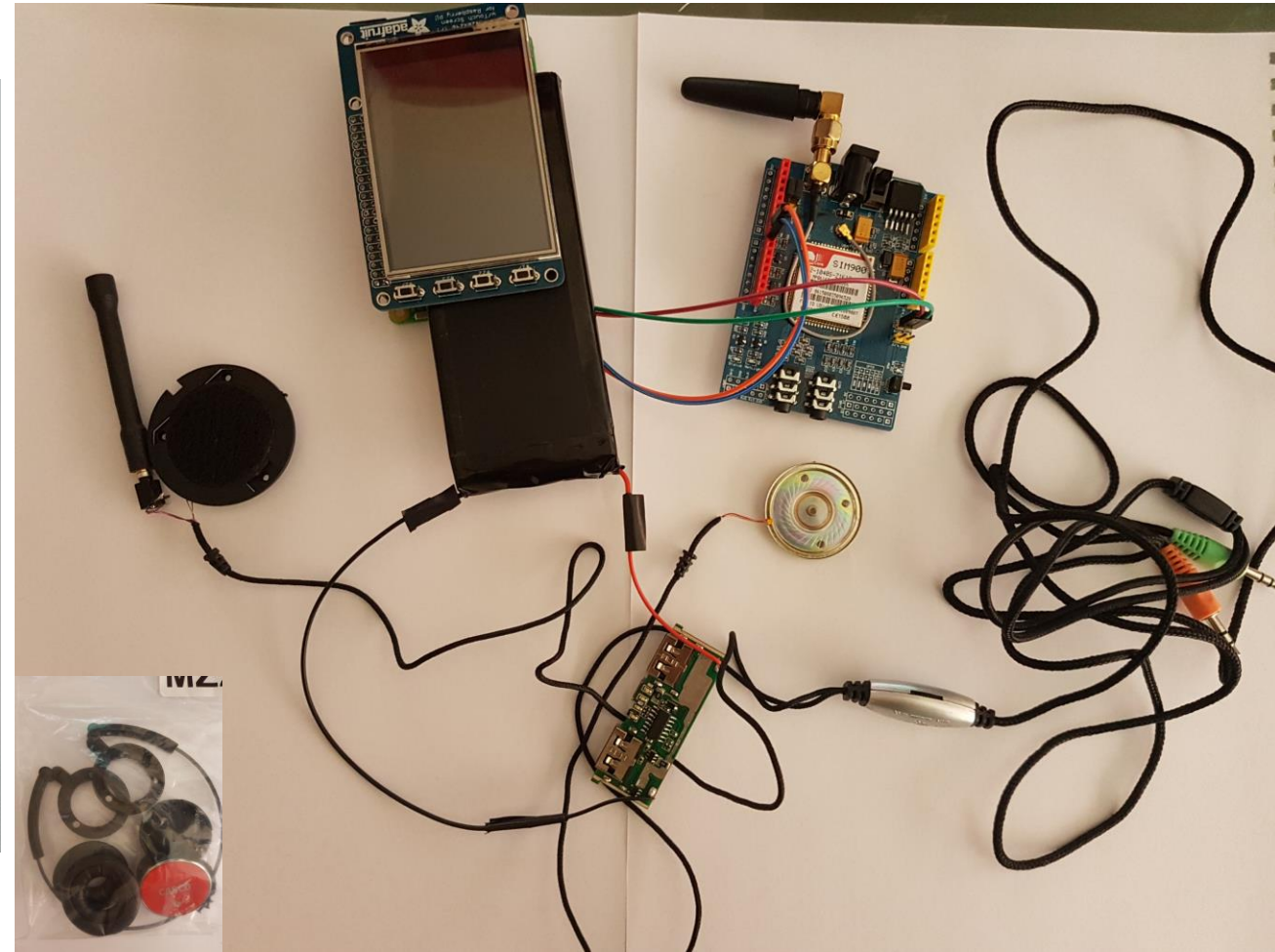
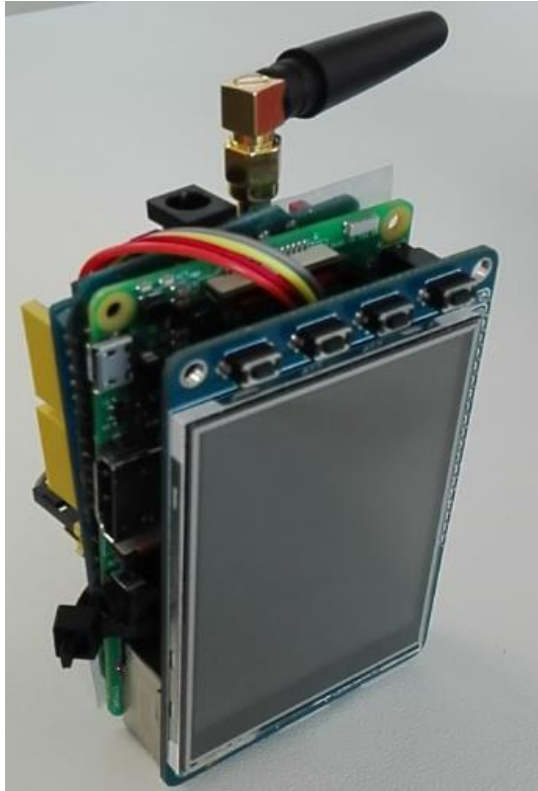


Tron - Spring 1998



1998: TRONs CRYPTOFON

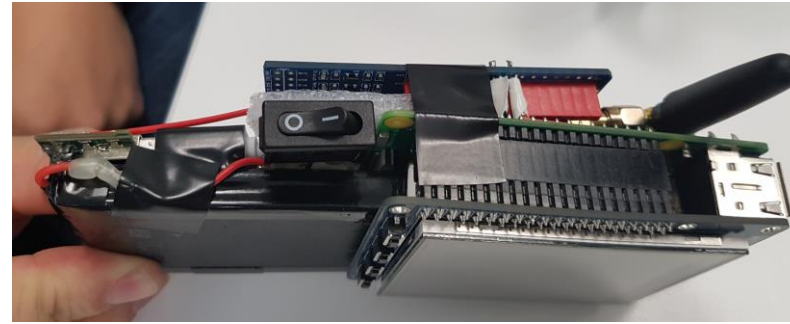
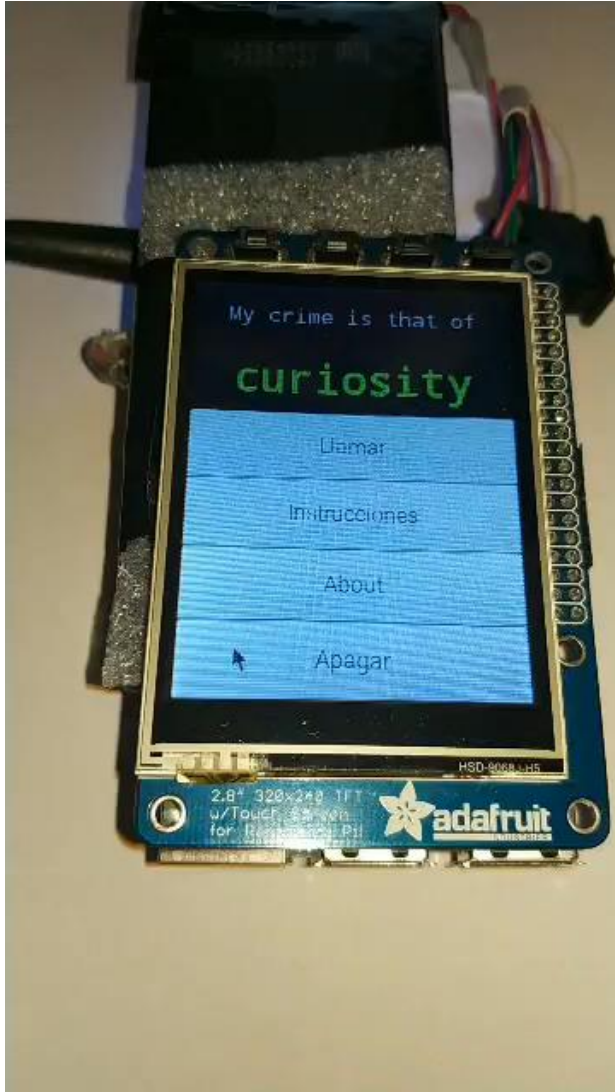
Homemade Phreaking - Making our own mobile phone



Yes, I am a criminal. My crime is that of curiosity (The Mentor - January 8, 1986)
<http://phrack.org/issues/7/3.html>



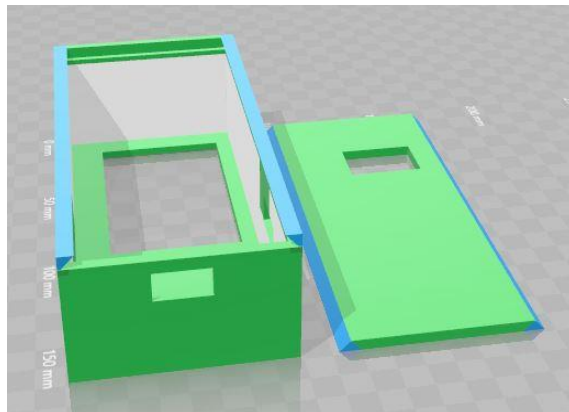
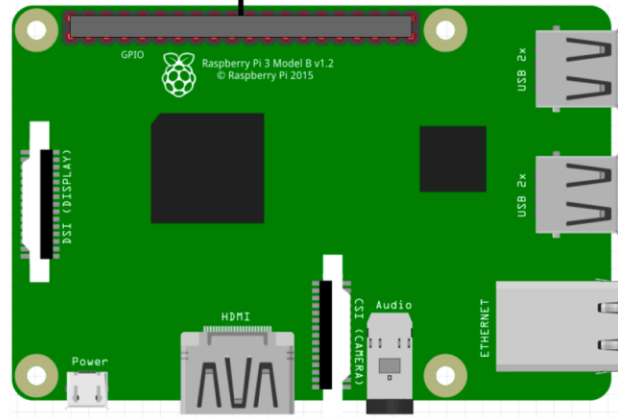
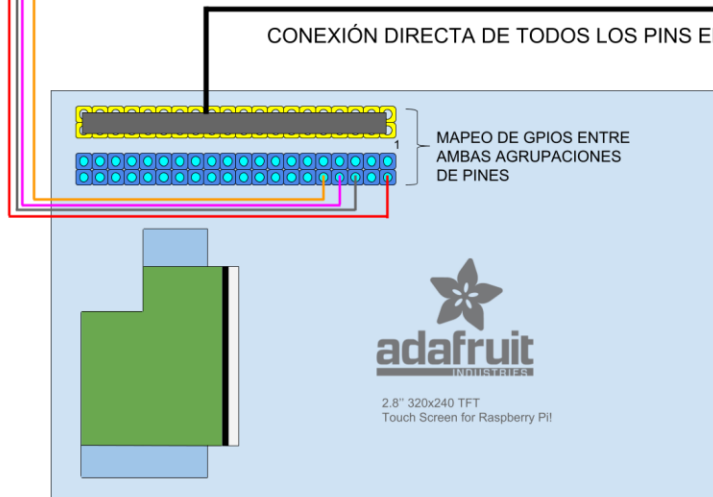
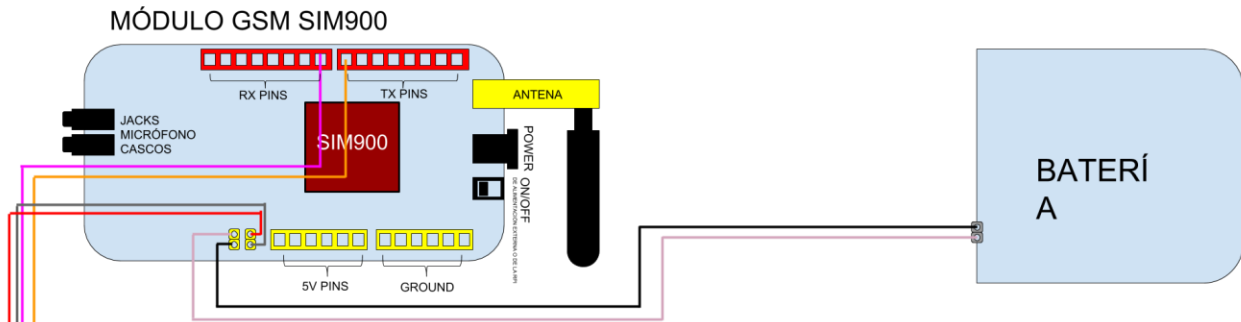
Homemade Phreaking - Making our own mobile phone



HAPPY
RELEASE
DAY!

<https://github.com/jorcuad/FreePhone/wiki>





HAPPY
RELEASE
DAY!

<https://github.com/jorcuad/FreePhone/wiki>



Our research



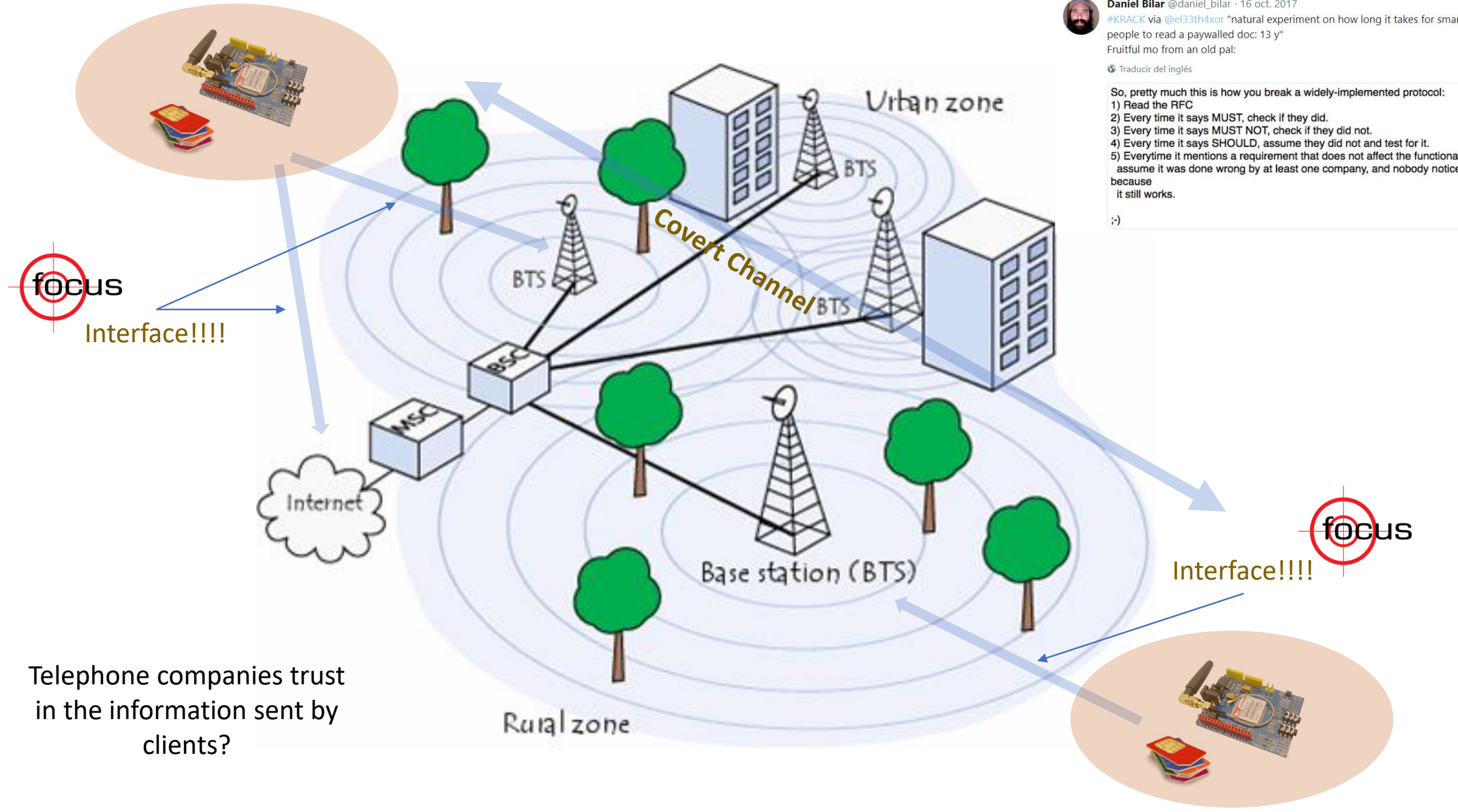
Covert Channel

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)



Retwitteado por ti
Daniel Bilar @daniel_bilar · 16 oct. 2017
#KRACK via @e133th4xor "natural experiment on how long it takes for smart people to read a paywalled doc: 13 y"
Fruitful mo from an old pal:
Traducir del inglés

So, pretty much this is how you break a widely-implemented protocol:
1) Read the RFC
2) Every time it says MUST, check if they did.
3) Every time it says MUST NOT, check if they did not.
4) Every time it says SHOULD, assume they did not and test for it.
5) Everytime it mentions a requirement that does not affect the functionality, assume it was done wrong by at least one company, and nobody noticed because it still works.
;-)



Antena GSM - Client attack

<http://simcom.ee/modules/gsm-gprs/sim900/>



Aihasd SIM900 GSM GPRS Module Quad-Band Development Board Wireless Data for Arduino Raspberry Pi
21 Euros - <http://goo.gl/8RgxxZ>

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



SIMS GSM - Client attack



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".^{[13][14]} 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.

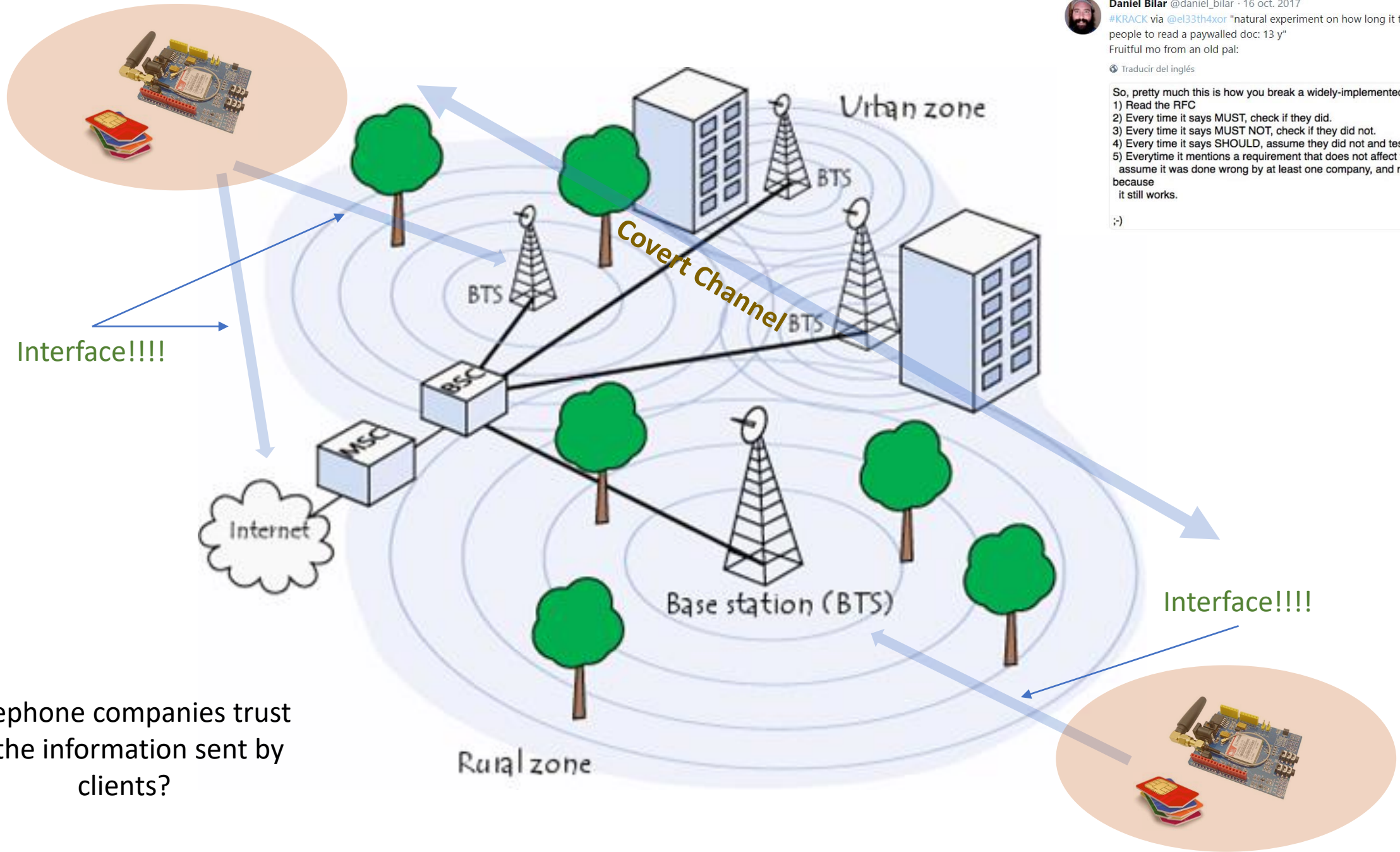
The law of conservation of data on electronic communications and public communications networks (Law 25/2007 October DE18) states that service operators should maintain a prepaid SIM logbook stating the identity of the each customer. Data may be required by order of a judge, in order to detect, investigate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



Retwitteado por ti
Daniel Bilar @daniel_bilar · 16 oct. 2017
#KRACK via @e33th4xor "natural experiment on how long it takes for smart people to read a paywalled doc: 13 y"
Fruitful mo from an old pal:
Traducir del inglés

- So, pretty much this is how you break a widely-implemented protocol:
- 1) Read the RFC
 - 2) Every time it says MUST, check if they did.
 - 3) Every time it says MUST NOT, check if they did not.
 - 4) Every time it says SHOULD, assume they did not and test for it.
 - 5) Everytime it mentions a requirement that does not affect the functionality, assume it was done wrong by at least one company, and nobody noticed because it still works.
- :)



Interface!!!!

Interface!!!!

Telephone companies trust in the information sent by clients?



AT commands & Standards

<http://simcom.ee/documents/?dir=SIM900>



SIM900 AT Commands Manual_V1.11

1.3 Conventions and abbreviations

In this document, the GSM engines are referred to as following term:

- 1) ME (Mobile Equipment);
- 2) MS (Mobile Station);
- 3) TA (Terminal Adapter);
- 4) DCE (Data Communication Equipment) or facsimile DCE (FAX modem, FAX board);

In application, controlling device controls the GSM engine by sending AT Command via its serial interface. The controlling device at the other end of the serial line is referred to as following term:

- 1) TE (Terminal Equipment);
- 2) DTE (Data Terminal Equipment) or plainly "the application" which is running on an embedded system;

1.4 AT Command syntax

The "AT" or "at" prefix must be set at the beginning of each Command line. To terminate a Command line enter <CR>.

Commands are usually followed by a response that includes. "<CR><LF><response><CR><LF>"

Throughout this document, only the responses are presented, <CR><LF> are omitted intentionally.

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:

- [1] 3GPP TS 27.005: Use of Data Terminal Equipment – Data Circuit terminating Equipment (DTE – DCE) interface for Short Message Service (SMS) and Cell Broadcast Service (CBS).
- [2] 3GPP TS 27.007: AT command set for User Equipment (UE).
- [3] ITU-T V.25 ter: Data communication over the telephone network – Serial asynchronous automatic dialing and control.
- [4] TIA/EIA-578-A: Facsimile Digital Interfaces – Asynchronous Facsimile DCE Control Standard, Service Class
- [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

Version History.....	3
Contents	6
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 syntax	15
1.4.1 Basic syntax	16
1.4.2 S Parameter syntax.....	16
1.4.3 Extended Syntax.....	16
1.4.4 Combining AT commands on the same Command line.....	17
1.4.5 Entering successive AT commands on separate lines.....	17
1.5 Supported character sets.....	17
1.6 Flow control	17
1.6.1 Software flow control (XON/XOFF flow control).....	18
1.6.2 Hardware flow control (RTS/CTS flow control).....	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
2.2.1 A/ Re-issues the Last Command Given.....	20
2.2.2 ATA Answer an Incoming Call.....	20
2.2.3 ATD Mobile Originated Call to Dial A Number.....	21
2.2.4 ATD<n> Originate Call to Phone Number in Current Memory.....	23
2.2.5 ATD<str> Originate Call to Phone Number in Memory Which Corresponds to Field <str>.....	24
2.2.6 ATDL Redial Last Telephone Number Used.....	25
2.2.7 ATE Set Command Echo Mode.....	26
2.2.8 ATH Disconnect Existing Connection.....	27
2.2.9 ATI Display Product Identification Information	27
2.2.10 ATL Set Monitor speaker loudness.....	28
2.2.11 ATM Set Monitor Speaker Mode.....	28
2.2.12 +++ Switch from Data Mode or PPP Online Mode to Command Mode.....	28
2.2.13 ATO Switch from Command Mode to Data Mode.....	29
2.2.14 ATP Select Pulse Dialling.....	29
2.2.15 ATQ Set Result Code Presentation Mode.....	29

2.2.16 ATSO Set Number of Rings before Automatically Answering the Call.....	30
2.2.17 ATSS Set Command Line Termination Character.....	30
2.2.18 ATSA Set Response Formatting Character.....	31
2.2.19 ATSE Set Command Line Editing Character.....	31
2.2.20 ATSP Pause Before Blind Dialling.....	32
2.2.21 ATST Set Number of Seconds to Wait for Connection Completion.....	32
2.2.22 ATSC Set Number of Seconds to Wait for Comma Dial Modifier Encountered in Dial String of D Command.....	33
2.2.23 ATSD Set Disconnect Delay after Indicating the Absence of Data Carrier.....	33
2.2.24 ATT Select Tone Dialling.....	34
2.2.25 ATV TA Response Format.....	34
2.2.26 ATX Set CONNECT Result Code Format and Monitor Call Progress.....	35
2.2.27 ATZ Reset Default Configuration.....	35
2.2.28 AT&C Set DCD Function Mode.....	36
2.2.29 AT&D Set DTR Function Mode.....	36
2.2.30 AT&F Factory Defined Configuration.....	37
2.2.31 AT&V Display Current Configuration.....	39
2.2.32 AT&W Store Active Profile.....	39
2.2.33 AT+GCAP Request Complete TA Capabilities List.....	40
2.2.34 AT+GMI Request Manufacturer Identification.....	40
2.2.35 AT+GMM Request TA Model Identification.....	40
2.2.36 AT+GMR Request TA Revision Identification of Software Release.....	41
2.2.37 AT+GOI Request Global Object Identification.....	41
2.2.38 AT+GSN Request TA Serial Number Identification (IMEI).....	42
2.2.39 AT+ICF Set TE-TA Control Character Framing.....	42
2.2.40 AT+IPC Set TE-TA Local Data Flow Control.....	43
2.2.41 AT+IPR Set TE-TA Fixed Local Rate.....	44
2.2.42 AT+HVIC Disconnect Voice Call Only.....	45
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+CACM Accumulated Call Meter (ACM) Reset or Query.....	47
3.2.2 AT+CAMM Accumulated Call Meter Maximum (ACM max) Set or Query.....	48
3.2.3 AT+CAOC Advice of Charge.....	49
3.2.4 AT+CBST Select Bearer Service Type.....	50
3.2.5 AT+CCFC Call Forwarding Number and Conditions Control.....	51
3.2.6 AT+CCWA Call Waiting Control.....	52
3.2.7 AT+CEER Extended Error Report.....	54
3.2.8 AT+CGMI Request Manufacturer Identification.....	56
3.2.9 AT+COMM Request Model Identification.....	56
3.2.10 AT+CGMR Request TA Revision Identification of Software Release.....	57
3.2.11 AT+CGSN Request Product Serial Number Identification (Identical with +GSN).....	57
3.2.12 AT+CSCS Select TE Character Set.....	57



	3.2.13 AT+CSTA	Select Type of Address	58
④	3.2.14 AT+CHLD	Call Hold and Multiparty	59
	3.2.15 AT+CIMI	Request International Mobile Subscriber Identity	60
	3.2.16 AT+CLCC	List Current Calls of ME	61
	3.2.17 AT+CLCK	Facility Lock	62
	3.2.18 AT+CLIP	Calling Line Identification Presentation	64
	3.2.19 AT+CLIR	Calling Line Identification Restriction	65
	3.2.20 AT+CMEE	Report Mobile Equipment Error	66
	3.2.21 AT+COLP	Connected Line Identification Presentation	67
	3.2.22 AT+COPS	Operator Selection	68
	3.2.23 AT+CPAS	Phone Activity Status	70
Libreta	3.2.24 AT+CPBF	Find Phonebook Entries	70
Contacta	3.2.25 AT+CPBR	Read Current Phonebook Entries	71
	3.2.26 AT+CPBS	Select Phonebook Memory Storage	72
	3.2.27 AT+CPBW	Write Phonebook Entry	73
	3.2.28 AT+CPIN	Enter PIN	75
	3.2.29 AT+CPWD	Change Password	75
	3.2.30 AT+CR	Service Reporting Control	76
	3.2.31 AT+CRIC	Set Cellular Result Codes for Incoming Call Indication	77
	3.2.32 AT+CREG	Network Registration	78
	3.2.33 AT+CRLP	Select Radio Link Protocol Parameters	79
	3.2.34 AT+CRSM	Restricted SIM Access	80
	3.2.35 AT+CSQ	Signal Quality Report	81
	3.2.36 AT+FCLASS	FAX: Select, Read or Test Service Class	82
FAX	3.2.37 AT+FMI	FAX: Report Manufactured ID	82
	3.2.38 AT+FMM	FAX: Report Model ID	83
	3.2.39 AT+FMR	FAX: Report Revision ID	83
	3.2.40 AT+VTD	Tone Duration	84
④	3.2.41 AT+VTS	DTMF and Tone Generation	84
	3.2.42 AT+CMUX	Multiplexer Control	85
	3.2.43 AT+CNUM	Subscriber Number	87
	3.2.44 AT+CPOL	Preferred Operator List	87
	3.2.45 AT+COPN	Read Operator Names	88
CUP +	3.2.46 AT+CFUN	Set Phone Functionality	89
	3.2.47 AT+CCLK	Clock	90
	3.2.48 AT+CSIM	Generic SIM Access	91
	3.2.49 AT+CALM	Alert Sound Mode	91
	3.2.50 AT+CALS	Alert Sound Select	92
	3.2.51 AT+CRSL	Ringer Sound Level	93
	3.2.52 AT+CLVL	Loud Speaker Volume Level	93
	3.2.53 AT+CMUT	Mute Control	94
	3.2.54 AT+CPUC	Price Per Unit and Currency Table	95
	3.2.55 AT+CCWE	Call Meter Maximum Event	95
	3.2.56 AT+CBC	Battery Charge	96

	3.2.57 AT+CUSD	Unstructured Supplementary Service Data	97
	3.2.58 AT+CSNN	Supplementary Services Notification	98
	4	AT Commands According to GSM07.05	100
	4.1	Overview of AT Commands According to GSM07.05	100
	4.2	Detailed Descriptions of AT Commands According to GSM07.05	100
	4.2.1	AT+CMGD Delete SMS Message	100
	4.2.2	AT+CMGF Select SMS Message Format	101
	4.2.3	AT+CMGL List SMS Messages from Preferred Store	102
	4.2.4	AT+CMGR Read SMS Message	105
	4.2.5	AT+CMGS Send SMS Message	108
SMS	4.2.6	AT+CMGW Write SMS Message to Memory	109
	4.2.7	AT+CMSS Send SMS Message from Storage	111
	4.2.8	AT+CNMI New SMS Message Indications	112
	4.2.9	AT+CPMS Preferred SMS Message Storage	114
	4.2.10	AT+CREG Restore SMS Settings	115
	4.2.11	AT+CSAS Save SMS Settings	116
	4.2.12	AT+CSCA SMS Service Center Address	116
	4.2.13	AT+CSCB Select Cell Broadcast SMS Messages	117
	4.2.14	AT+CSDH Show SMS Text Mode Parameters	118
	4.2.15	AT+CSMP Set SMS Text Mode Parameters	119
	4.2.16	AT+CSMS Select Message Service	120
	4.2.17	AT+CMGS="<index>" Send SMS Message by Index	121
	5	AT Commands for SIM Application Toolkit	123
	5.1	Overview	123
	5.2	STK AT Command	123
	5.2.1	AT+PSSTKI SIM Toolkit Interface Configuration	123
	5.2.2	AT+PSSTK SIM Toolkit Control	124
	5.2.3	AT+PSSTKREJ Response Reject Message to STK Automatically	125
	6	AT Commands Special for SIMCOM	126
	6.1	Overview	126
	6.1.1	CLOSE OR OPEN THE FUNCTION OF LOCK NETWORK	127
	6.1.2	SET MCC&MNC LIST FOR LOCK NETWORK	127
	6.1.3	SET THE SOUND LEVEL OF SPECIAL AT COMMAND	127
	6.2	Detailed Descriptions of Commands	128
	6.2.1	AT+SIDET Change the Side Tone Gain Level	128
	6.2.2	AT+CPOWD Power Off	128
	6.2.3	AT+SPIC Times Remained to Input SIM PIN/PUK	129
	6.2.4	AT+CMIC Change the Microphone Gain Level	129
	6.2.5	AT+CALA Set Alarm Time	130
	6.2.6	AT+CALD Delete Alarm	131
	6.2.7	AT+CADC Read ADC	132



6.2.8 AT+CSNS	Single Numbering Scheme	132
6.2.9 AT+CDSCB	Reset Cell Broadcast	133
6.2.10 AT+CMOD	Configure Alternating Mode Calls	133
6.2.11 AT+CFGRI	Indicate R1 When Using URC	133
6.2.12 AT+CLTS	Get Local Timestamp	134
6.2.13 AT+CEXTHS	External Headset Jack Control	136
6.2.14 AT+CEXTBUT	Headset Button Status Reporting	136
6.2.15 AT+CSMINS	SIM Inserted Status Reporting	137
6.2.16 AT+CLDTMF	Local DTMF Tone Generation	138
6.2.17 AT+CDRIND	CS Voice/Data Call Termination Indication	139
6.2.18 AT+CSPN	Get Service Provider Name from SIM	140
6.2.19 AT+CCVM	Get and Set the Voice Mail Number on the SIM	140
6.2.20 AT+CBAND	Get and Set Mobile Operation Band	141
6.2.21 AT+CHF	Configure Hands Free Operation	142
6.2.22 AT+CHFA	Swap the Audio Channels	143
6.2.23 AT+CSCLK	Configure Slow Clock	143
6.2.24 AT+CENG	Switch On or Off Engineering Mode	144
6.2.25 AT+SCLASS0	Store Class 0 SMS to SIM When Received Class 0 SMS	146
6.2.26 AT+CCID	Show ICCID	146
6.2.27 AT+CMTE	Set Critical Temperature Operating Mode or Query Temperature	147
6.2.28 AT+CBTE	Battery Temperature Query	147
6.2.29 AT+CSDT	Switch On or Off Detecting SIM Card	147
6.2.30 AT+CMGDA	Delete All SMS	148
6.2.31 AT+STTONE	Play SIM Toolkit Tone	149
6.2.32 AT+SIMTONE	Generate Specifically Tone	150
6.2.33 AT+CCPD	Enable or Disable Alpha String	150
6.2.34 AT+CGID	Get SIM Card Group Identifier	151
6.2.35 AT+MORING	Show State of Mobile Originated Call	151
6.2.36 AT+CMGHEX	Enable or Disable Sending Non-ASCII Character SMS	152
6.2.37 AT+CCODE	Configure SMS Code Mode	153
6.2.38 AT+CIURC	Enable or Disable Initial URC Presentation	153
6.2.39 AT+CPSPWD	Change PS Super Password	154
6.2.40 AT+EXUNSOL	Enable or Disable Proprietary Unsolicited Indications	155
6.2.41 AT+CGMSCLASS	Change GPRS Multislot Class	156
6.2.42 AT+CDEVICE	View Current Flash Device Type	156
6.2.43 AT+CCALR	Call Ready Query	156
6.2.44 AT+GSV	Display Product Identification Information	157
6.2.45 AT+SGPIO	Control the GPIO	157
6.2.46 AT+SPWM	Generate the Pulse-Width-Modulation	158
6.2.47 AT+ECHO	Echo Cancellation Control	159
6.2.48 AT+CAAS	Control Auto Audio Switch	160
6.2.49 AT+SVR	Configure Voice Coding Type for Voice Calls	161
6.2.50 AT+GSMBUSY	Reject Incoming Call	162
6.2.51 AT+CEMNL	Set the List of Emergency Number	163

6.2.52 AT*CELLLOCK	Set the List of ARFCN Which Needs to Be Locked	163
6.2.53 AT+SLEDS	Set the Timer Period of Net Light	164
6.2.54 AT+CCHGMODE	Indicates If the Module Is Powered Off	165
6.2.55 AT+CBUZZERRING	Use the Buzzer Sound as the Incoming Call Ring	165
6.2.56 AT+CEXTERNTONE	Close or Open the Microphone	166
6.2.57 AT+CNETLIGHT	Close the Net Light or Open It to Shining	166
6.2.58 AT+CWHITELIST	Set the White List	167
6.2.59 AT+CUSACC	Accelerate Uart Response Speed	167
6.2.60 AT+CNETSCAN	Performing A Net Survey to Show All the Cells Information	168
6.2.61 AT+CSGS	Netlight Indication of GPRS Status	169
6.2.62 AT+SKPD	Enable Keypad Indication	169
6.2.63 AT+CUSD	Unstructured Supplementary Service Data	170
6.2.64 AT+NETLOCK	Close or Open the Function of Lock Network	171
6.2.65 AT+CLNWPLMN	Set MCC&MNC List for Lock Network	172
6.2.66 AT+SNLEVEL	Set the Sound Level of Special AT Command	172
7 AT Commands for GPRS Support		174
7.1 Overview of AT Commands for GPRS Support		174
7.2 Detailed Descriptions of AT Commands for GPRS Support		174
7.2.1 AT+CGATT	Attach or Detach from GPRS Service	174
7.2.2 AT+CGDCONT	Define PDP Context	175
7.2.3 AT+CGQMIN	Quality of Service Profile (Minimum Acceptable)	177
7.2.4 AT+CGQREQ	Quality of Service Profile (Requested)	178
7.2.5 AT+CGACT	PDP Context Activate or Deactivate	179
7.2.6 AT+CGDATA	Enter Data State	180
7.2.7 AT+CGADDR	Show PDP Address	181
7.2.8 AT+CGCLASS	GPRS Mobile Station Class	182
7.2.9 AT+CGEREP	Control Unsolicited GPRS Event Reporting	183
7.2.10 AT+CGREG	Network Registration Status	184
7.2.11 AT+CGSMS	Select Service for MO SMS Messages	185
8 AT Commands for TCP/IP Application Toolkit		187
8.1 Overview		187
8.2 Detailed Descriptions of Commands		188
8.2.1 AT+CIPMUX	Start Up Multi-IP Connection	188
8.2.2 AT+CIPSTART	Start Up TCP or UDP Connection	188
8.2.3 AT+CIPSEND	Send Data Through TCP or UDP Connection	191
8.2.4 AT+CIPQSEND	Select Data Transmitting Mode	192
8.2.5 AT+CIPACK	Query Previous Connection Data Transmitting State	193
8.2.6 AT+CIPCLOSE	Close TCP or UDP Connection	194
8.2.7 AT+CIPSHUT	Deactivate GPRS PDP Context	194
8.2.8 AT+CLPORT	Set Local Port	195
8.2.9 AT+CSTT	Start Task and Set APN, USER NAME, PASSWORD	196
8.2.10 AT+CIICR	Bring Up Wireless Connection with GPRS or CSD	197

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

APPROVED



CONNECT<text> TA switches to data mode. Note: <text> output only if ATX<value> parameter setting with the <value>>0 When TA returns to Command mode after call release OK Response in case of voice call, if successfully connected OK Response if no connection NO CARRIER	
Reference V.25ter	Note See also ATX

→ is mode on or text?

2.2.3 ATD Mobile Originated Call to Dial A Number

ATD Mobile Originated Call to Dial A Number

Execution	Response
Command	This Command can be used to set up outgoing <i>voice, data or fax calls</i> . It also serves to control <i>supplementary services</i> .
ATD<n>[<mgsml>][:]	Note: This Command may be aborted 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 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

Usables



	Parameter
<value>	0 Echo mode off 1 Echo mode on
Reference V.25ter	Note

2.2.8 ATH Disconnect Existing Connection

ATH Disconnect Existing Connection

Execution	Response
Command	Disconnect existing call by local TE from Command line and terminate call
ATH[n]	OK Note: OK is issued after circuit 109(DCD) is turned off, if it was previously on.
	Parameter
	<n>
	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, CSD calls, GPRS call will be disconnected. (clean 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)
Reference V.25ter	Note

→ 7 receive el receptor?

2.2.9 ATI Display Product Identification Information

ATI Display Product Identification Information

Execution	Response
-----------	----------



	<p>"PP" Service Provider Personalization Correspond to SPCK code</p> <p><mode> 0 unlock 1 lock 2 query status</p> <p><passwd> String type (Shall be the same as password specified for the facility from the ME user interface or with command Change Password +CPWD)</p> <p><class> 1 Voice (telephony) 2 Data refers to all bearer services; with <mode>=2 this may refer only to some bearer service if TA does not support values 16, 32, 64 and 128 4 Fax (facsimile services) 7 All classes</p> <p><status> 0 Not active 1 Active</p>
Reference	Note
GSM 07.07 [14]	CME errors if SIM not inserted or PIN is not entered.

3.2.18 AT+CLIP Calling Line Identification Presentation

AT+CLIP Calling Line Identification Presentation

Test Command	Response
AT+CLIP=?	+CLIP: (list of supported <n>s)
	OK
Parameter	See Write Command
Read Command	Response
AT+CLIP?	+CLIP: <n>, <m>
	OK
	If error is related to ME functionality: +CME ERROR: <err>
Parameters	See Write Command
Write Command	Response
AT+CLIP=<n>	TA enables or disables the presentation of the CLI at the TE. It has no effect on the execution of the supplementary service CLIP in the network.
	OK
	If error is related to ME functionality: +CME ERROR: <err>
Parameters	

→ da metadatos del que llame
tfn, tipo, addr...

↳ puede el llamante
ocultarlos dando
asi información

→ ESTE
DEBERIA
FUNCIONAR!

	<p><n> 0 Disable +CLIP notification. 1 Enable +CLIP notification.</p> <p><m> 0 CLIP not provisioned 1 CLIP provisioned 2 unknown (e.g. no network, etc.)</p>
	<p>Unsolicited Result Code</p> <p>When the presentation of the CLI at the TE is enabled (and calling subscriber allows), an unsolicited result code is returned after every RING (or +CRING: <type>) at a mobile terminating call.</p> <p>+CLIP: <number>, <type>, <subaddr>, <stype>, <alphaId>, <CLI validity></p>
	<p>Parameters</p> <p><number> String type (string should be included in quotation marks) phone number of calling address in format specified by <type>.</p> <p><type> Type of address octet in integer format: 129 Unknown type 161 National number type 145 International number type 177 Network specific number</p> <p><subaddr> String type (subaddress of format specified by <stype>)</p> <p><stype> Integer type (type of subaddress)</p> <p><alphaId> String type (string should be included in quotation marks) alphanumeric representation of <number> corresponding to the entry found in phone book.</p> <p><CLI validity></p> <p>0 CLI valid 1 CLI has been withheld by the originator. 2 CLI is not available due to interworking problems or limitations of originating network.</p>
Reference	Note

3.2.19 AT+CLIR Calling Line Identification Restriction

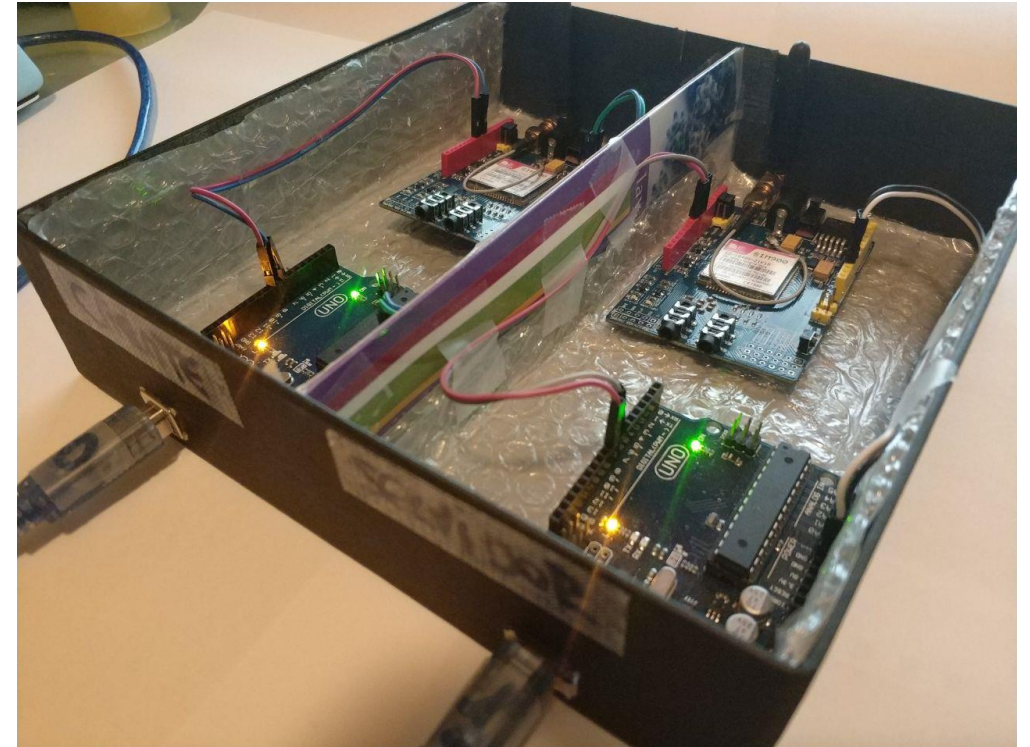
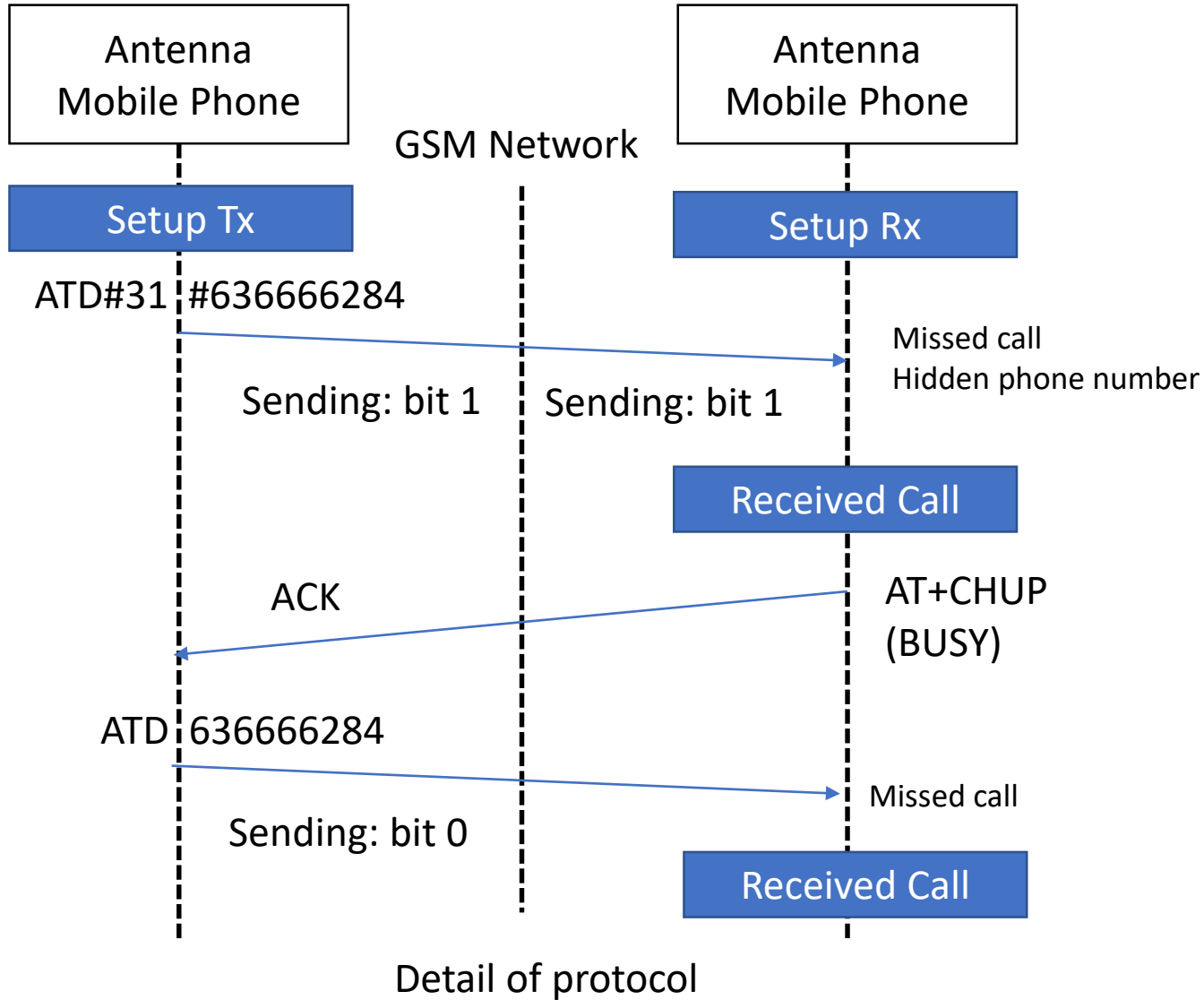
AT+CLIR Calling Line Identification Restriction

Test Command	Response
AT+CLIR=?	+CLIR: (list of supported <n>s)
	OK
Parameter	

→ ocultar metadatos al receptor



DEMO – Abusing GSM using covert channels with AT commands



Aihasd SIM900 GSM



Arduino

DEMO – Abusing GSM using covert channels with AT commands



COM4 (Arduino/Genuino Uno)

Enviar

COM3 (Arduino/Genuino Uno)

Enviar

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 = '63XXXX084'
```



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)

Services & Users

Buy Number
Add conference
Add voice app
Add user

My settings
Billing

▲ Phone numbers [Buy number](#) | [Help](#)

Number	Calls go to	
+34911 [redacted] 57 (Spain)	[redacted]	Change
+349119 [redacted] 8 (Spain)	[redacted]	Change

▲ Conference rooms [Add conference](#) | [Help](#)

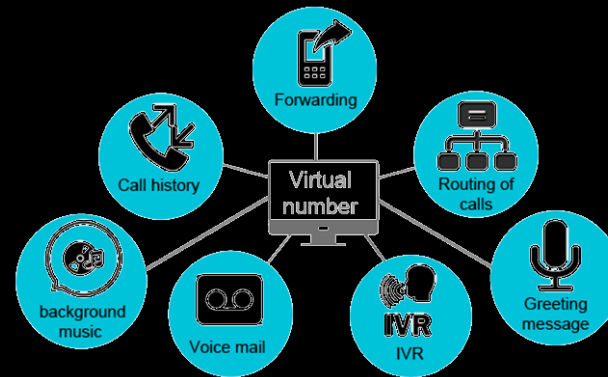
Conference rooms
No conference rooms [Add a conference](#)

▲ Call recordings [Configure](#) | [Help](#)

Call recording disabled [Configure](#)

▼ Voice apps [Add app](#) | [Help](#)

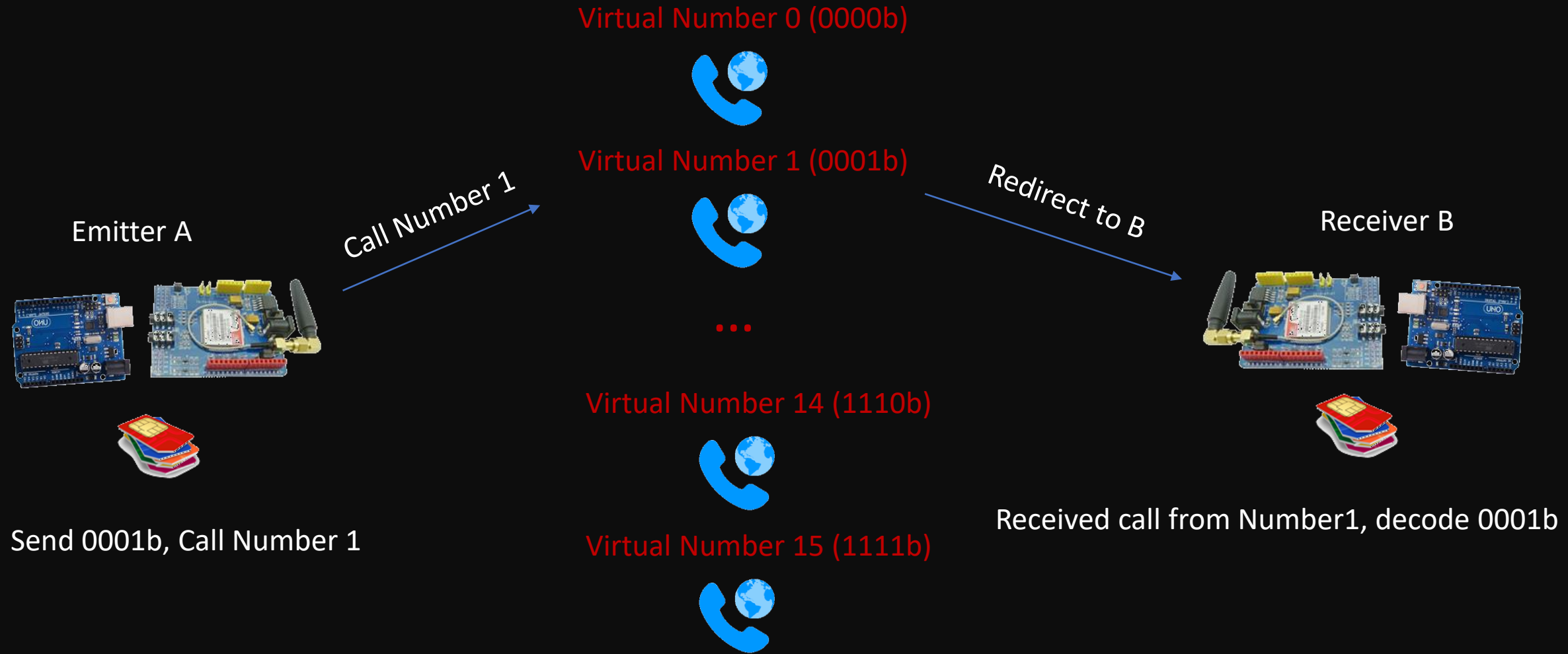
▼ Users [Add user](#) | [Help](#)



GSM/GPRS Modem Pool



Ejemplo – Abusing GSM using covert channels with AT commands + Virtual Numbers



$E_j / 7 * \log_2(\text{Virtual Numbers}) \text{ bits/min} \rightarrow E_j / 28 \text{ bits/min}, 7 \text{ calls/min}$



DEMO – Abusing GSM using covert channels with AT commands + Virtual Numbers

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: LISTEN

DEMO – Abusing GSM using covert channels with AT commands + Virtual Numbers

```
COM4 (Arduino/Genuino Uno)
Enviar

Demo HackInTheBox 2018, April 13, Amsterdam.
By Alfonso Muñoz (@mindcrypt) and Jorge Cuadrado (@coke727)

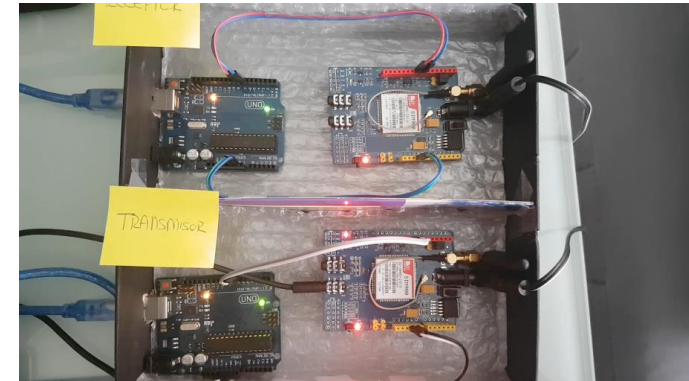
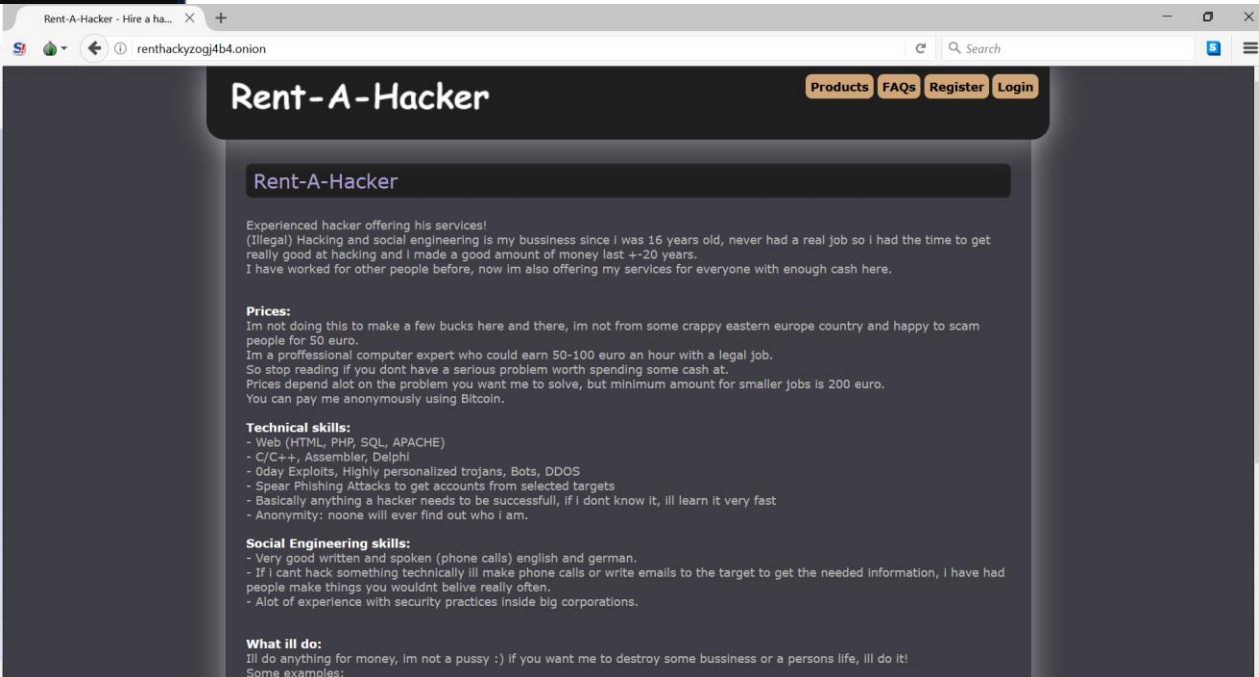
$device = 'EMITTER'
$ hiding_method = 'Virtual Number Amplification & missed call & hidden number'
$mobile_number = '63XXXX392'
$binary_msg = '0110100001110100011000100011000100111000'

Setup configuration for sending info...
[0] Sending: 0110
```

```
COM3 (Arduino/Genuino Uno)
Enviar

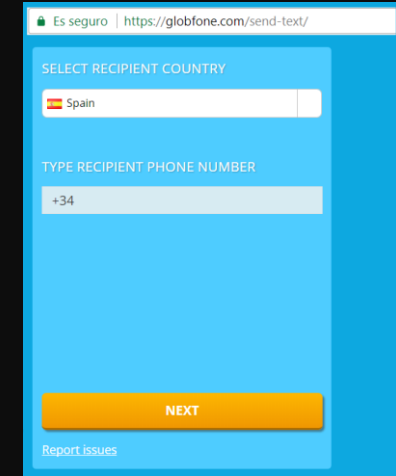
Demo HackInThebox 2018, April 13, Amsterdam.
By Alfonso Muñoz (@mindcrypt) and Jorge Cuadrado (@coke727)

[RECEIVER] Waiting info...
```



“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**



Ej, Phone number: 123456789
→ bits (000000...0000001)
Phone number: 123456790
→ bits (000000...0000010)

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

Hiding capacity:

$$VR_{10,13} = 10^{13} \rightarrow 13 / \log_2 = 43 \text{ bits}$$

$$VR_{10,9} = 10^9 \rightarrow 9 / \log_2 = 29 \text{ bits}$$

Demo: Covert channel – Caller ID Spoofing

www.llamadasperdidas.com



wrong code
zanox-affiliate

Número de origen desde donde llamar: [?]

Número de destino al que quieres llamar: [?]

Código captcha: [?]

7mji749j

Hacer llamada perdida



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)

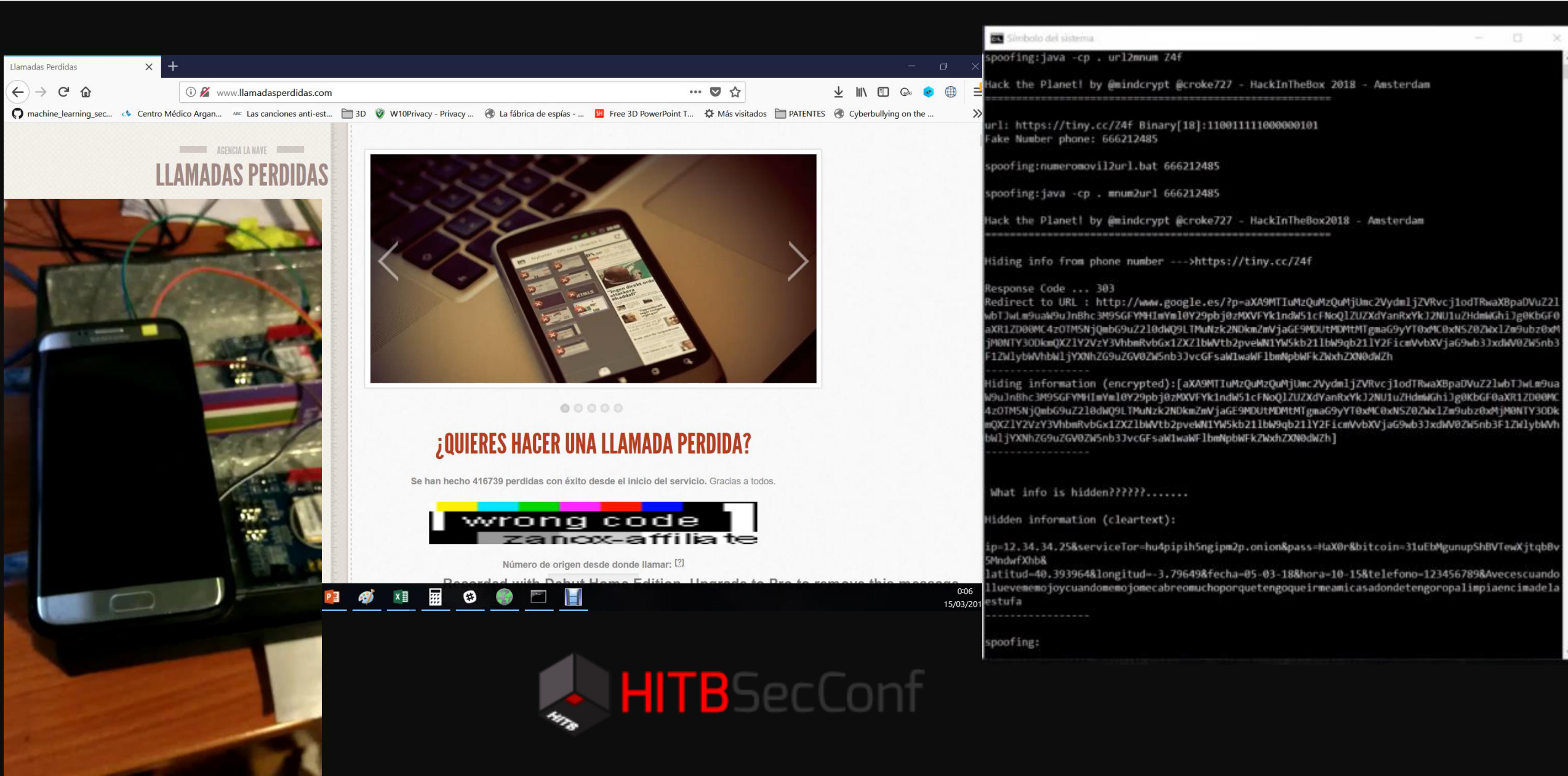
Ej/ tiny.cc/A2bE $\rightarrow 24$ bits

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

The screenshot shows the Tiny URL website interface. At the top, there are navigation tabs: Home, Example, Branded, and Help. A user is logged in as 'Guest!' with 'Login' and 'Register' buttons. Below the navigation is a banner for 'TINY shorter URLs + QR codes' with a magnifying glass icon over the word 'URL'. An advertisement for 'compramostucoche.es' is displayed, featuring two red cars and the text '¿Cuánto vale mi coche? Descúbrelo ahora [Evaluación gratuita y sin compromiso]'. Below the ad is a form to create a new URL, with a 'TINY!' button. The 'Recent URLs' section shows a list of URLs, including 'http://fakeweb.com' and 'http://tiny.cc/plctry'. A 'START NOW' button is visible at the bottom. The browser's address bar shows 'https://tiny.cc' and the taskbar at the bottom includes various application icons.

Demo: Covert channel – Caller ID Spoofing



The image shows a demonstration of a covert channel using caller ID spoofing. On the left, a smartphone is connected to a computer via a USB cable. The browser window displays the website 'Llamadas Perdidas' (Lost Calls), which features a navigation menu with 'AGENCIA LA NAVE' and 'LLAMADAS PERDIDAS'. The main content area includes a smartphone image showing a list of lost calls, a heading '¿QUIERES HACER UNA LLAMADA PERDIDA?' (Do you want to make a lost call?), and a sub-heading 'Se han hecho 416739 perdidas con éxito desde el inicio del servicio. Gracias a todos.' (416,739 calls have been successfully made since the start of the service. Thanks to everyone.). Below this is a 'wrong code' error message and a 'Número de origen desde donde llamar: []' (Origin number from where to call: []).

On the right, a terminal window shows the execution of a Java-based spoofing tool. The terminal output includes the following commands and results:

```
spoofing:java -cp . url2num 24f
Hack the Planet! by @mindcrypt @croke727 - HackInTheBox 2018 - Amsterdam
url: https://tiny.cc/24f Binary[18]:110011111000000101
Fake Number phone: 666212485
spoofing:numeroovil2url.bat 666212485
spoofing:java -cp . mnum2url 666212485
Hack the Planet! by @mindcrypt @croke727 - HackInTheBox2018 - Amsterdam
Hiding info from phone number --->https://tiny.cc/24f
Response Code ... 303
Redirect to URL : http://www.google.es/?p=aXA9MTIuMzQuMzQuMjUmc2VydmljZVRvcj1odTRwaXBpaDVuZ21wbTJwLm9uaW9uJnBhc3M9SGFYMH1mYm10Y29pbj0zM0VYFk1ndw51cFN0Q1ZUZXdVanRyYk12NU1uZhdmGh1jg0KbGF0aXR1ZD00MC4zOTMSNjQmbG9uZ210dWQ9LTMuNzk2NDkmZmVjaGE9M0UtMDMtMTgmaG9yYT0xMC0xNSZ0ZmxiZm9ubz0xMjM0NTY3ODkqXzI1Y2VzY3VhbmRvbGx1ZXZ1bWVtb2pveW5kb211bW9qb211Y2F1cmVvbXVjaG9wb3JxdWV0ZW5nb3F1ZWIyYbWVhbn1jYXNhZG9uZGV0ZW5nb3JvcGFsaWwWF1bmNpbWFKZm90dWZh]
Hiding information (encrypted):[aXA9MTIuMzQuMzQuMjUmc2VydmljZVRvcj1odTRwaXBpaDVuZ21wbTJwLm9uaW9uJnBhc3M9SGFYMH1mYm10Y29pbj0zM0VYFk1ndw51cFN0Q1ZUZXdVanRyYk12NU1uZhdmGh1jg0KbGF0aXR1ZD00MC4zOTMSNjQmbG9uZ210dWQ9LTMuNzk2NDkmZmVjaGE9M0UtMDMtMTgmaG9yYT0xMC0xNSZ0ZmxiZm9ubz0xMjM0NTY3ODkqXzI1Y2VzY3VhbmRvbGx1ZXZ1bWVtb2pveW5kb211bW9qb211Y2F1cmVvbXVjaG9wb3JxdWV0ZW5nb3F1ZWIyYbWVhbn1jYXNhZG9uZGV0ZW5nb3JvcGFsaWwWF1bmNpbWFKZm90dWZh]
What info is hidden?????.....
Hidden information (cleartext):
ip=12.34.34.25&serviceTor=hu4piph5ngipm2p.onion&pass=HaX0r&bitcoin=31uEbMgunupShBVTewXjtqbV5Mndwfxhb&
latitud=40.393964&longitud=-3.796498&fecha=05-03-18&hora=10-15&telefono=123456789&Avecscuando
llueveemojocucandomemojomecabreomuchoporquetengoqueirmeamicasadondetengoropaliempiaenciadela
estufa
spoofing:
```

At the bottom of the image, there is a logo for 'HITB SecConf'.

AT + CONCLUSION CR LF ["APLAUSOS"]

HackintheBox's Blue Box System V1.0

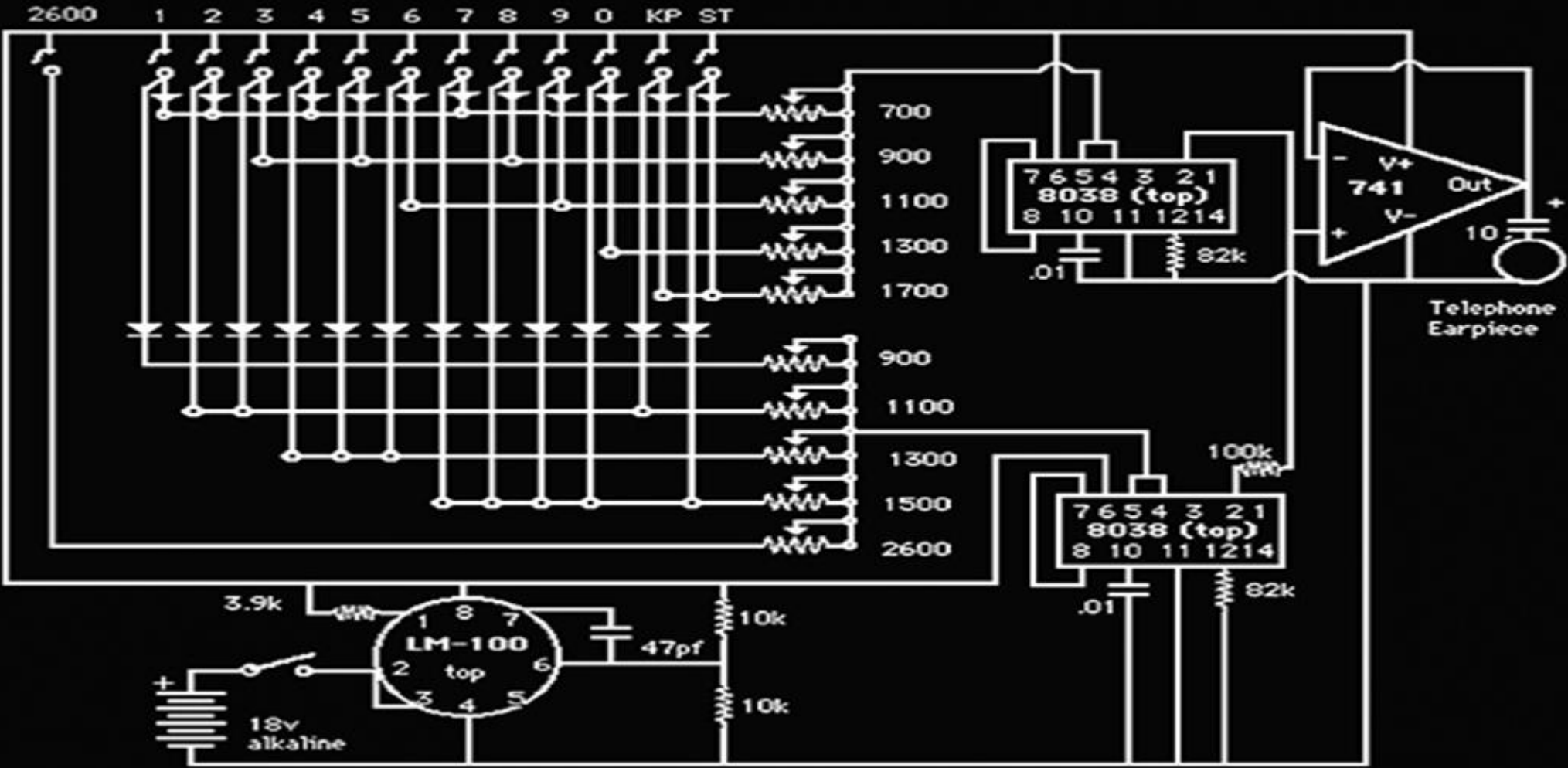
```
[1] [2] [3]
[4] [5] [6]
[7] [8] [9]
[*] [0] [#]
```

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)