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

HackersCorner – International Journalism Festival

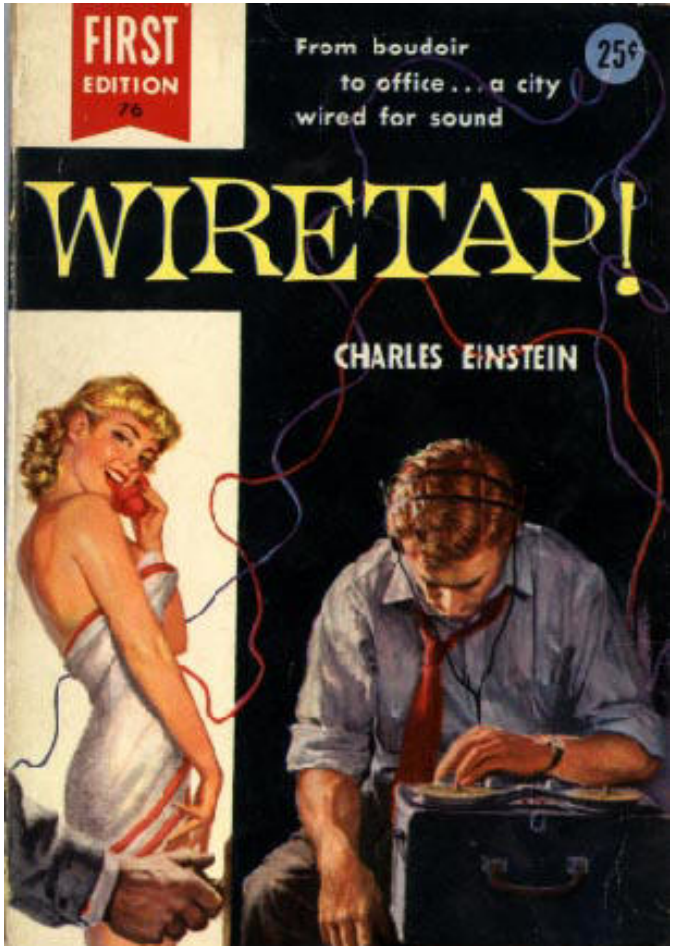
15 Apr 2011

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

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

I

The need to intercept phone calls



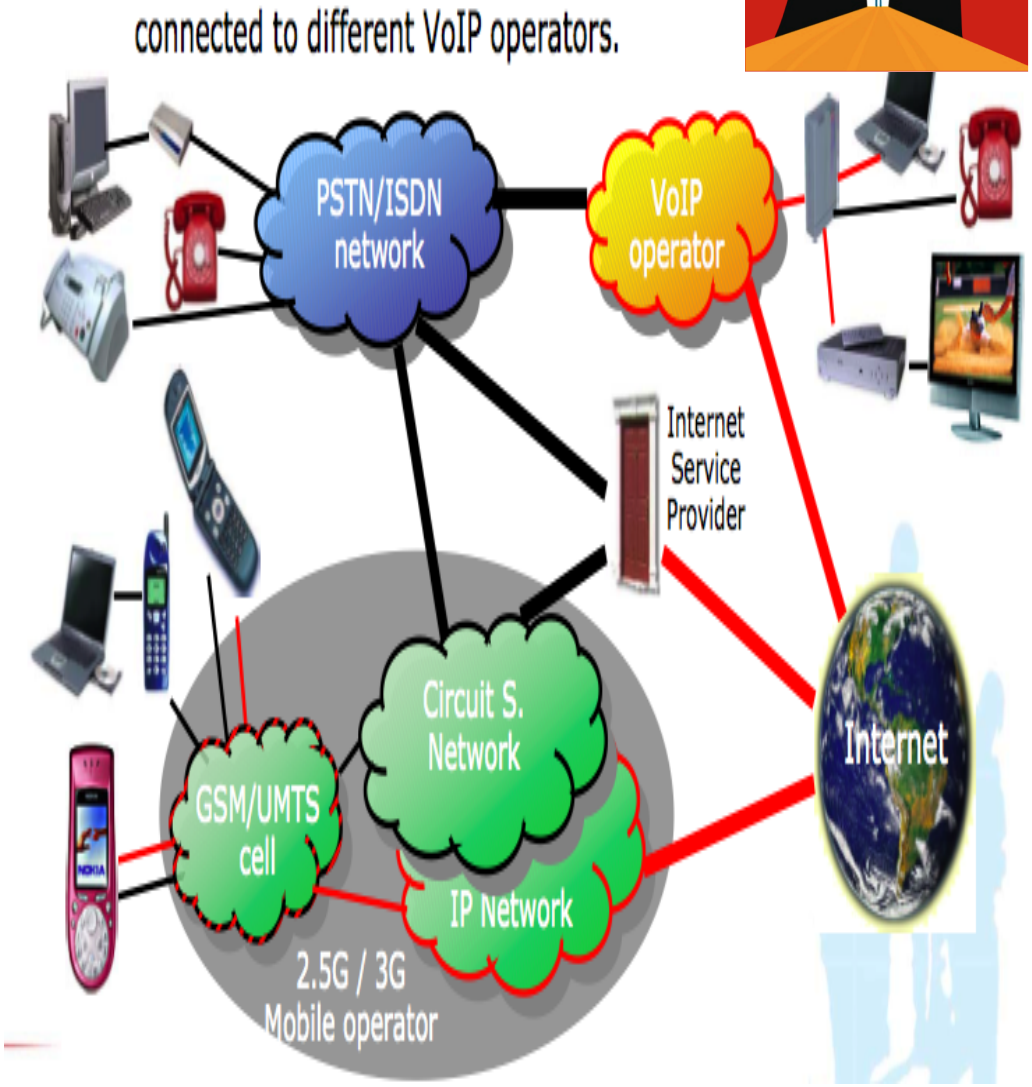
The need to intercept phone calls

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,)



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)

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

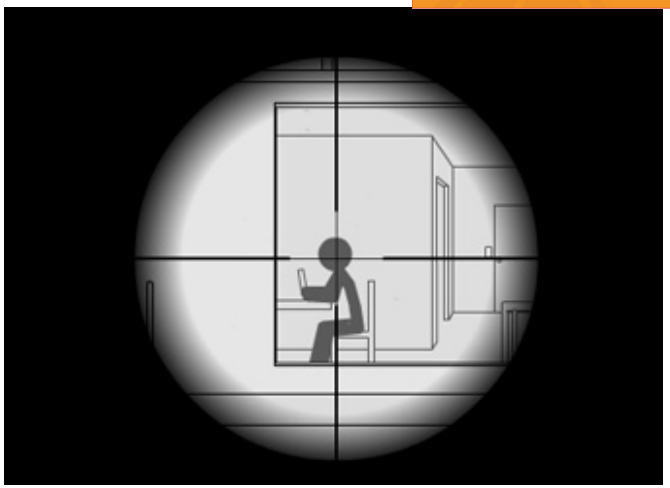
Unlawful interception

- 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)

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

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)

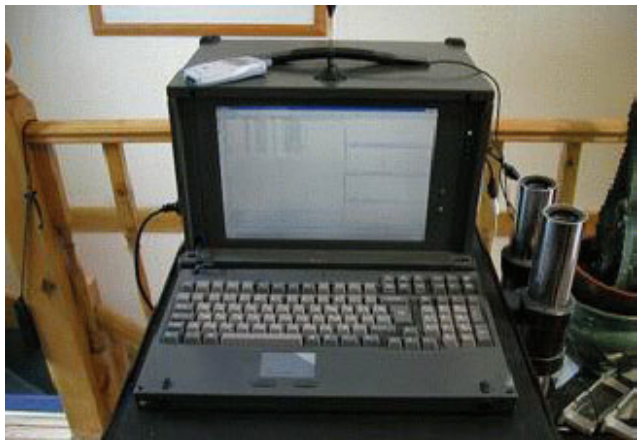
Practical Approach: Once upon a time...

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

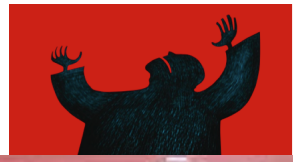
Practical Approach: Mobile interception (I)

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

Practical Approach: Mobile interception (2)



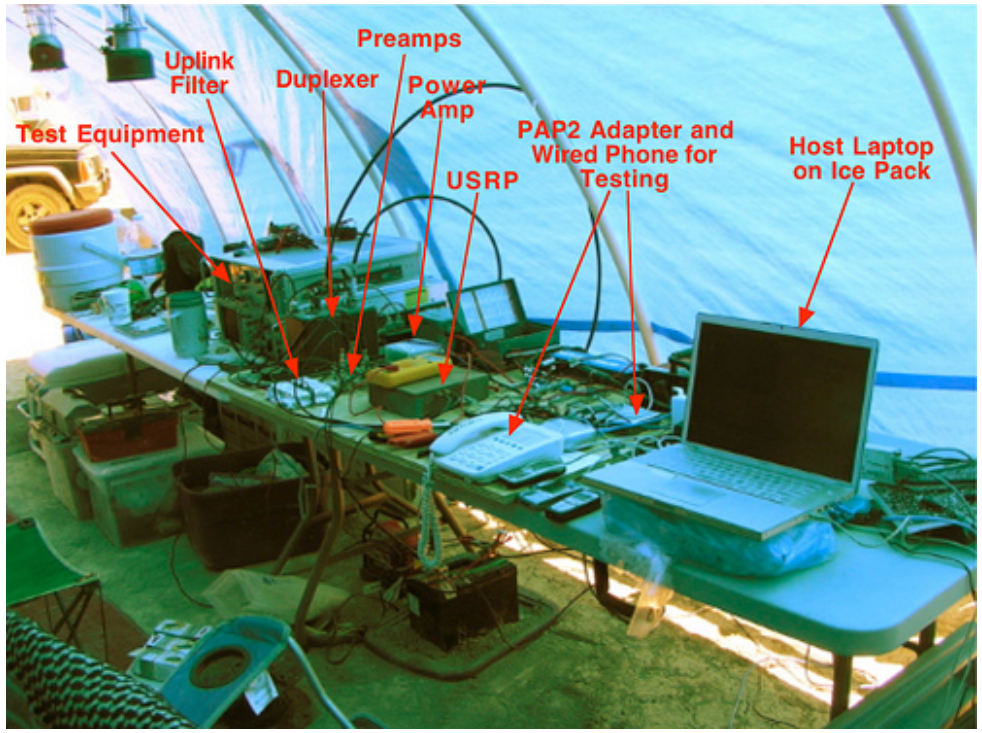
- Many approach to crack different GSM crypto algorithms:
  - A5/0
  - A5/1
  - A5/2
  - A5/3



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



Practical Approach: GSM A5/1 passive

- Using rainbowtables to cracking A5/1 encryption
- Fully passive encryption cracking
- Based on known plan text of certain GSM messages (SI5, SI6, SI6bis)
- In theory fixed… but upcoming public attack via SMS!

SECURITY RESEARCH LABS

- Available via cheap USRP1 + airprobe + kraken or trough professional products

- http://srlabs.de - http://reflextor.com/a51

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

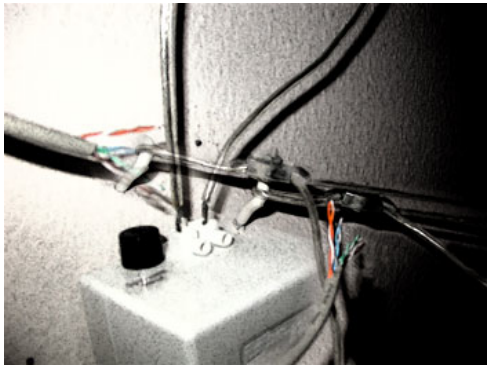
2 - Methods to intercept phone calls

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

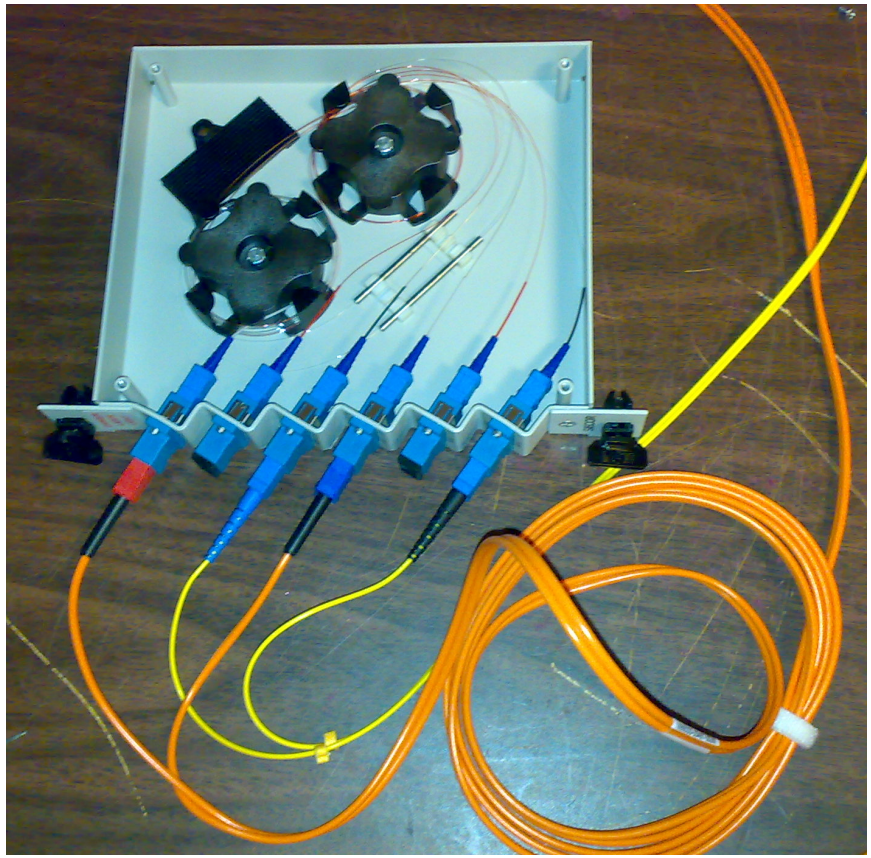
Practical Approach: ISDN/PSTN Interception



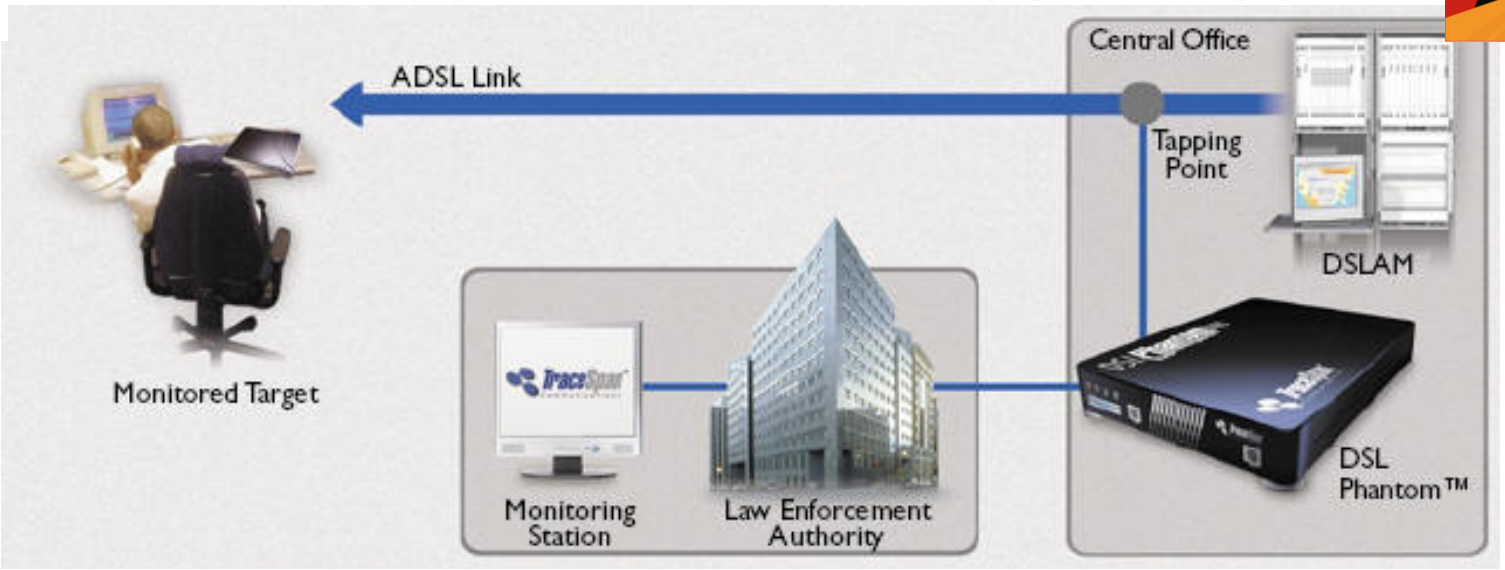
- Simple cable cut give impressive results!
- Budget? Less than 250 USD for a professional equipment transmitting in VHF

Practical approach: Fiber Tapping (voip)

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



Practical approach: DSL copper tapping

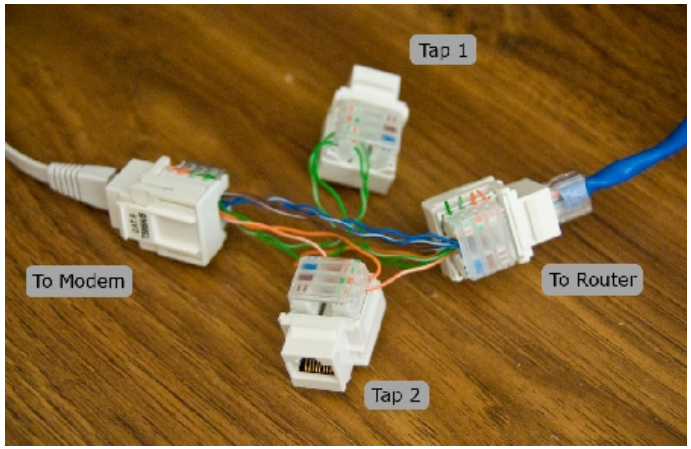


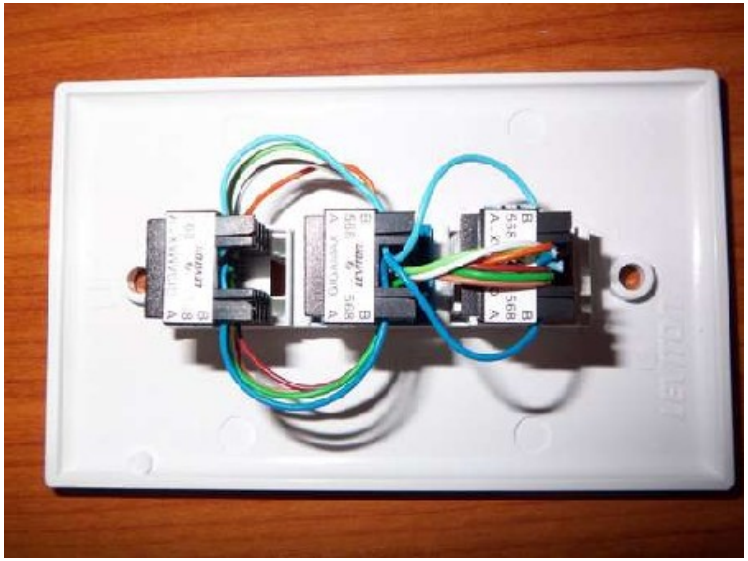
- Tap directly on ADSL copper with Tactical ADSL probe (Trace Span)
- System integrated one with 3500 EUR

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

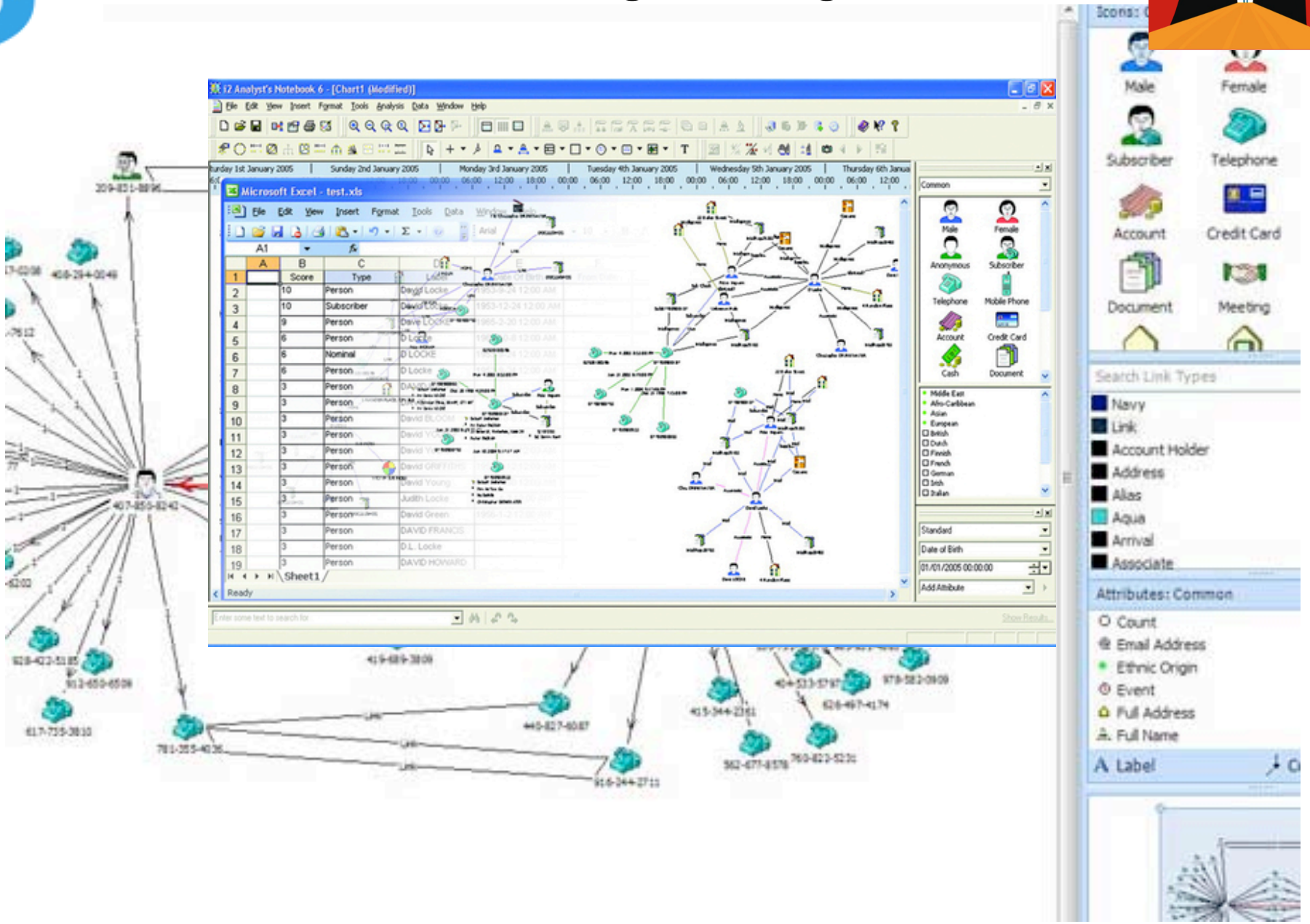
Analysis of call data records (CDRs) for law enforcement and other agencies

At A Glance

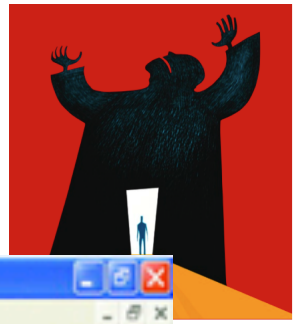
- Collects, integrates, and analyzes large volumes of call data records from disparate sources
- Dynamically displays data and analyses, with drill-down capabilities
- Automatically triggers alerts based on customizable rules
- Features integrated analytics, including text mining, visual link analysis, 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

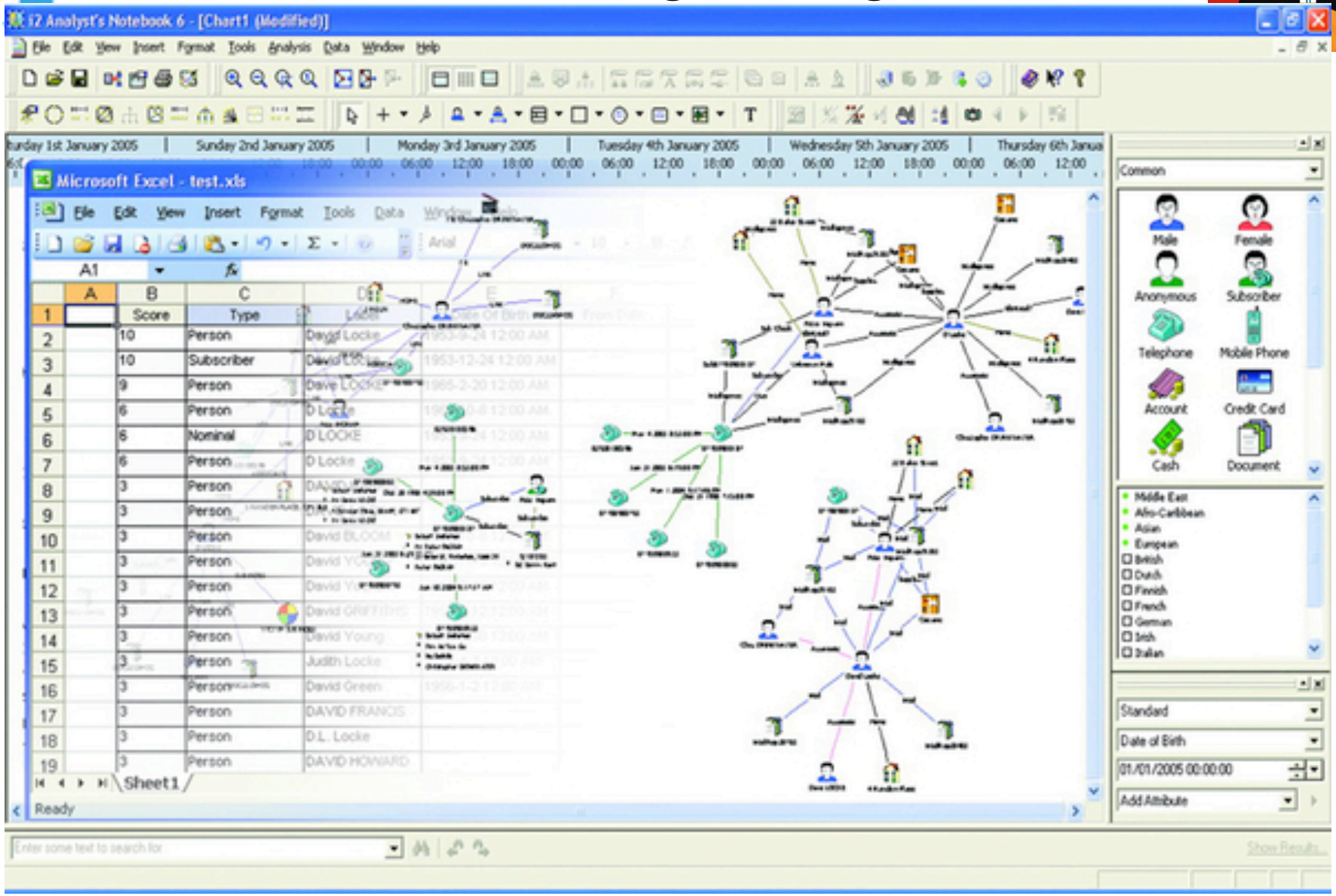
2 - Methods to intercept phone calls

Phone call logs intelligence



Phone call logs intelligence



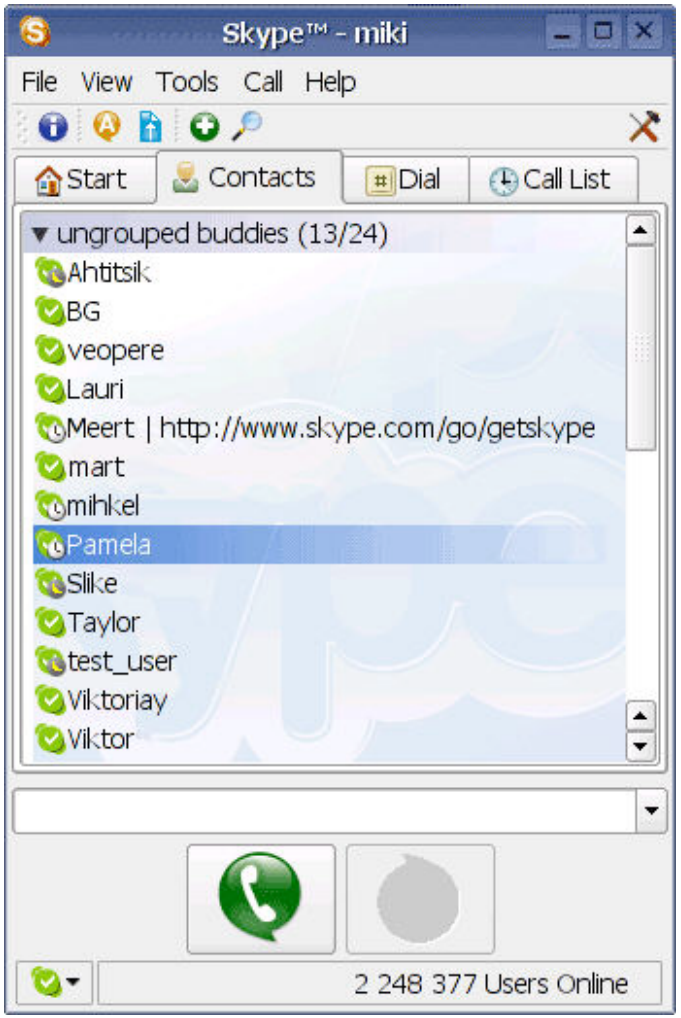


OK

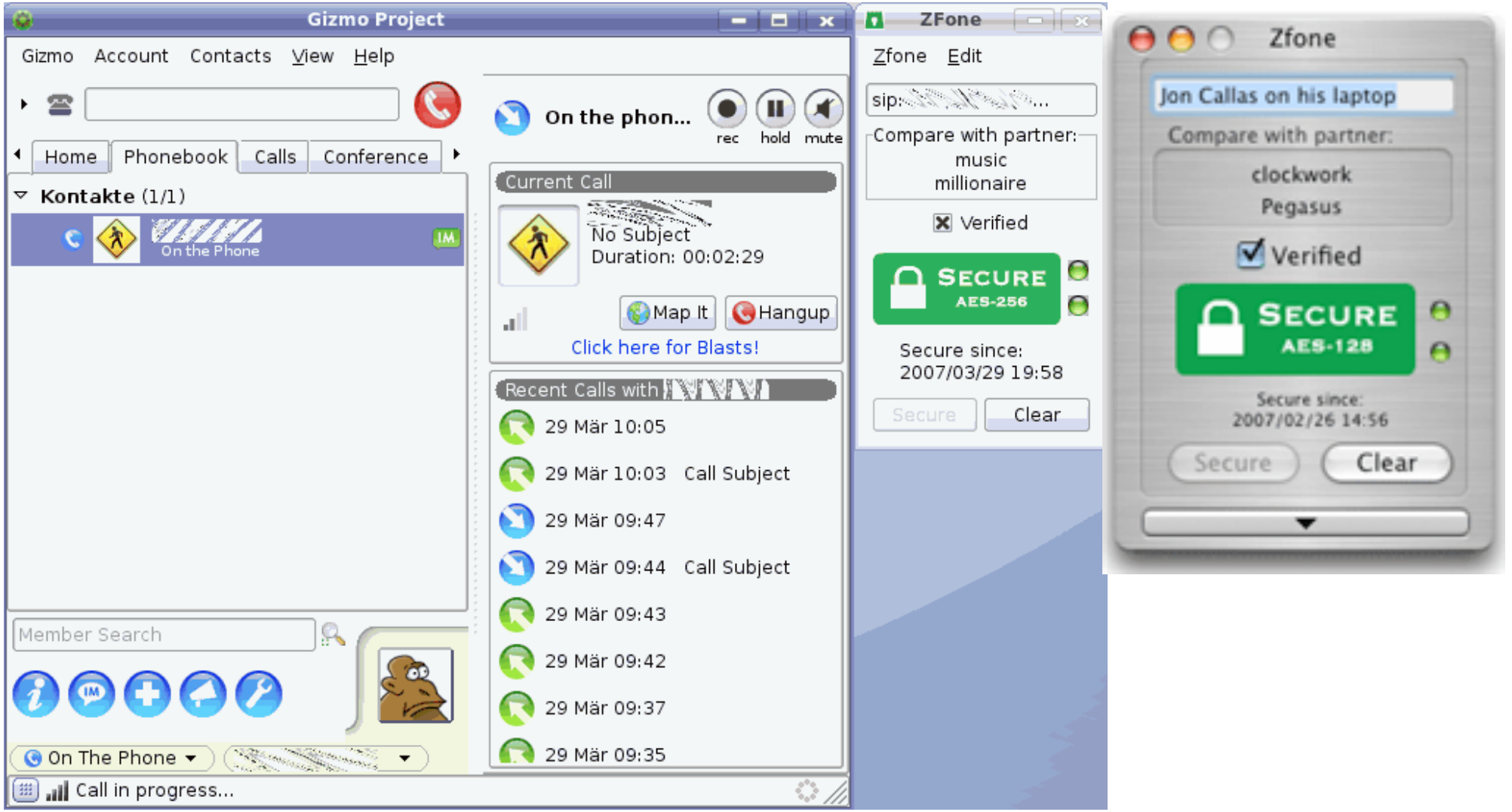
Practically what do we need to protect ourself?

Skype: What's about security?

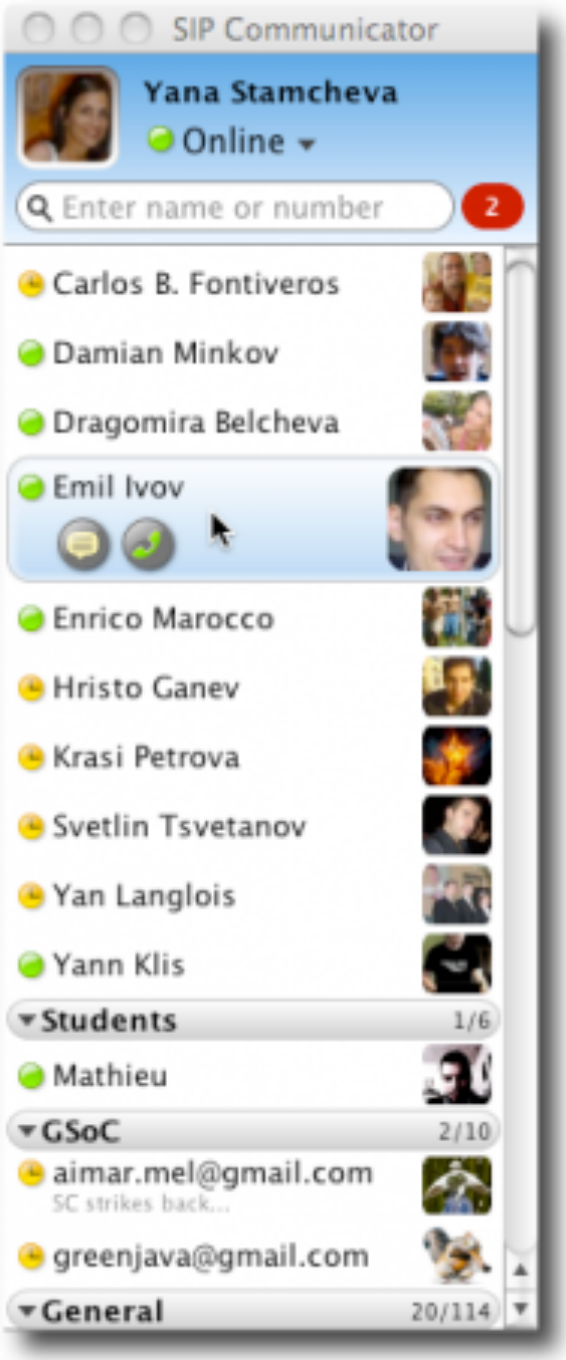
- Voice calls are enciphered (skype could have it but it's not available to most governments)
- Messages are available for Skype
- Skype IN/OUT are wiretappable
- Skype can be blocked in certain countries (es: UAE)



Zfone Free ZRTP encryption (only voice)



SIP Communicator – With ZRTP



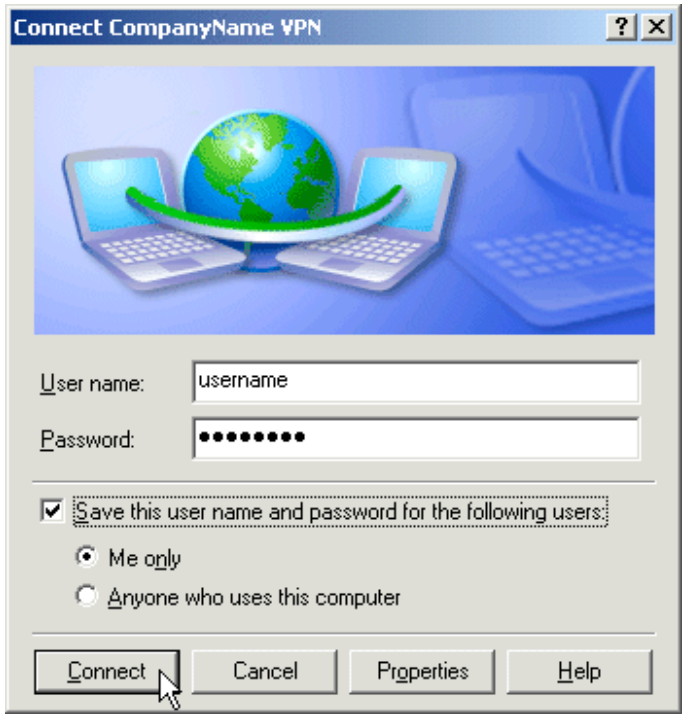
Mobile Encrypted products

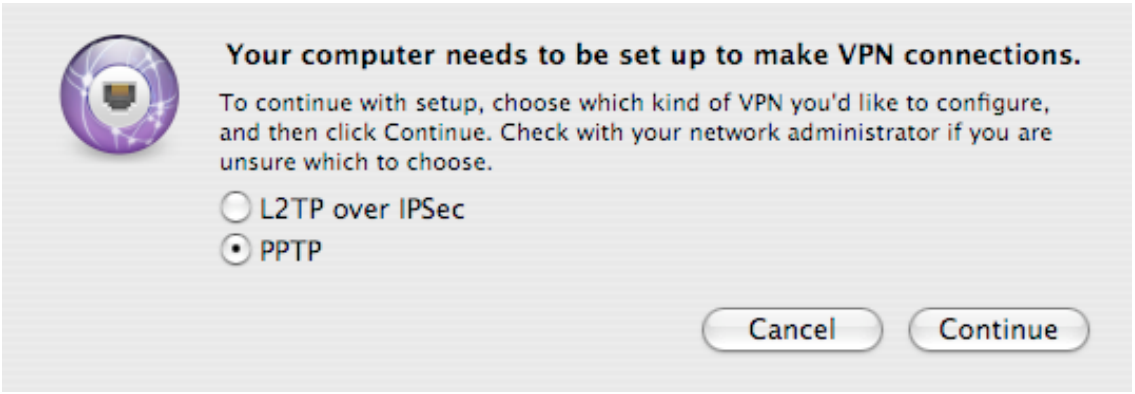
Only the ethical ones

PrivateGSM & Cryptophone

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