

## **Voice security and privacy:**

**Confidentiality protection, today solutions and upcoming technologies and standards**

**Security Summit**

**26 Mar 2009**

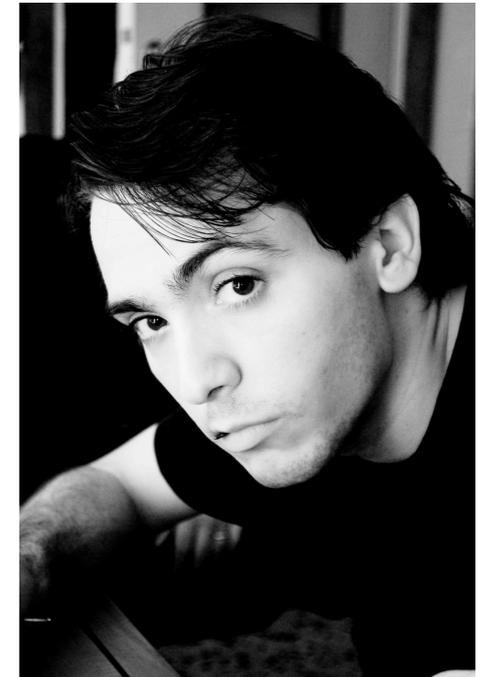
**Fabio Pietrosanti (naif)**

# Agenda: Mission impossible in 40 minutes?

- 1 - The need to intercept phone calls
- 2 - Methods to intercept phone calls **(tech)**
- 3 - The risk of eavesdropping (for ppl safety and democracy)
- 4 - Real case, Real world, Real risk scenario
- 5 - Currently available protection technologies **(tech)**
- 6 - Upcoming protection technologies **(tech)**



# Who am i Fabio Pietrosanti



Works in IT Sec till '98

Stay in digital underground with nickname "naif" till '95

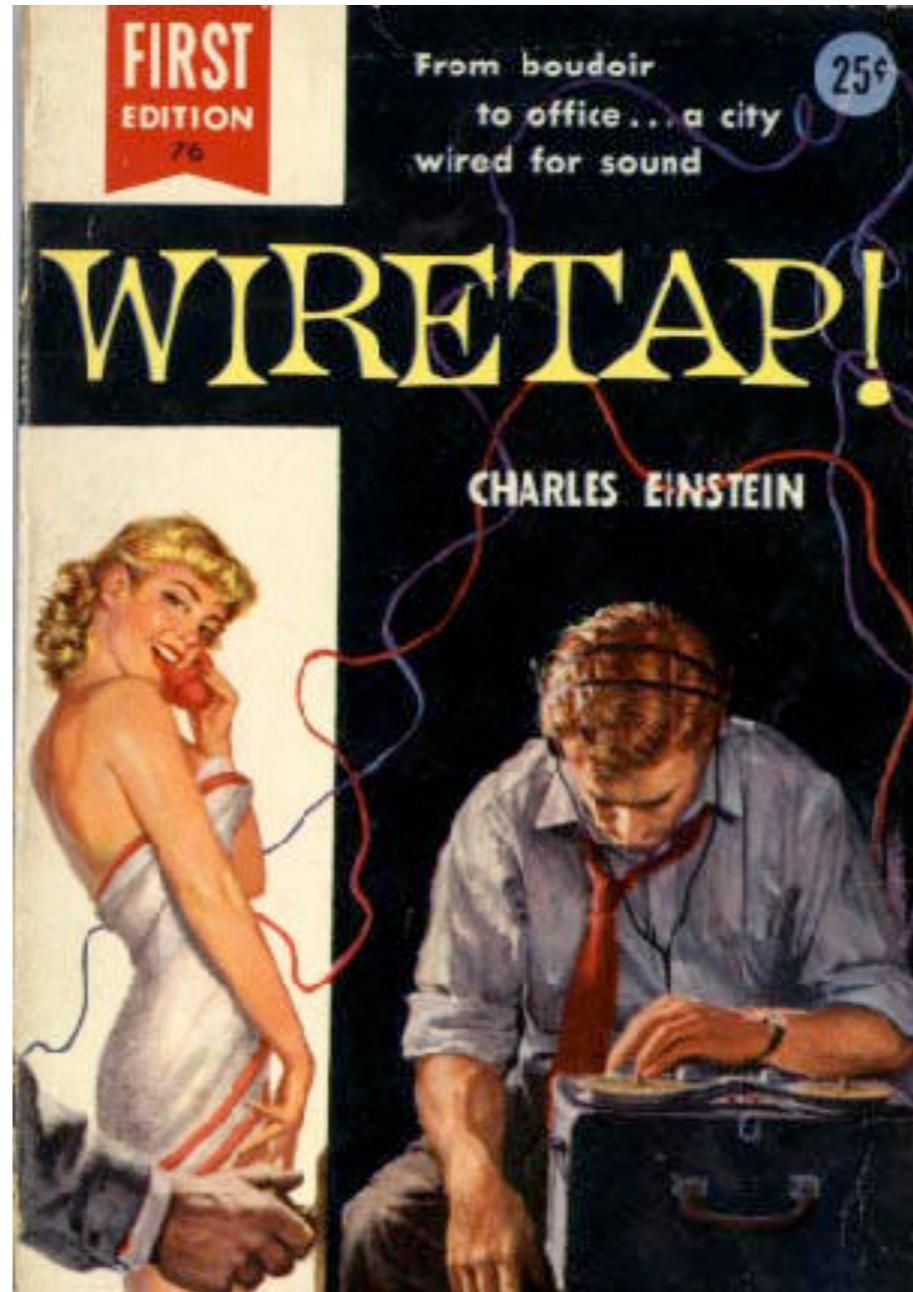
Worked as network security manager for I.NET SpA, Security Advisor Corporate Security Telecom Italia, now CTO of KHAMSA SA

Project and engineer end-to-end encryption products and technologies for VOICE and EMAIL messaging

- Technology partnership with Philip Zimmermann
- Participate to underground communities, sikurezza.org, s0ftpj, metro olografix, progetto winston smith, etc

I

## The need to intercept phone calls



## I - The need to intercept phone calls

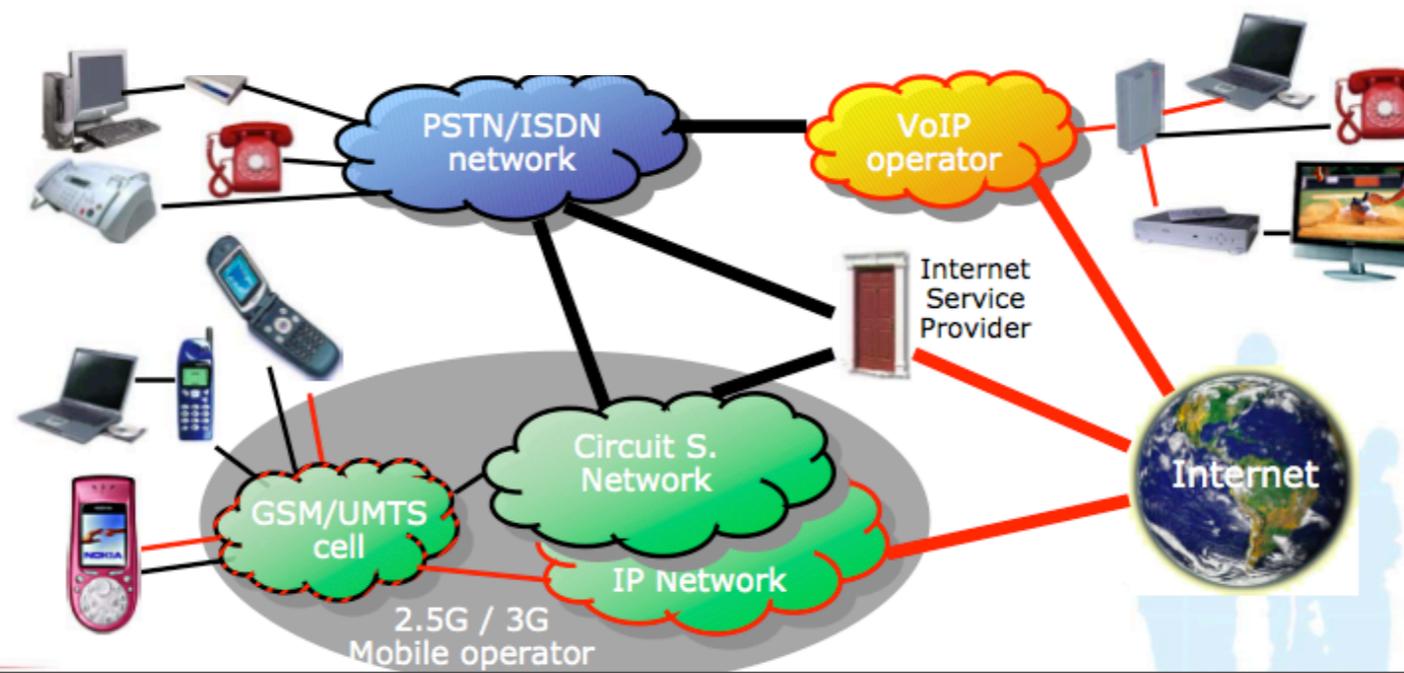
### Once upon a time...

- 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



## 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,)



I - 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?

## I - 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

(those information may require dedicated slides for each subject)

# I - 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

# I - 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

Perhaps it  
would be better  
if I just whispered  
the next bit...



**DON'T DISCUSS  
SECRETS ON THE  
TELEPHONE**

**2**

**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**



- Most methods can be cheap, only a few are expensive

## 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

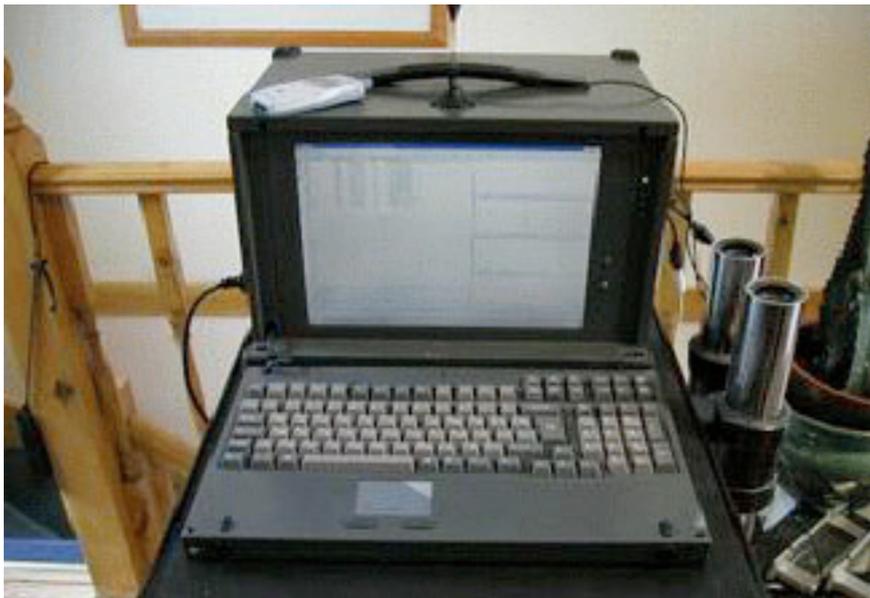
# Practical Approach: Mobile interception (I)

- Mobile phones can be intercepted with appropriate equipment (GSM, CDMA, UMTS)
- Passive Method (A5 Cracking)
- Active Method (Risk of detection)
- Active/Passive Method (100% success)



## 2 - Methods to intercept phone calls

# Practical Approach: Mobile interception (2)



- Can be leased along with intelligence professionals for 2000 EUR/day list price
- In theory are illegal in their use but in practice...Ask a quotation to serious investigation agency!

## 2 - Methods to intercept phone calls

### Practical Approach: Mobile interception (3)

- Uplink of operators between towers are not encrypted and monitoring devices are even less costly!



## 2 - Methods to intercept phone calls

# Practical Approach: ISDN/PSTN Interception

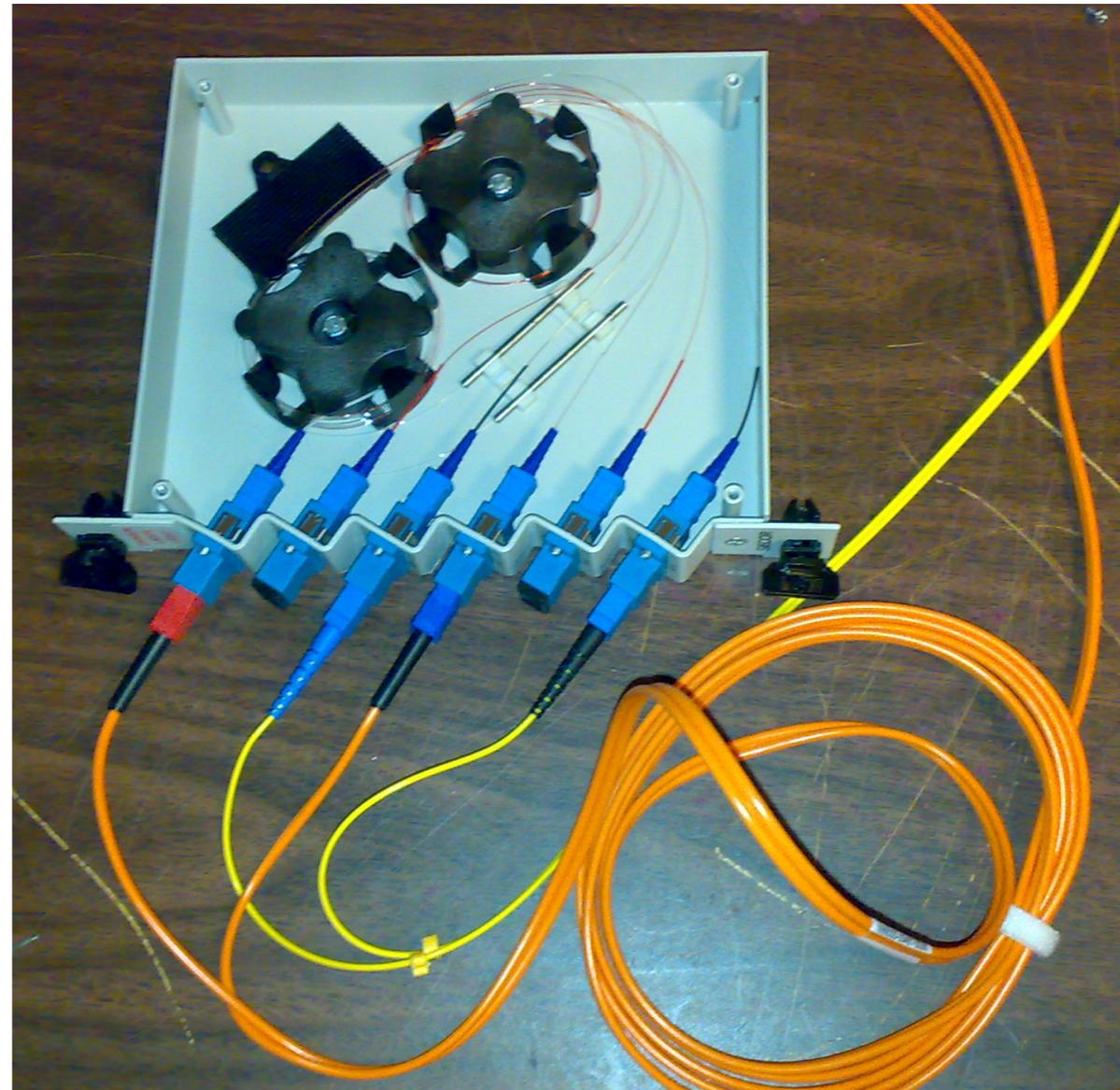


- Simple cable cut give impressive results!
- Budget? Less than 250 USD for a professional equipment transmitting in VHF

## 2 - Methods to intercept phone calls

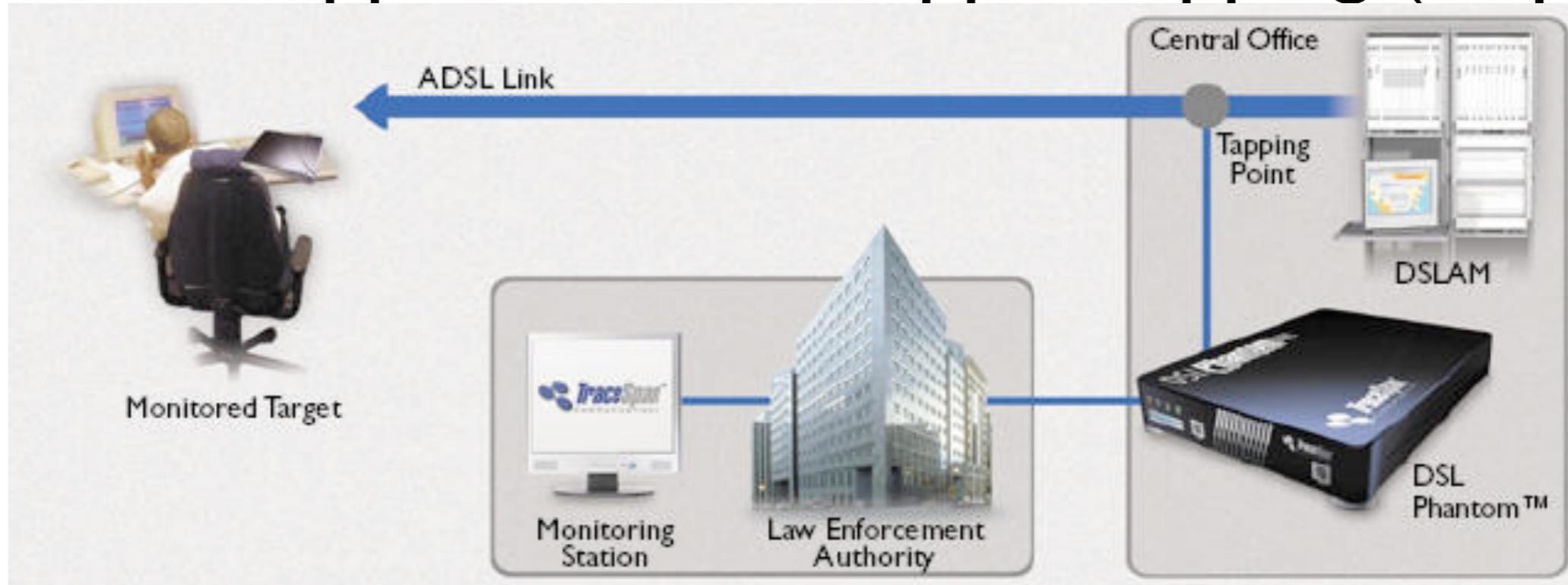
# Practical approach: Fiber Tapping (voip)

- 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 (voip)

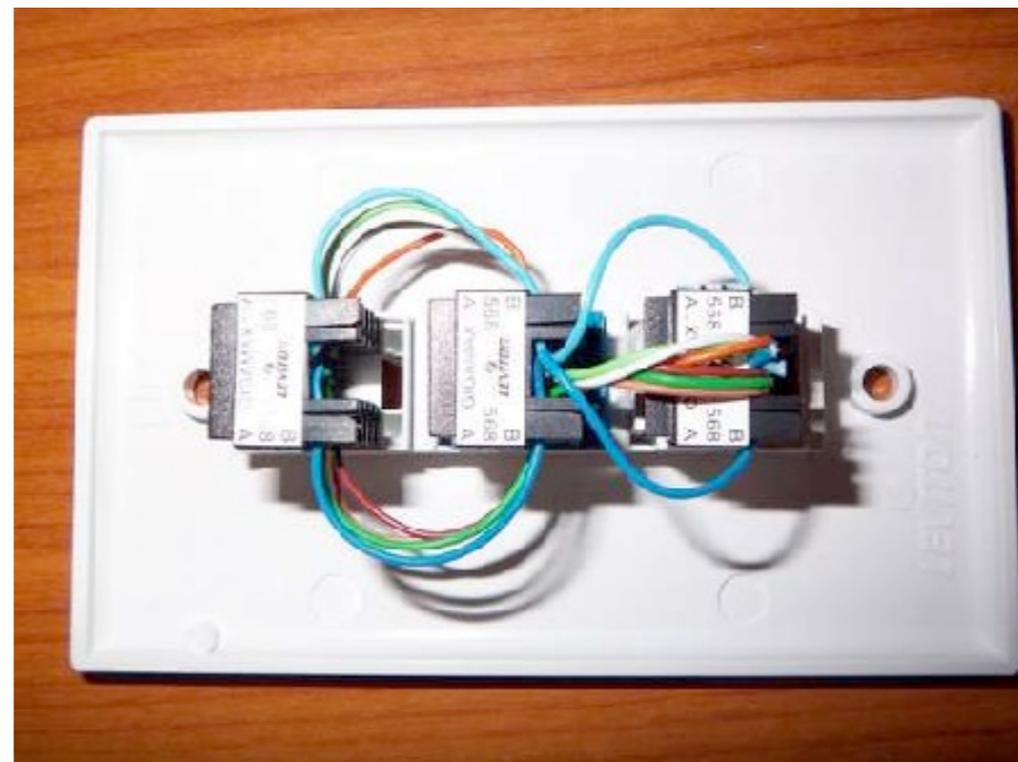
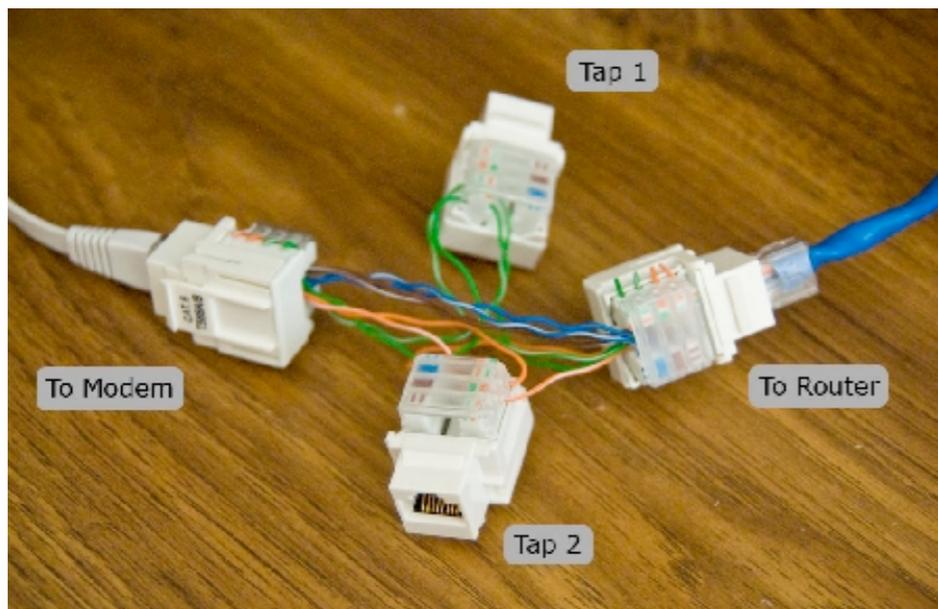


- Tap directly on ADSL copper with Tactical ADSL probe.

## 2 - Methods to intercept phone calls

# Practical Approach: Easy ethernet tapping (voip)

- From 20 to 150 USD budget



# The risk of eavesdropping (for people safety and democracy)



### 3 - The risk of eavesdropping

## **Quis custodiet ipsos custodes?**

Who will watch the watchers?

- The most important sentence.
- Reflect on the impact that eavesdropping have on the democracy



### 3 - The risk of eavesdropping

The human factor: Can we trust all of them together?

- Law Enforcement Employee
- Telco Employee
- Outsourced interception services employee
- Technical support employee of interception products
- Any party involved in the process...



### 3 - The risk of eavesdropping

## The human factor: Quiz

An employee of a Telco, 1800 USD net salary, working on technical structure is asked by an unknown person to wiretap a certain line. Is given 20k USD in advance. What he will do?

- a) Refuse the offer and report to the authority the request. He has an ethic!
- b) Accept the offer and execute the taping
- c) Accept and propose also a list price for phone call logs and details on owners of lines



## 3 - The risk of eavesdropping

### The technical factor

- Most interception are done by redirecting and/or copying intercepted traffic to a centralized place
- Do you think that the diverted traffic is protected? NO!
- From one place, the LEA office lines, every interception can be intercepted.
- VoIP multiply the risk factor by moving the intercepted traffic over the internet without protection.

### 3 - The risk of eavesdropping



#### The political factor and new freedom risks

- New parametric interception techniques are able to detect certain kind of pattern in ALL voice flows.
- Language blacklisting, gender detection and blacklisting, keyword matching give too much power in the hands of few persons and there's no law on how to deal with it.



### 3 - The risk of eavesdropping

## The need of perfectly enforceable laws on wiretapping

- Laws and procedures for efficient, controlled and guaranteed wiretapping are required
- Wiretapping of civil, secret and military agencies has to be regulated and the rules has to be subject to public scrutiny

## 3 - The risk of eavesdropping

# The need of perfectly enforceable laws on wiretapping

- **USA: Foreign Intelligence Surveillance Act (1978)**
- **Church Committee Report**
  - The Committee finds that information has been collected and disseminated in order to serve the purely political interests of an intelligence agency or the administration, and to influence social policy and political action.
  - White House officials have requested and obtained politically useful information from the FBI, including information on the activities of political opponents or critics.
  - The FBI has also used intelligence as a vehicle for covert efforts to influence social policy and political action.
- **NSA Warrantless Wiretapping (Bush Administration)**
  - **New York Times: Bush Lets U.S. Spy on Callers Without Courts**
  - “The White House asked The New York Times not to publish this article”
  - <http://www.cfr.org/publication/9763/>
  - <http://www.commondreams.org/headlines05/1216-01.htm>

**4**

**Real case, Real world, Real risk scenario**

## 4 - Real case, Real world, Real risk scenario

# Global interception: Echelon

- USA confirmed their global interception program with support of Great Britain and New Zealand
- European Parliament confirmed that Echelon was used to illegally divert airplanes deals to make US company wins respect to EU company



## 4 - Real case, Real world, Real risk scenario

2006 - Italy: Interception scandals, thousands of persons was profiled, intercepted and someone blackmailed.

- Adamo Bove, the head of Security of the Mobile Telco TIM was found “suicided”
- The head of secret services was wiretapped
- Thousands of people phone logs was acquired
- A numbers of illegal interception has been done
- <http://www.edri.org/edrigram/number4.15/italy>

10/05/2006

[Print](#) | [E-Mail](#) | [Share](#) | [Feedback](#)

EAVESDROPPING ON LA BELLA VITA

Font:

### Listening Quietly in Italy

By *Alexander Smoltczyk*

**Hardly anywhere in the world is the illegal monitoring of phone calls so prevalent as it is in Italy. Notwithstanding its negative connotations, such eavesdropping occasionally uncovers scandals that would otherwise remain undiscovered.**



AP   
A man and a woman on their

Statistically speaking, every Italian between the ages of zero and 100 has a mobile phone, and some even have two. According to a United Nations study, Italians lead Europe when it comes to chatting on their phones, with the rate of mobile ownership at a record-breaking 109 percent. In Italy, the mobile phone is as much an accessory as a pair of sunglasses, a fact that was never a problem for Italians, at least not until Sept. 20.

## 4 - Real case, Real world, Real risk scenario

### 2005 - Grece: Interception scandals, a bug has been put in Vodafone ICT infrastructure

- Costas Tsalikidis has been found dead head of Security of the Mobile Telco was found “suicided”
- The prime minister, the chief of secret services, a lot of activists has been intercepted
- No responsibility has been found
- All phone calls were diverted to a bunch of prepaid anonymous SIM cards

Last Updated: Friday, 24 March 2006, 08:31 GMT

[E-mail this to a friend](#)

[Printable version](#)

#### **Death muddies Greek spy probe**

By Richard Galpin  
BBC News, Athens

**A senior aide to the Greek prime minister is expected to be the next person to testify before a parliamentary committee investigating what is believed to be the worst espionage scandal in the country's history.**



Costas Tsalikidis: Did he help set up the phone-tapping?

Last month, the government admitted that the mobile phones of the prime minister, the most senior members of the cabinet and top security officials had all been tapped in 2004 - the year Athens hosted the Olympic Games.

## 4 - Real case, Real world, Real risk scenario

### 2001 - Finland: Interception scandals, mobile phones intercepted without warrants

- 3 top official of Finland Security Policy and the head of the security department of Sonera are charged for illegally intercepting user phone calls.
- The recording has been going for nearly a year without any formal authorization nor request

Business & Finance - Wednesday 6.11.2002

#### **Police believe Sonera security unit illegally monitored telephone records for nearly a year**

► Case could involve hundreds of aggrieved parties

Investigators at Finland's central criminal police, the National Bureau of Investigation (NBI), suspect that the security unit of the telecommunications company Sonera may have been illegally checking private telephone records for nearly a year.



Kimmo Sasi

Helsinki District Court has ordered two members of Sonera's security staff remanded in custody for aggravated violation of privacy in communications. According to the ruling, the two are suspected of having engaged in the illegal surveillance from August 1, 2000 to May 31, 2001.

## 4 - Real case, Real world, Real risk scenario

### 1996-today - Turkey: Continuous interception scandals, blackmailing and transcripts of wiretapping

#### In Turkey, Phone Users Fear Big Brother May Be Listening

By Amberin Zaman  
June 18, 1999

When journalist Fehmi Koru went out for dinner here recently with Islamist lawmaker Nazli Ilicak, he took his cellular phone along with him as usual. An hour later, Koru got a call from a fellow journalist. "He repeated almost word for word," Koru says, "my entire conversation with Mrs. Ilicak."

- Since 1996 in Turkey the political instability has caused a continuous tapping of phone calls of journalists, politicians, military and police representative
- Almost every year a scandals get out

## 4 - Real case, Real world, Real risk scenario

### France: Political spying by Mitterand cause him to loose election

#### **French Wiretapping Scandal Leads to Electoral Defeat**

*by Dave Banisar, Special to the Privacy Times*

The French Socialist Party suffered a resounding defeat in parliamentary elections on March 21 and 28 in part due to a wiretapping scandal that broke a week before the elections. Results showed that they lost over 200 seats in the Parliament and became the minority party. Socialist President Francois Mitterrand will remain in office but is expect to face a tough election in 1994.

The scandal emerged after reports and transcripts were leaked to Paris Daily Liberation that a special counter-intelligence group directly responsible to President Mitterrand illegally wiretapped numerous people during the 80's. Included in those wiretaps was

## 4 - Real case, Real world, Real risk scenario

### USA (2007): FBI missed to get authorization for interceptions because of too complicated laws

Hundreds of records unlawfully intercepted by FBI

**Complex interception laws confuse Feds and ISPs**

By [John Leyden](#) • [Get more from this author](#)

Posted in [Government](#), 15th June 2007 09:39 GMT

An internal audit has discovered that the FBI overstepped the mark in intercepting communication records at least 1,000 times since 2002.

The figures - based on an analysis of 10 per cent of the bureau's national security investigations over the last five years - are far higher than estimates of 22 wiretap "mistakes" in a Justice Department study released as recently as March.

## 4 - Real case, Real world, Real risk scenario

# 2009 - Colombia: Continue the debate and fight on corrupted officials doing wiretapping paid by drug traffickers

### Colombian prosecutors probe illegal wiretap scandal

---

*Posted 2009/02/22 at 6:14 pm EST*

BOGOTA, Feb. 22, 2009 (Reuters) — Colombian state prosecutors swooped on headquarters of the national intelligence agency on Sunday to probe charges that rogue agents illegally wiretapped politicians and judges as a paid favor to drug traffickers.

The telephone bugging accusations are the latest scandal to rock the state security agency, known as DAS, and could further stain President Alvaro Uribe's campaign to stamp out corruption of state law enforcement in the world's top cocaine supplier.

---

#### Related Topics

- ▶ [Drug Trafficking](#)
- ▶ [Illegal Drugs](#)
- ▶ [Political Policy](#)
- ▶ [Politics](#)
- ▶ [World Politics](#)

## 4 - Real case, Real world, Real risk scenario

UK: Incredible increased interception power and revelation of past activities

### UK Politics

#### UK 'monitored Irish phone calls'



The messages were scanned for key words

The UK Government tapped all telephone messages between Britain and Ireland during the past 10 years, it has been alleged.

Channel 4 News said a tower in Capenhurst, Cheshire, was used to intercept all telephone signals between Ireland and the UK from 1989 to when it closed down earlier this year.

### Secret plan to spy on all British phone calls

**Kamal Ahmed, political editor**  
**Sunday December 3, 2000**  
**The Observer**

Britain's intelligence services are seeking powers to seize all records of telephone calls, emails and internet connections made by every person living in this country.

## 4 - Real case, Real world, Real risk scenario

Poland (1996): Plenty of requests by citizens to ombudsman that received illegal transcripts of intercepted phone calls

### **Bugged About Wiretapping**

*Shortly after arriving in office, ombudsman Adam Zieliński attacks what he sees as governmental invasions of privacy.*

The Commissioner for Civil Rights Protection has voiced concern about government wiretapping after the ombudsman's office received 12 letters from "normal citizens" complaining about bugged telephone conversations.

"There are grounds to believe that the right to privacy is being violated in Poland," said ombudsman Adam Zieliński on May 16 during his first press conference since being appointed. He also expressed concern about the legality of tapping telephones.

The Polish press has reported that some local telephone exchanges are again using surveillance equipment exploited by the Polish Secret Police during the martial law in the '80s.

## 4 - Real case, Real world, Real risk scenario

### 2002 - Netherland: Dutch secret services interception equipment brought from Israel is tapping the interceptors

#### Dutch tapping room not kosher

by Paul Wouters, Patrick Smits



According to anonymous sources within the Dutch intelligence community, all tapping equipment of the Dutch intelligence services and half the tapping equipment of the national police force, is insecure and is leaking information to Israel. How difficult is it to make a back-door in the Dutch *Transport of Intercepted IP Traffic*[1] system?

The discussion focusses on the tapping installations for telephony and internet delivered to the government in the last few years by the Israeli company Verint[2].

This company was called Comverse-Infosys[3] until half a year ago, but was quickly renamed when the FBI started several investigations against it and arrested some of its employees in the US on suspicion of espionage. (See [pulled FoxNews stories](#), [Politech](#), [Cryptome](#) or [Google](#)).

- Interception equipment used by Dutch Intelligence agencies was brought from the israel company Verint. That equipment was leaking information on interception to israel.
- Interception technology is intercepting the interceptor! Another fall into the monitoring systems!

## 4 - Real case, Real world, Real risk scenario

### Conclusion of real world scenarios The tip of the iceberg.

- It's a serious problem that affect democracy and freedom even of western "democratic" countries
- It's a concrete and real problem
- Only few facts reach the public media



**CONFIDENTIAL**

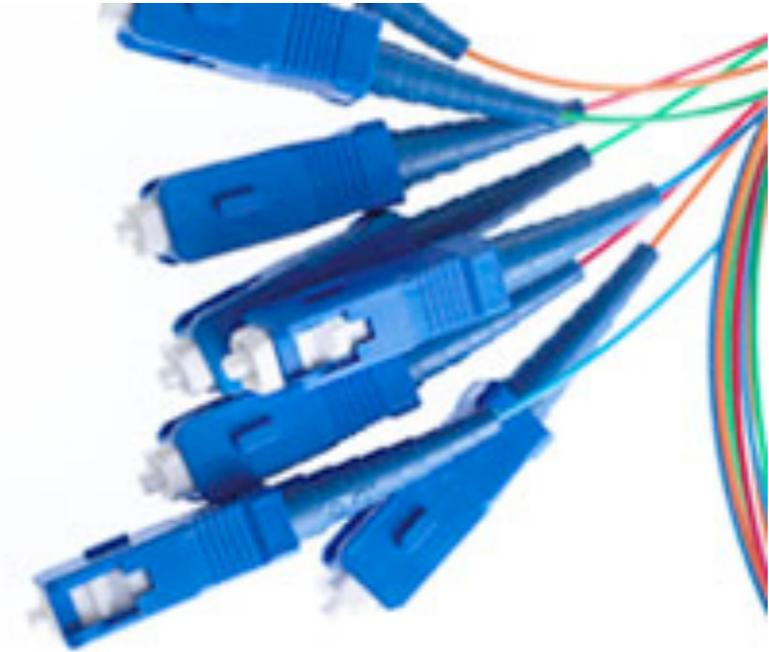
**5**

**Currently available protection technologies**

## 5 - Currently available protection technologies

# Communication technologies

- Traditional telephony (circuit switched)
  - ISDN (fixed)
  - PSTN (fixed)
  - GSM/CDMA/UMTS (mobile)
  - SAT (iridium, turaya, inmarsat, etc)
- VoIP Telephony (packet switched)
  - Softphone on PC
  - Hardware phones
  - Mobile internet (GPRS, EV-DO, EVDO, etc)



## 5 - Currently available protection technologies

# Authorities for standards

- ISO
- ITU-T
- GSM Consortium
- 3GPP
- 3GPP2
- NSA
- NATO
- IETF
- Telecom Industry Association (US interim standards)

## 5 - Currently available protection technologies

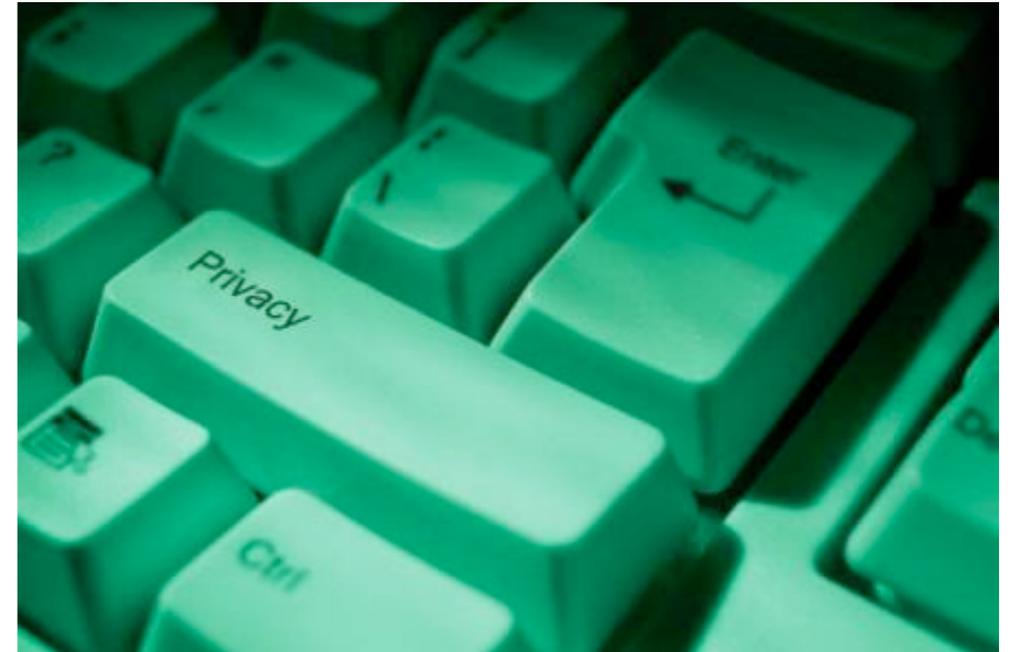
### Result of complexity in technologies and authorities

- NO single standard for telephony
- NO single standard for security (not even enough!)

## 5 - Currently available protection technologies

# Securing unsecure media

- Scrambling Vs. Encryption
- Voice connection Vs. Data connection
- Creating a digital data path over the media
  - Circuit Switched: the lossy codec issue ending with...“data calls”
  - VoIP: required standardization for interoperability
- And what about the signaling?



## 5 - Currently available protection technologies

# Communication technologies

Data Transmission	Circuit Switched	Packet Switched
	ISDN, GSM, CDMA, UMTS, PSTN, SAT	VoIP
Quality of service	Granted	GPRS / EDGE / UMTS Not Granted
Coverage	Full	Only Urban Area
Billing	Per-second (sender pay)	Per-packet (sender/receiver pay)
Signaling	Outband	In-band (over IP)

## 5 - Currently available protection technologies

# VoIP basic

- SIP is used to transport signaling informations
- RTP is used to carry media traffic (audio, video)
- Both usually works over UDP protocol

## 5 - Currently available protection technologies

# VoIP Security: media encryption

- Born without security in mind (like most technologies)
- Encryption has been brought to IETF standard in March 2004 with SRTP (RFC3711), even if it was including a NULL encryptor...
- SRTP support “Counter mode” and f8-mode for symmetric encryption and HMAC-SHA1 for integrity checking (32bit)
- There was only one BIG issue, no really secure and efficient key agreement method
  - MIKEY
  - SDES

## 5 - Currently available protection technologies

# VoIP Security: SRTP SDES

- SDES is the only widely diffused and implemented key agreement method
- It's transported over SIP

So useful and secure!

```
INVITE sips:*97@ietf.org;user=phone SIP/2.0
Via: SIP/2.0/TLS 172.20.25.100:2049;branch=z9hG4bK-s5kcqg8jqjv3;rport
From: "123" <sips:123@ietf.org>;tag=mogkxsrhm4
To: <sips:*97@ietf.org;user=phone>
Call-ID: 3c269247a122-f0ee6wcrvkcq@snom360-000413230A07
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:123@172.20.25.100:2049;transport=tls;line=gyhiepdm>;reg-id=1
User-Agent: snom360/6.2.2
Accept: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO
Allow-Events: talk, hold, refer
Supported: timer, 100rel, replaces, callerid
Session-Expires: 3600;refresher=uas
Min-SE: 90
Content-Type: application/sdp
Content-Length: 477

v=0
o=root 2071608643 2071608643 IN IP4 172.20.25.100
s=call
c=IN IP4 172.20.25.100
t=0 0
m=audio 57676 RTP/AVP 0 8 9 2 3 18 4 101
a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:WbTBosdVUZqEb6Htqhn+m3z7wUh4RJVR8nE15GbN
a=rtpmap:0 pcmu/8000
a=rtpmap:8 pcma/8000
a=rtpmap:9 g722/8000
a=rtpmap:2 g726-32/8000
a=rtpmap:3 gsm/8000
a=rtpmap:18 g729/8000
a=rtpmap:4 g723/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
aptime:20
a=encryption:optional
a=sendrecv
```

## 5 - Currently available protection technologies

# VoIP Security: SIP/TLS

- But SIP channel can be enciphered, there is SIP/TLS
- The key can be transported securely between the client and the intermediary (much like the security model of GSM/UMTS between mobile and radio network controller)

## 5 - Currently available protection technologies

# VoIP Security: end-to-end encryption?

- NO!
- There's still a little detail, and in security details **matter** .

The PBX can always observe and record the key!



[www.jo-bild.de](http://www.jo-bild.de)

## 5 - Currently available protection technologies

### Traditional telephony: no security by default

- Circuit Switched Telephony is considered secure, as secure as the Telco network can be considered secure
- Standards for secure telephony was built only for governmental use and usually specifications was not available

## 5 - Currently available protection technologies

# Traditional telephony: clipper, born to fail

- Clipper Chip was created by White House in 1993 implementing SkipJack algorithm
- In 1994 FIPS 185 Escrowed Encryption Standard has been approved
- AT&T release TD3600E
  - 56bit encryption
  - 4800bps data path over PSTN
- In 1996 the project was considered a complete failure
- In 1998 skipjack has been declassified



## 5 - Currently available protection technologies

# Traditional telephony: PGPhone

- In 1995 mr. Philip Zimmermann (2 'n) created PGPhone
- PGPhone was a software for Windows to be used connecting the PC trough a modem an dialing the other party
- Was using ephemeral Diffie-Hellmann protocol
- Was using a short authentication string to detect man in the middle attack
- Unfortunately he was too visionary, in 1996 the internet world was still not ready for such technology
- In 1997 it became abandonware



## 5 - Currently available protection technologies

# Traditional telephony: STE and STU

- From 1987 US Government standard using STU-III
  - A set of cryptographic algorithm inside crypto cards programmed by National Security Agency
- In 2004 the STE (Secure Terminal Equipment) succeeded to STU-III
- STE now use the SCIP, Secure Communication Interoperability Protocol, formerly named Future Narrowband Digital Terminal (FNDDT)
- SCIP has been first used in 2001 in Condor Secure mobile Phone



## 5 - Currently available protection technologies

# Traditional telephony: SCIP

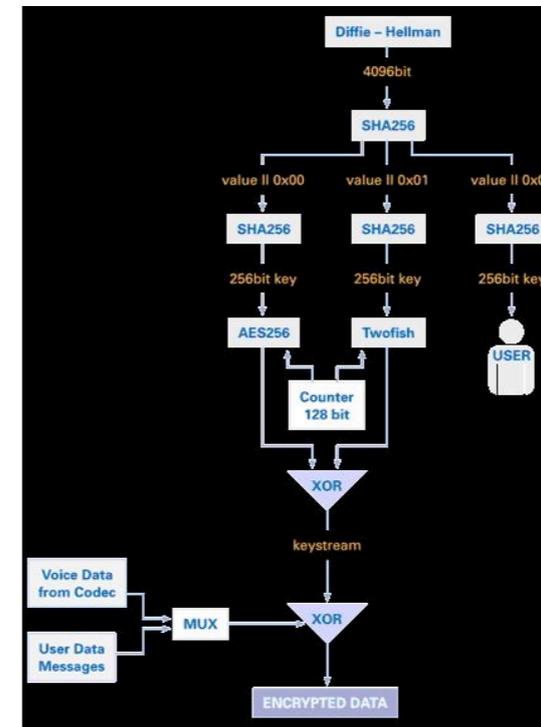
- SCIP is also known as the NATO extension of FNDT
- Born to work over land line, military radios, communication satellite and Voice over IP (used in us over SIPRNET, Secret Internet Protocol Router Network)
- Use MELPe codec, royalty free only for US Government and NATO
- Very narrowband stay at minimum of 2400hz (2400bps) as it works also over crap iridium data links
- Mr. Obama use SCIP over a Sectera Phone as a blackberry replacement

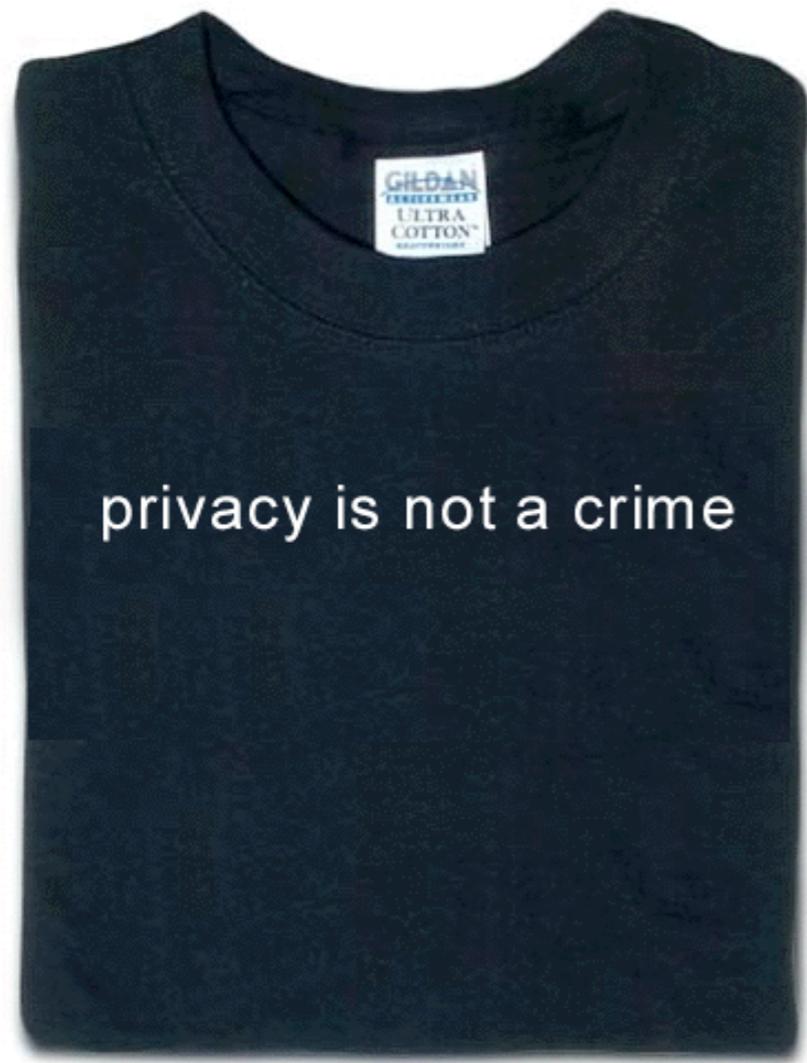


## 5 - Currently available protection technologies

# Traditional telephony: Cryptophone

- In 2001 Cryptophone was born and it kept fully open their source code and security protocol design
- The company (composed of several xs4all and ccc hackers) build up the product and started selling the hardware phones
- Unfortunately the protocol did not get public attention and did not get strong public auditing nor other interoperable use





**6**

**Upcoming protection technologies**

## 6 - Upcoming protection technologies

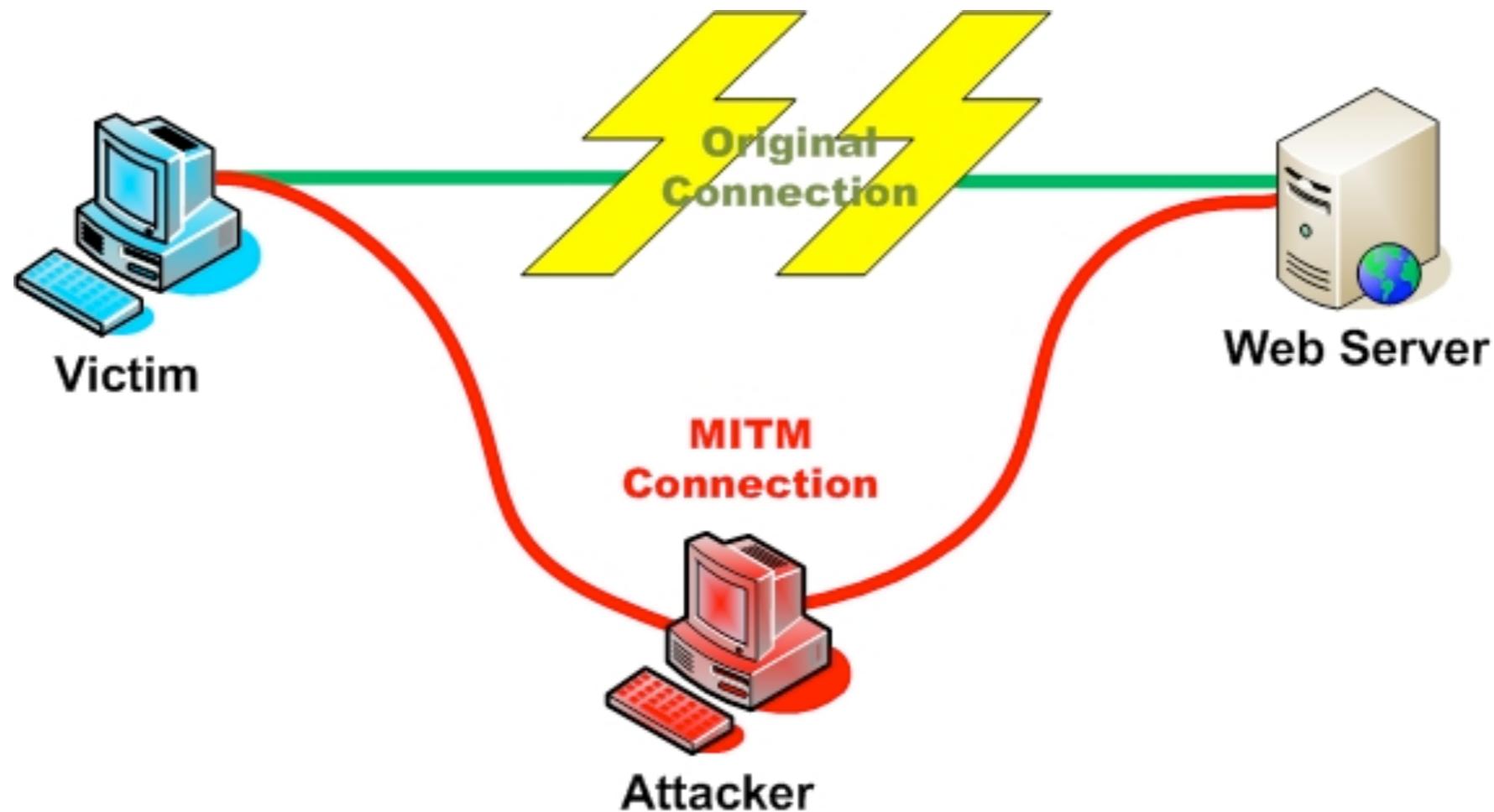
### Voice Over IP Security: Finally end-to-end encryption!

- Voice over IP finally got end-to-end encryption with key agreements methods and new protocol approved by IETF
- As a story we all have already seen with OpenPGP/MIME vs. S/MIME there are two competing standards
- A Hierarchical standard to be integrated within PKI infrastructure - DTLS
- A non hierarchical standard with a very high level or paranoid - ZRTP



## 6 - Upcoming protection technologies

### Voice Over IP Security: The main the middle problem



## 6 - Upcoming protection technologies

### Voice Over IP Security: The main the middle problem

- Even if the call is 'encrypted' it does not mean that is secure
- Key agreements can be compromised and security broken if a successful MiTM (Man in The Middle) attack is carried on
- MiTM attacks carry hacks and tricks to the cryptographic key exchange making the communication appear "as secure" even if a malicious third party is diverting and wiretapping all the traffic

## 6 - Upcoming protection technologies

### Voice Over IP Security: DTLS & DTLS-SRTP

- In March 2006 DTLS (Datagram Transport Layer Security) has been defined to protect UDP streams much like SSL and the successor TLS used in the web world
- RTP runs over UDP
- In 2008 a method to use DTLS as a key exchange method of SRTP to encipher RTP packets won the standardization path of IETF

## 6 - Upcoming protection technologies

### Voice Over IP Security: DTLS-SRTP

- Require a PKI to be used
- It completely rely on SIP channel integrity
- In order to keep the SIP channel integrity “Enhanced SIP identity” standard (RFC4475) has to be used .
- Unfortunately MiTM protection cannot be guaranteed when calling a phone number (+4179123456789) and so DTLS-SRTP collapse in providing security
- So the basic concept is that DTLS require a PKI to works, with all the burocracy and complexity around building it
- But don't worry, most of the vendor that announced to use DTLS-SRTP said that they will provide self-signed certificate. No security assured.

## 6 - Upcoming protection technologies

### Voice Over IP Security: ZRTP

- Mr. Zimmermann did it again and by leveraging the old PGPhone concept of 1995 he designed and proposed for standardization ZRTP VoIP security protocol
- ZRTP does not use SIP but instead use in a clever way the RTP packet to perform in-band (inside RTP) key handshake
- The concept is simple: what we need to protect?
  - The media
- So why modify the SIP signaling increasing complexity?
- KISS principle always stay ahead
- Implemented by Philip Zimmermann (zfoneproject.com), Werner Viettmann (gnutelephony.org), MT5 (unknown non-public implementation)

## 6 - Upcoming protection technologies

### Voice Over IP Security: ZRTP

- ZRTP is provided to IETF as a standard (currently in standardization path) as a key initialization method for SRTP
- ZRTP use different key agreements method inside the cryptographic protocol
  - ECDH
  - DH
  - Preshared Key
- ZRTP support PFS (Perfect Forward Secrecy)
- Can be used over most signaling protocols that use RTP for media transport (SIP, H.323, Jingle, P2P SIP)

## 6 - Upcoming protection technologies

### Voice Over IP Security: ZRTP

- Short Authentication String as a method to detect MiTM wiretapper
- the two users at the endpoints verbally compare a shared value displayed at both end
- If the value don't match, it indicates the presence of someone doing a man in the middle attack



## 6 - Upcoming protection technologies

### Voice Over IP Security: Comparison of key agreements method of SRTP

Technology	SRTP - SDES	SRTP - DTLS	SRTP - ZRTP
Require SIP security	Yes	Yes (with additional complexity)	No
The PBX can see the key?	Yes	No (but it depends)	No
Man in the middle protection (always)	No	Yes (not always)	Yes
Different implementation in Q1 2009	Yes	No	Yes

## 6 - Upcoming protection technologies

### Traditional Telephony Security: ZRTP/S

- In 2008 Mr. Zimmermann developed jointly with KHAMSA SA an extension of ZRTP to works again, like PGPhone already does in 1995, over traditional phone lines
- ZRTP/S is a communication and security protocol that works over traditional telephony technologies (GSM, UMTS, CDMA IS94a, PSTN, ISDN, SATCOM, BLUETOOTH)
- Basically it works over a 'bitstream channel' that can be easily represented like a 'serial connection' between two devices

## 6 - Upcoming protection technologies

### Traditional Telephony Security: ZRTP/S (Design)

- ZRTP/S can be, oversimplifying, a subset of a “compatible” RTP packet refactored to work over narrowband channels
- It works over very narrowband links (4800 - 9600bps)
- It works over high latency links (GSM CSD and SAT) with a “compressed” ZRTP handshake
- In order to work over most channels it requires the usage of narrowband codecs with advanced DTX and CNG features (AMR 4.75, Speex 3.95, MELPe 2.4)
- Implemented in open source as an additional module to libzrtp
- Soon to be released for public and community usage

## 6 - Upcoming protection technologies

### Traditional Telephony: Comparison of technologies

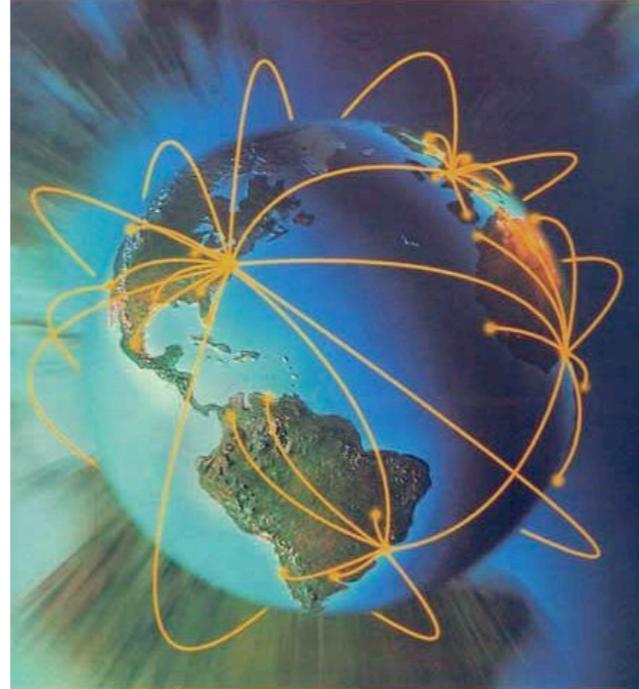
Technology	SCIP	ZRTP/S	Cryptophone	PGPhone
Usage	Government only	Any	Business or Government	Any
Interoperable	Yes	Yes	No	No
Codec	MELPe	Speex, AMR, MELPe	ACELP	N/A
Peer review	NSA/NATO	IETF, Community	Cryptophone itself	Deprecated

Conclusion

Conclusion



- Market and technologies are fragmented
- Big Telco & Big Governments are against end-to-end encryption
- A standard must win
- The opensource and the security communities play a fundamental role
- Anyone should think about supporting it



## **Voice security and privacy:**

**Confidentiality protection, today solutions and upcoming technologies and standards**

**Security Summit**

**26 Mar 2009**

**Fabio Pietrosanti (naif) - [fp@khamisa.ch](mailto:fp@khamisa.ch)**

**Questa sera Hacking Film Festival al Cinema Anteo!**