



The Hacker's Corner: Phone Call Risks and Phone call protection systems



HackersCorner – International Journalism Festival

15 Apr 2011

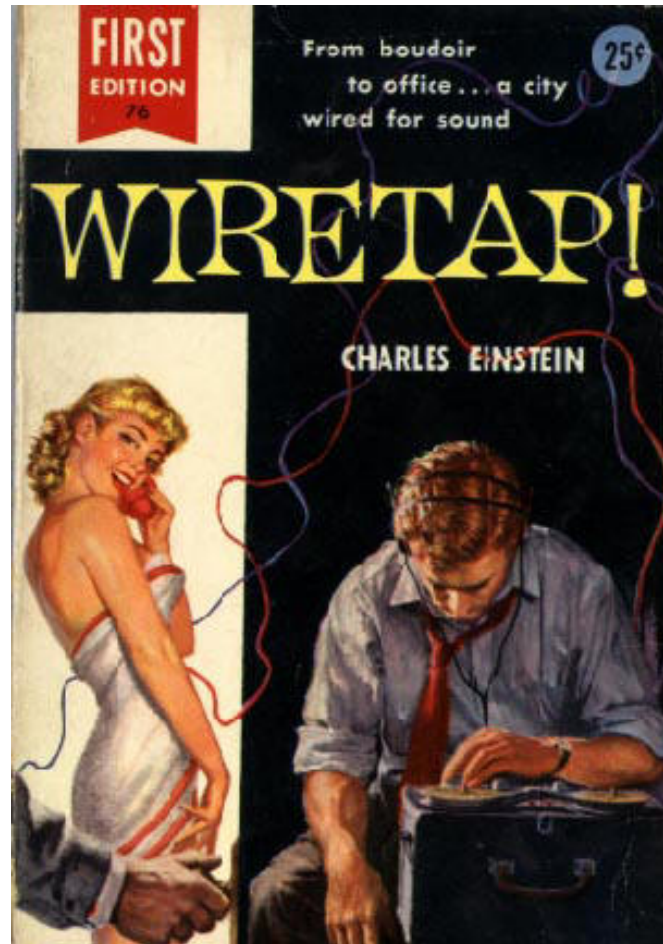
Fabio Pietrosanti (naif) – <http://www.hackerscorner.org>

My mail: fabio@pietrosanti.it - My blog: <http://infosecurity.ch>



I

The need to intercept phone calls





The need to intercept phone calls

Once upon a time...



- Communication interception was limited to fixed phone lines
- Few companies, Telco monopoly, was involved
- The interception was limited in providing useful information for investigation and intelligence needs





The need to intercept phone calls But now...



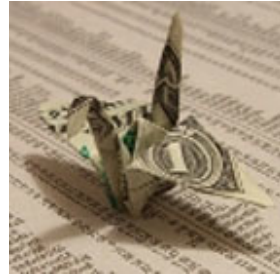
- Ubiquitous computing is a reality and mobility is everywhere
- Plenty of different operators
- Plenty of different technologies (voip, virtual operators, etc)
- Cross-border communication services complexity
- More data can be retrieved (ex: Location data, phone call logs, sms messages, etc,)





The need to intercept phone calls

An appealing business today



- Acquiring access to communications today means acquiring ***full*** access to a person life
- But who has such need?



The need to intercept phone calls



Subjects interested in other parties communications

- Law Enforcement Agencies
- National Secret Services
- Foreign Secret services
- Almost all large corporation in international context
- Outsourced intelligence service providers
- Organized crime
- Military organization in battlefield

(those information may require dedicated slides for each subject)



The need to intercept phone calls

Lawful interception

- Lawful interception
- Action (based on the law) *performed* by a network operator / access provider / service provider (NWO/AP/SvP), of making available certain information and providing that information to a law enforcement monitoring facility for investigation purposes





The need to intercept phone calls

Unlawful interception

- **Unlawful interception**
- Action (against the law) *performed* by a government agency / network operator / access provider / service provider (NWO/AP/SvP) / Large enterprise / Intelligence Agency / Intelligence professional / disgruntled employee, of making available certain information and providing that information to an interested third party that provided enough budget to proceed to that information collection





**Methods to intercept phone calls
(do it by yourself)**



2 - Methods to intercept phone calls

Tactical Vs. Non-Tactical Interception



- Tactical interception
 - It directly apply to communication lines
 - Does not involve the telecommunication operator knowledge
 - It can be lawful or unlawful
 - Almost most unlawful interception use Tactical methods





2 - Methods to intercept phone calls



Interception targets and approach

- Target Identity
- Target Devices
- Target Communication lines
- Parametric Interception
 - Target a perimeter
 - Target specific content (keyword, language, stress, mix of all of them)





2 - Methods to intercept phone calls

Practical Approach: Once upon a time...



- Manual switching cable on Telco offices was an easy to do task.



2 - Methods to intercept phone calls

Practical Approach: Mobile interception (1)



- Mobile phones can be intercepted with appropriate equipment (GSM, UMTS)
- Active Method (Risk of detection)
- Passive Method (A5 Cracking)
- Mobile spyware intelligence
- UMTS

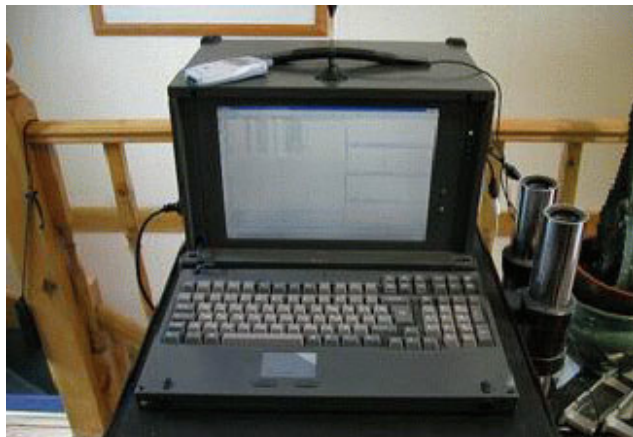




2 - Methods to intercept phone calls



Practical Approach: Mobile interception (2)



- Many approach to crack different GSM crypto algorithms:
 - A5/0
 - A5/1
 - A5/2
 - A5/3

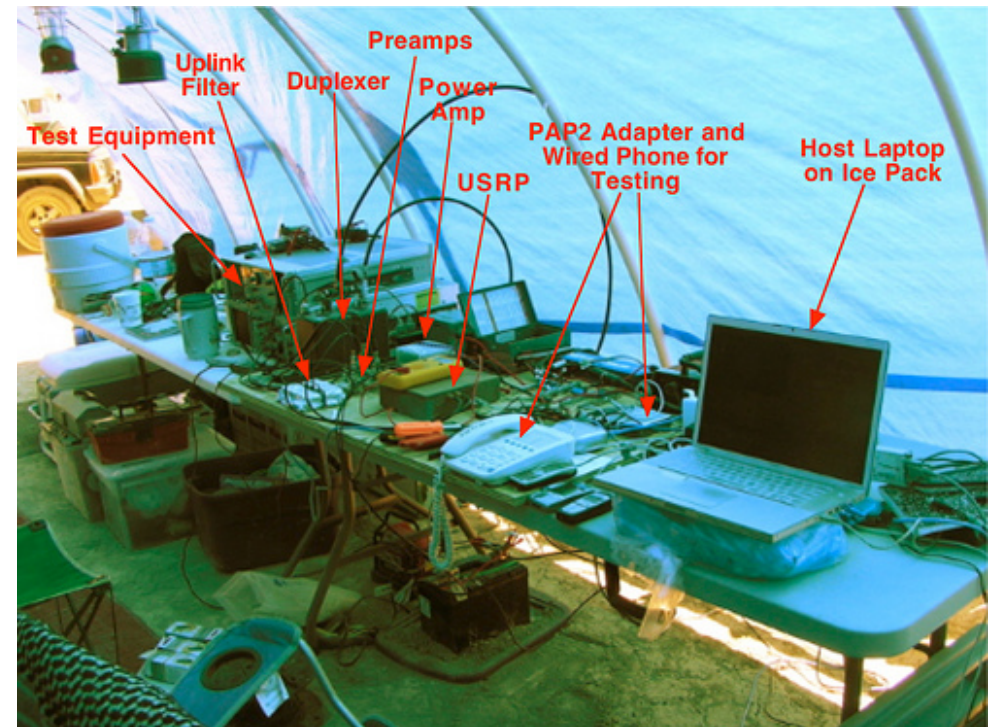


2 - Methods to intercept phone calls



Practical Approach: GSM Active IMSI-catcher

- Create a fake GSM network with powerful antenna and RX/TX power
- Mobile phones goes to powerful BTS
- Wiretapping trough man in the middle
- Patented by Rohde & Schwarz “Virtual base station”
- Can be easily done with OpenBTS + USRP device
- Dozen of commercial products for intelligence purpose





2 - Methods to intercept phone calls

Practical Approach: GSM A5/I passive



- Using rainbowtables to cracking A5/I encryption
- Fully passive encryption cracking
- Based on known plain text of certain GSM messages (SI5, SI6, SI6bis)
- In theory fixed... but upcoming public attack via SMS!
- Available via cheap USRP1 + airprobe + kraken or trough professional products

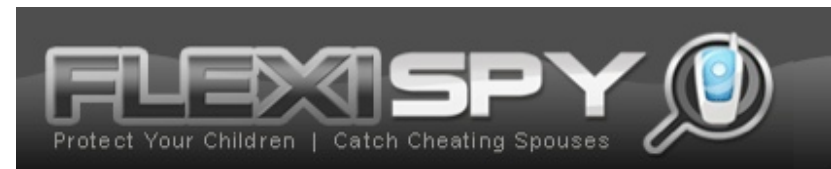


- <http://srlabs.de> - <http://reflexor.com/a51>



2 - Methods to intercept phone calls

Practical Approach: Mobile spyware



- On device spyware
- Many commercial trojan for Symbian, Blackberry, iPhone, Android
- Tap phone calls by conference calling
- Someone is able to tap silently and send via GPRS





2 - Methods to intercept phone calls

Practical Approach: UMTS?



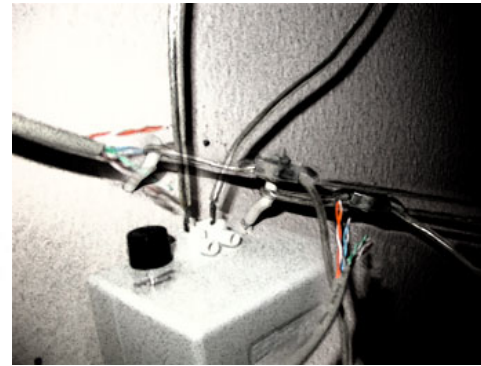
- Theoretically broken
- No practical implementation around
- All phones are Dual-Mode
- If you can't crack it, just block it with a Jammer
- Automatic UMTS -> GSM roaming





2 - Methods to intercept phone calls

Practical Approach: ISDN/PSTN Interception



- Simple cable cut give impressive results!
- Budget? Less than 250 USD for a professional equipment transmitting in VHF

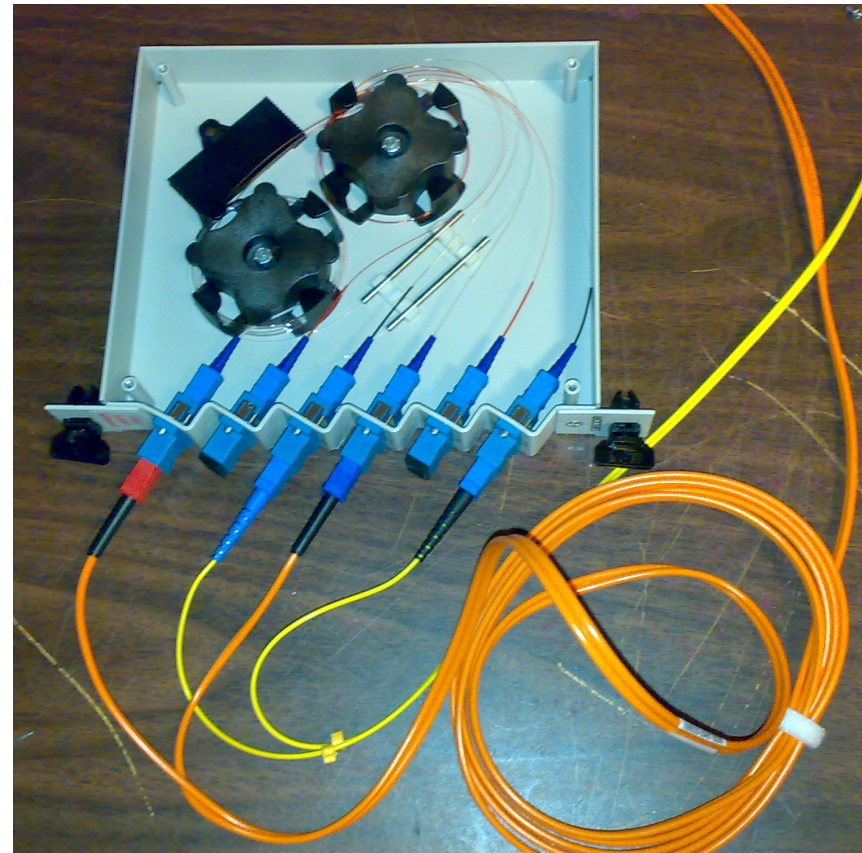


2 - Methods to intercept phone calls



Practical approach: Fiber Tapping (voip)

- Less than 300 USD equipment
- Open the bottle, bypass the fiber, get the whole traffic of area

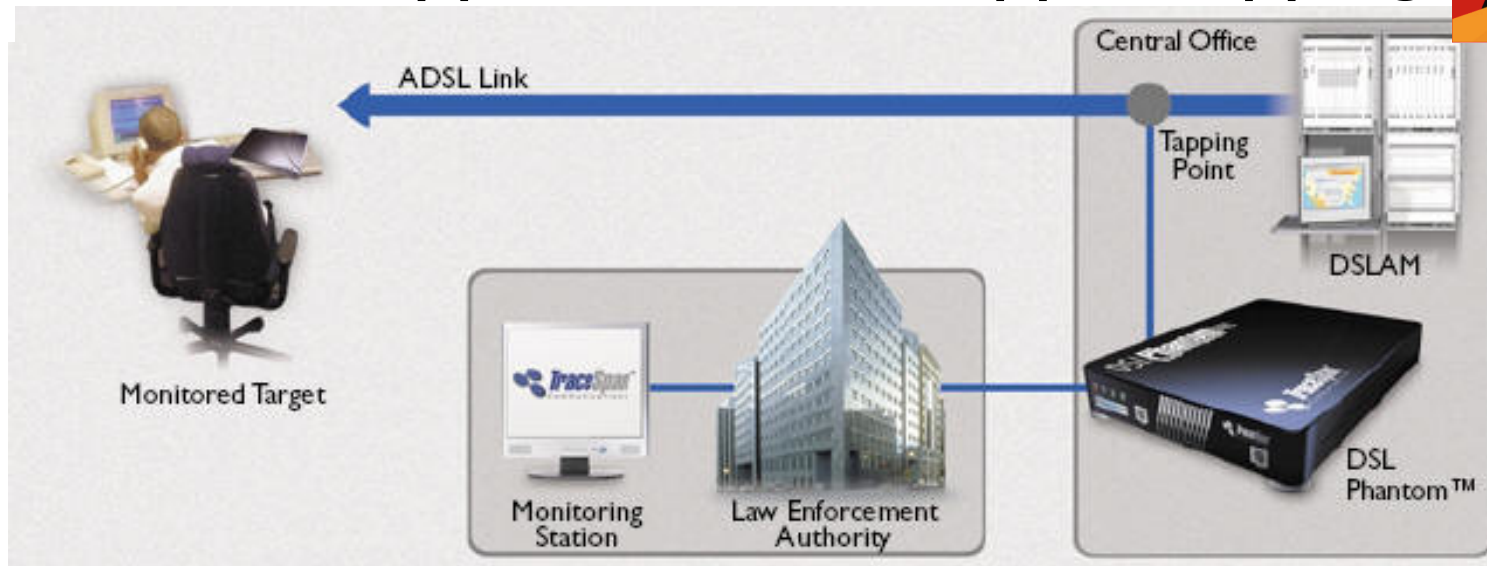




2 - Methods to intercept phone calls



Practical approach: DSL copper tapping



- Tap directly on ADSL copper with Tactical ADSL probe (Trace Span)
- System integrated one with 3500 EUR

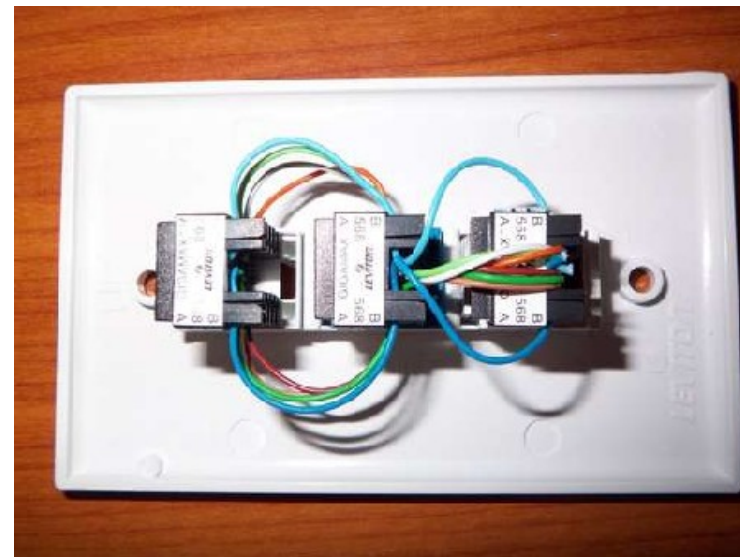
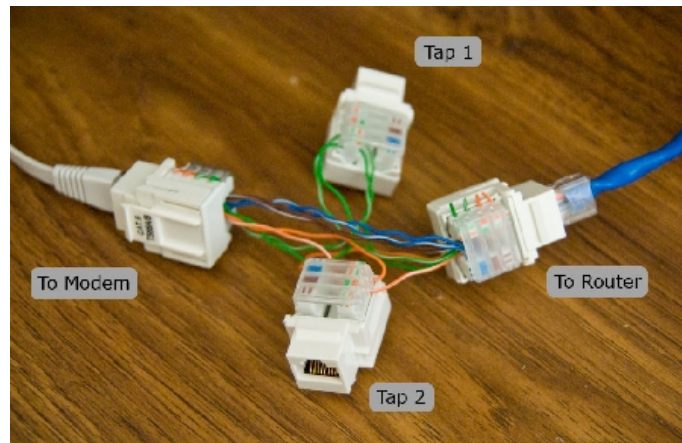


2 - Methods to intercept phone calls

Practical Approach: Easy ethernet tapping (voip)



- From 20 to 150 USD budget





2 - Methods to intercept phone calls



Practical Approach: What about CDR?

- Call data records give full mapping of a person social network
- Identify relations strength
- Analysis of CDR always done before wiretapping
- Commercial available software such as verint.com X-Tract
- NSA call database count 1.9 trillion CDRs

X-TRACT CDR Analysis

Analysis of call data records (CDRs) for law enforcement and other agencies

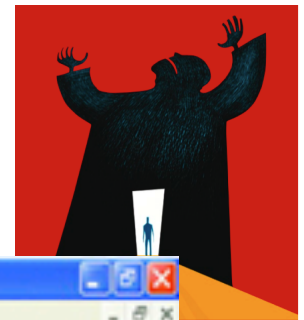
At A Glance

- Collects, integrates, and analyzes large volumes of call data records from disparate sources
- Dynamically displays data and analyses, with drill-down capabilities
- Automatically triggers alerts based on customizable rules
- Features integrated analytics, including text mining, visual link analysis, and statistical reports, for more comprehensive, accurate intelligence
- Aggregates all case-related data and analyses using case management tools
- Designed to reduce investigation time, save manpower, and surface intelligence that might not otherwise be found



2 - Methods to intercept phone calls

Phone call logs intelligence



17 Analyst's Notebook 6 - [Chart1 (Modified)]

Microsoft Excel - test.xls

A1	A	B	C	D	E	F
1		Score	Type	Label	Date of Birth	From Data
2		10	Person	David Locke	1953-9-24 12:00 AM	
3		10	Subscriber	David Locke	1953-12-24 12:00 AM	
4		9	Person	Dave Locke	1955-3-30 12:00 AM	
5		6	Person	D Locke	1955-07-08 12:00 AM	
6		6	Nominal	D LOCKE	1955-07-08 12:00 AM	
7		6	Person	D Locke	1955-07-08 12:00 AM	
8		3	Person	DAVID		
9		3	Person	DAVID		
10		3	Person	David BLOOM		
11		3	Person	David YC		
12		3	Person	David YC		
13		3	Person	David GRIFFITHS		
14		3	Person	David Young		
15		3	Person	Judith Locke		
16		3	Person	David Green	1956-1-12 12:00 AM	
17		3	Person	DAVID FRANCIS		
18		3	Person	D.L. Locke		
19		3	Person	DAVID HOWARD		

Common

- Male
- Female
- Anonymous
- Subscriber
- Telephone
- Mobile Phone
- Account
- Credit Card
- Cash
- Document

Middle East

Afro-Caribbean

Asian

European

British

Dutch

Finch

French

German

Irish

Italian

Standard

Date of Birth

01/01/2005 00:00:00

Add Attribute

Enter some text to search for

Show Results



OK

Practically what do we need to protect ourself?

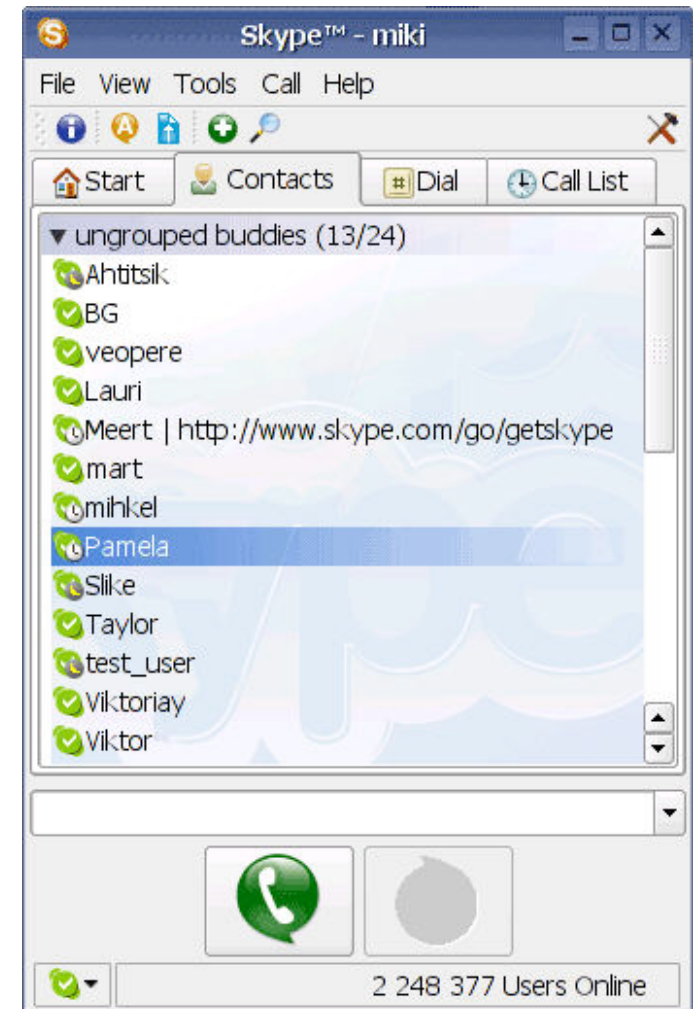


2 - Methods to intercept phone calls

Skype: What's about security?



- Voice calls are enciphered (skype could have it but it's not available to most governments)
- Messages are available for Skype
- Skype IN/OUT are wiretappable
- Skype can be blocked in certain countries (es: UAE)





Zfone Free ZRTP encryption (only voice)



Gizmo Project

Gizmo Account Contacts View Help

On the phone... [rec] [hold] [mute]

Current Call

No Subject
Duration: 00:02:29

Map It Hangup

[Click here for Blasts!](#)

Recent Calls with

- 29 Mär 10:05
- 29 Mär 10:03 Call Subject
- 29 Mär 09:47
- 29 Mär 09:44 Call Subject
- 29 Mär 09:43
- 29 Mär 09:42
- 29 Mär 09:37
- 29 Mär 09:35

ZFONE

Zfone Edit

Compare with partner:
music
millionaire

Verified

SECURE
AES-256

Secure since:
2007/03/29 19:58

Secure Clear

Zfone

Jon Callas on his laptop

Compare with partner:
clockwork
Pegasus

Verified

SECURE
AES-128

Secure since:
2007/02/26 14:56

Secure Clear



SIP Communicator – With ZRTP



SIP Communicator
1.0-alpha3-nightly.build.2488

Open Source VoIP & Instant Messaging
(c)2003-2009 Copyright sip-communicator.org. All rights reserved. Visit <http://sip-communicator.org>.

The SIP Communicator is distributed under the terms of the LGPL (<http://www.gnu.org>).

OK

SIP Communicator

Yana Stamcheva
Online

Enter name or number 2

- Carlos B. Fontiveros
- Damian Minkov
- Dragomira Belcheva
- Emil Ivov**
- Enrico Marocco
- Hristo Ganev
- Krasi Petrova
- Svetlin Tsvetanov
- Yan Langlois
- Yann Klis
- Students** 1/6
- Mathieu
- GSoC** 2/10
- aimar.mel@gmail.com
SC strikes back...
- greenjava@gmail.com
- General** 20/114



Mobile Encrypted products Only the ethical ones PrivateGSM & Cryptophone



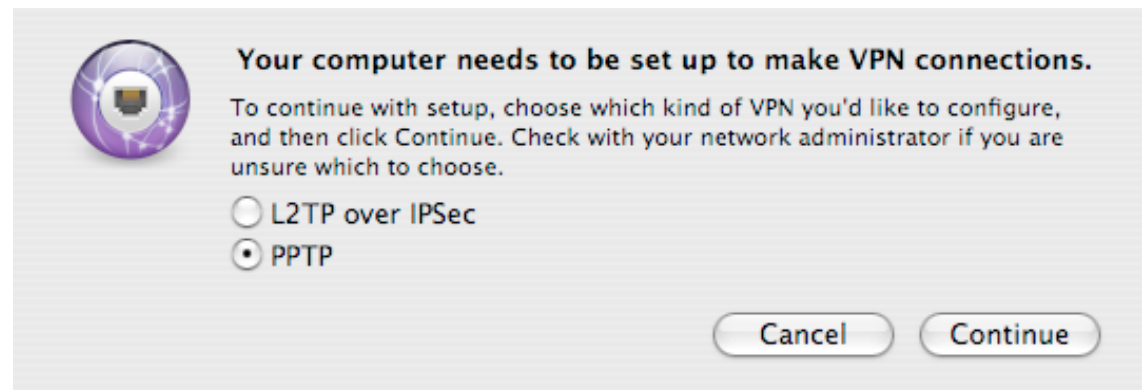


Mobile Encrypted products



Home Made: Standard VoIP + VPN

- You can always use (from your PC) a standard VoIP clients with any free providers (such as messagenet.it) and make it working over a VPN





The Hacker's Corner: Phone Call Risks and Phone call protection systems



HackersCorner – International Journalism Festival

15 Apr 2011

Fabio Pietrosanti (naif) – <http://www.hackerscorner.org>

My mail: fabio@pietrosanti.it - My blog: <http://infosecurity.ch>