

Intrusioni, voice spam, “phone phreakers”, hacking telefonico:

tipologie dei rischi connessi all'utilizzo
delle comunicazioni IP, wireless e WiMax.



Roma, 26 Settembre 2007



Raoul Chiesa (OPST, OPSA)



Socio Fondatore,
Membro del Comitato Direttivo e del
Comitato Tecnico-Scientifico del CLUSIT

Agenda

- Il relatore
- Il CLUSIT
- Cybercrime VS Telecomunicazioni: le relazioni pericolose
- La storia insegna
- Tipologie di attacchi e frodi
- Cosa ci riserva il prossimo futuro ?
- Conclusioni
- Bibliografia

Who is Who

\$ whois raoul

□ Hacker dal 1986 al 1995, quando vengo arrestato per una lunga serie di violazioni informatiche presso istituzioni ed enti ad alta criticità, nel corso dell'operazione "Ice Trap" condotta dalla S.C.O., Criminalpol, Interpol ed FBI.

□ Da allora il mio approccio all'ICT Security è maturato: nel 1996 inizio ad occuparmi professionalmente di ethical hacking e, dal 1997, coordino il Tiger Team di @ **Mediaservice.net**, società di consulenza vendor-independent molto nota a livello europeo.

□ Sono inoltre socio fondatore del **CLUSIT** (Associazione italiana per la sicurezza informatica), dove ricopro anche la carica di membro del Comitato Direttivo (C.D.) e del Comitato Tecnico Scientifico (C.T.S.). Membro del Board of Directors **ISECOM** (Institute for Security and Open Methodologies), **TSTF** (Telecom Security Task Force), del Capitolo Italiano di **OWASP** (Open Web Applications Security Project) e dell'Italian ISO ISMS IUG 2700*.



\$ whois CLUSIT

- Associazione Italiana per la Sicurezza Informatica, fondata nell'anno 2000 e con sede presso l'Università degli Studi di Milano, Dipartimento di Scienze dell'Informazione (DSI).
- I nostri obiettivi:
 - Diffondere la **cultura della sicurezza informatica** presso le Aziende, la Pubblica Amministrazione e i cittadini
 - Partecipare alla elaborazione di **leggi, norme e regolamenti** che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo
 - Contribuire alla definizione di percorsi di **formazione** per la preparazione e la **certificazione** delle diverse figure professionali operanti nel settore della sicurezza
 - Promuovere l'uso di **metodologie** e **tecnologie** che consentano di migliorare il livello di sicurezza delle varie realtà

I Soci del Clusit

Rappresentano l'intero "Sistema Paese":

- RICERCA
- INDUSTRIA
- COMMERCIO e DISTRIBUZIONE
- BANCHE, FINANZA e ASSICURAZIONI
- PUBBLICA AMMINISTRAZIONE
- SANITÀ
- CONSULENZA, AUDIT
- SERVIZI
- TELECOMUNICAZIONI
- INFORMATICA

CLUSIT: il Ruolo Istituzionale

In ambito nazionale, Clusit opera in collaborazione con:

- Ministero delle **Comunicazioni**
- Ministero degli **Interni**
- Ministero dell'**Istruzione**
- Presidenza del Consiglio, Dipartimento per l'**Innovazione** e le **Tecnologie**
- **Polizia** Postale e delle Comunicazioni
- Autorità **Garante** per la tutela dei dati personali
- Autorità per le **Garanzie** nelle **Comunicazioni**
- **Confindustria** Servizi Innovativi e Tecnologici
- **Università** e Centri di **Ricerca**
- **Associazioni** Professionali e Associazioni dei **Consumatori**

CLUSIT: i Rapporti Internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con:

- **CERT**
- **CLUSI** (CLUSIB, CLUSIF, CLUSIS, CLUSSIL)
- **Università** e Centri di **Ricerca** in Austria, Belgio, Danimarca, Francia, Estonia, Grecia, Inghilterra, Irlanda, Lussemburgo, Olanda, Polonia, Spagna, Svezia e Svizzera
- **Commissione Europea** DG Information Society
- **ENISA** (European Network and Information Security Agency)
- **OCSE** (Organisation for Economic Co-operation and Development)
- **Associazioni Professionali** (ISACA, ASIS, ISC², ISSA, SANS) e **Associazioni dei Consumatori**

Cybercrime VS Telecomunicazioni [le relazioni pericolose]

Il cybercrime: ieri

- Si parla tanto di “Cybercrime”... Spesso ci si dimentica, però, di una constatazione tanto semplice quanto banale:

**“Ogni nuova forma di tecnologia,
apre la strada a nuove forme di criminalità”.**

- Il rapporto tra tecnologia e criminalità è stato, da sempre, caratterizzato da una sorta di “gara” tra buoni e cattivi.
- ✓ Per esempio, agli inizi del ‘900, con l’avvento dell’automobile, i “cattivi” iniziarono a rubarle.
- ✓la polizia, per contrastare il fenomeno, definì l’adozione obbligatoria delle targhe (car plates)...
- ✓ed i ladri iniziarono a rubare le targhe delle auto (o a falsificarle).

Il cybercrime: oggi

- Le automobili sono state sostituite dalle informazioni.

Hai l'informazione, hai il potere.

(Quantomeno, nella politica, nel mondo del business, nelle relazioni personali...)

- Questo, semplicemente perché l'informazione è immediatamente trasformabile in:

- ✓ Vantaggio competitivo
- ✓ Informazione sensibile/critica
- ✓ Denaro
- ✓ Ricatto

- Esempi ?

- Calciopoli
- Scandalo Telecom
- Emanuele di Savoia
- Vallettopoli
- Corona
- Mc Laren/Ferrari
-

- ... ecco perché tutti “vogliamo essere *sicuri*”.

- Non a caso, si chiama IS – Information Security ☺

Le relazioni pericolose

- **Storicamente, gli hacker sono da sempre interessati al mondo delle TLC**
- **Infatti, che si parli di hacking, phreaking, warez o carding, è essenziale:**
 - **Non pagare le comunicazioni (dati o voce che sia)**
 - **Non rilasciare i propri numeri telefonici (quindi, utilizzare numeri altrui)**
 - **Non essere rintracciabili**
 - **Divertirsi, ove possibile/applicabile**

La storia insegna

Phreaking

- “ I do it for one reason and one reason only. I'm learning about a system. **The phone company is a System.** A computer is a System, do you understand? If I do what I do, it is only to explore a system. Computers, systems, that's my bag. **The phone company is nothing but a computer.** ”

Captain Crunch

Tratto da “*Secrets of the Little Blue Box*”
Esquire Magazine, Ottobre 1971



Hacking & Phreaking historical overview

- '60 Hacking Roots: MIT & TMRC
- '70 Phone Phreaking and Captain Crunch (Wozniak & Jobs)
- '80: Hacking Message Boards and Hacking Groups
- 1983: War Games, Kids Games
- 1984: Ezines-> Phrack & 2600 The Hacker's Quarterly
- 1986: Use a computer, go to Jail (CFAA: Computer Fraud & Abuse Act)
- 1988: RTM: Internet is NOT secure (?) / The WANK Worm
- 1989: CCC & KGB (Spy Game ?)
- January the 15th, 1990: the Big Black Out (AT&T Intl. Phone System Crash, MOD & LOD)
- 1990: Operation Sundevil (The Hacker's Crackdown)
- 1993: Buy a Porsche or hack one ? -> Kevin Poulsen and the L.A. gangs
- 1994: Hacking tools
- 1995: Kevin D. Mitnick & Tsutomu Shimomura ("IP Spoofing is not practically applicable")
- 1998: CdC & Back Orifice / Gulf War & Israeli Connection (The Analyzer)
- 1999: Steal money, get died (China)
- 2000: Yahoo, Amazon, Ebay DDoS Attacks: Intl. Hacking Scene says NO
- [2001-2005] : 144/166/899 frauds, SMS spoofing, wardriving, telephone scams,,
- 2006-2007: Telecom Italia scandal: The Vodafone Hellas Wiretapping scandal

Evolution of Mobile Networks

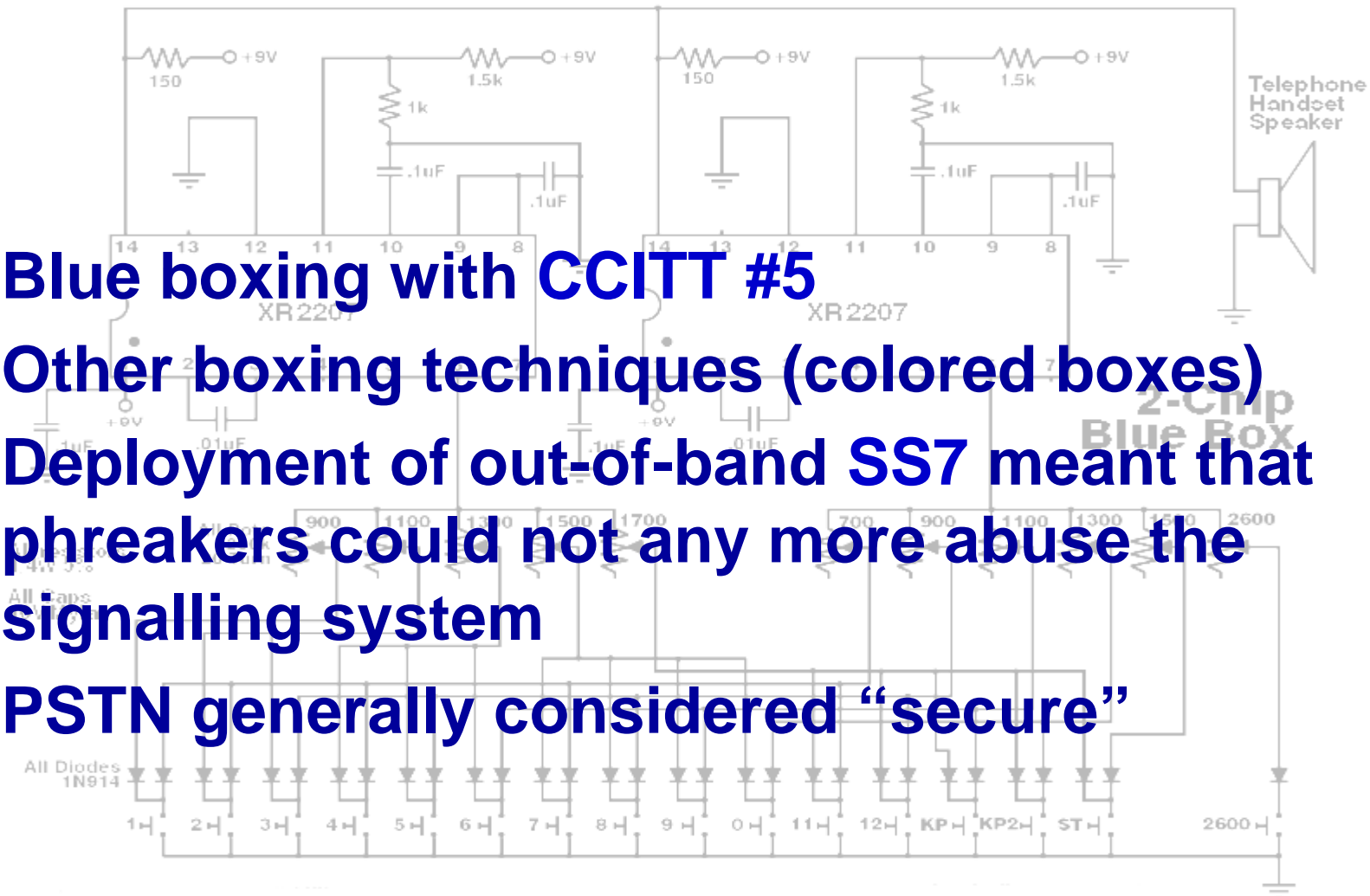
- **Pre-mobile: the PSTN**
- **Early analog systems: NMT, AMPS, TACS (“1G”)**
- **Digital systems: GSM, CDMA**
- **2G: CSD, HSCSD**
- **2.5G: GPRS, EDGE**
- **3G: CDMA1x, CDMA-2000, WCDMA**
- **NGN, 4G, IMS**
- **5G: no operator required?**



Tipologie di attacchi e frodi

PSTN security issues

- Blue boxing with CCITT #5
- Other boxing techniques (colored boxes)
- Deployment of out-of-band SS7 meant that phreakers could not any more abuse the signalling system
- PSTN generally considered “secure”



Security issues in 1G systems

- **Eavesdropping (no over the air encryption, easy to listen in to frequencies with a simple radio scanner)**
- **VERY EASY Cloning of phones by intercepting the serial number (ESN)**



Lessons from 1G systems

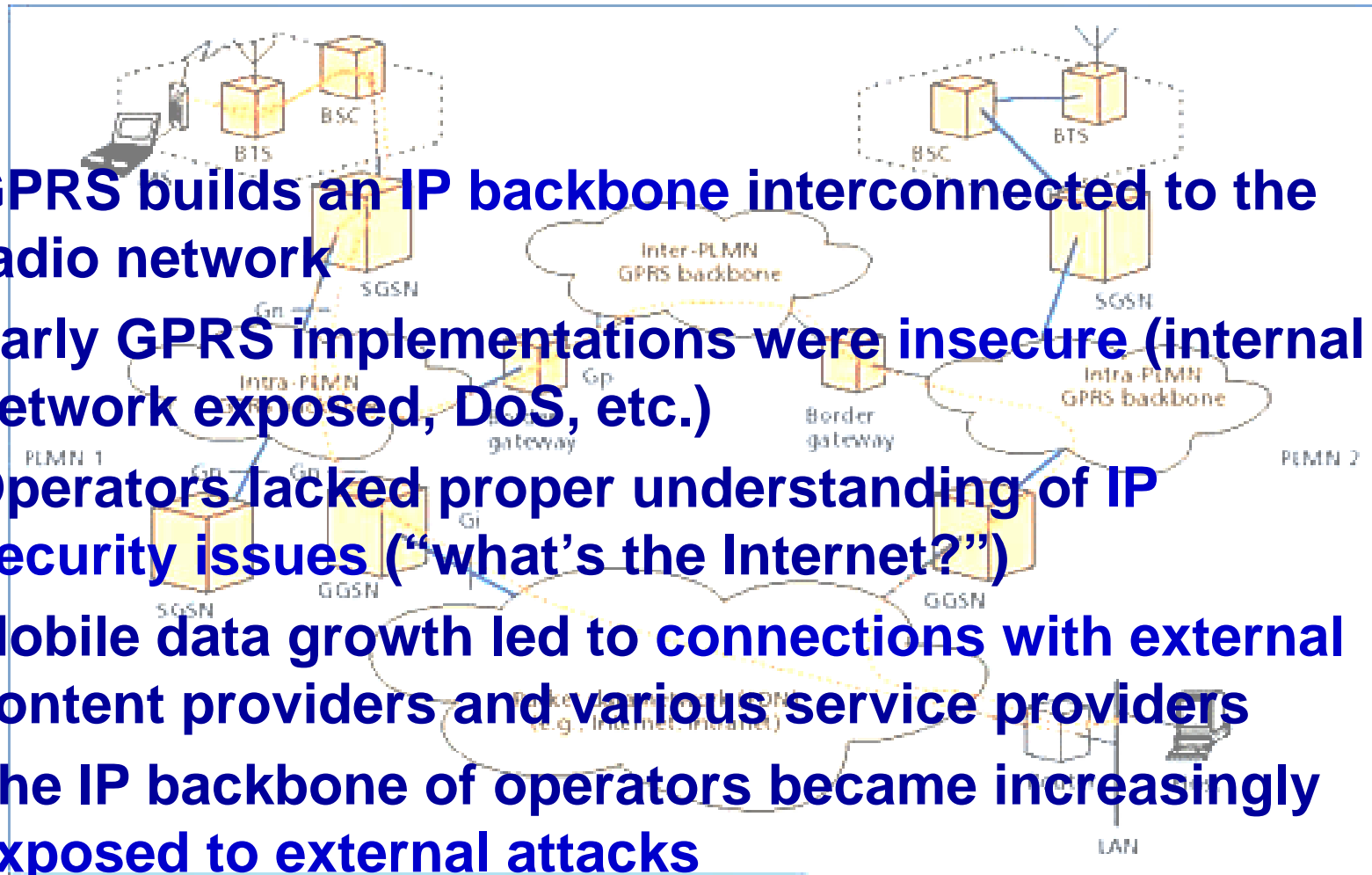
- **Designers of early systems had no considerations for security – just for functionality**
- **Phreakers were quick to learn how to abuse the system**
- **Countermeasures to limit the increasingly large fraud were only “band aid” that never really eradicated the problem**

Security issues in 2G

- ***Details in Emmanuel Gadaix's (TSTF.net) Black Hat presentation Asia 2001***
- **Eavesdropping and cloning foiled by use of encryption (no more scanners) and authentication (no more cloning).**
- **SIM cloning demonstrated due to weaknesses in crypto algorithms (A3/A5/A8) that were not submitted to peer review due to non disclosure.**

2.5G – an IP network overlay

- **GPRS builds an IP backbone interconnected to the radio network**
- **Early GPRS implementations were insecure (internal network exposed, DoS, etc.)**
- **Operators lacked proper understanding of IP security issues (“what’s the Internet?”)**
- **Mobile data growth led to connections with external content providers and various service providers**
- **The IP backbone of operators became increasingly exposed to external attacks**



Bluetooth



Bluetooth Security

- **Bluejacking** allows phone users to send business cards anonymously using Bluetooth. Bluejackers often look for the receiving phone to ping or the user to react. Sending and receiving devices must be within 10 meters of one another.
- **Bluesnarfing** allows hackers to gain access to data stored on a Bluetooth enabled phone without alerting the phone's user of the connection made to the device: phonebook and associated images, calendar, and IMEI. Without specialized equipment the hacker must be within a 10 meter range of the device while running a device with specialized software. Only specific older Bluetooth enabled phones are susceptible to bluesnarfing.
- **Bluebugging** allows access the mobile phone commands using Bluetooth without notifying or alerting the phone's user. This vulnerability allows the hacker to initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet. Discovered by Martin Herfurt.



TIP: presentazione su BT hacking di Dino Covotsos/TELSPACE ad HITB 2007

(<http://conference.hitb.org/hitbsecconf2007kl/materials/D2T2%20-%20Dino%20Covotsos%20-%20Hacking%20the%20Bluetooth%20Stack%20for%20Fun%20Fame%20and%20Profit.pdf>)

Wi-Fi e Wi-Max security evolution

- **Wi-Fi 802.11 a/b/g: c'è davvero bisogno di parlarne ? :(**
- **Wi-Max: i soliti problemi del wi-fi e dell'IT (vendor, default cfgs, protocolli “vergini”)**

TIP: Matteo G.P. “LastKnight” Flora ci fornirà un'attenta overview dell'attuale situazione wireless-security in Italia.

VoIP security evolution

- **VoIP (SIP, H.323). La situazione non è decisamente bella...**

TIP: Alessio L.R. “mayhem” Pennasilico ci parlerà della sicurezza in ambienti VoIP.

**TIP2: La presentazione di “The Grugq” ad Hack in the Box Malaysia 2006 su VoIPhreaking SIP Unveiled!
(<http://conference.hackinthebox.org/hitbsecconf2006kl/materials/DAY%202%20-%20The%20Grugq%20-%20VoIPhreaking%20-%20SIPhalis%20Unveiled.pdf>)**

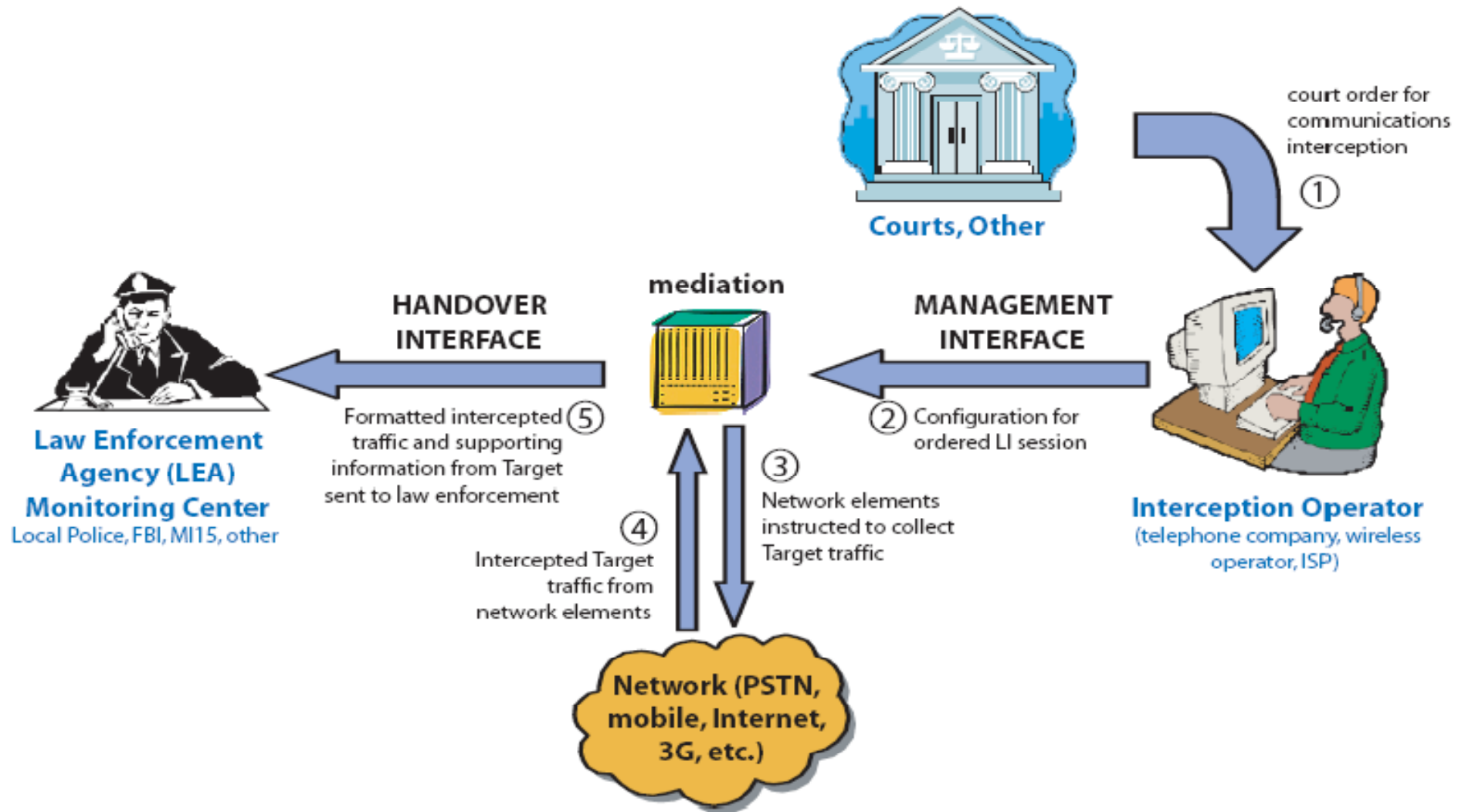
**(sezione aggiunta all'ultimo
minuto :)**

Lawful Interception

Definitions

- **Lawful interception (aka wiretapping) of telecommunications. Interception of telecommunications by law enforcement authorities (LEA's) and intelligence services, in accordance with local law and after following due process and receiving proper authorization from competent authorities.**
- **Various countries have different rules with regards to lawful interception. In the United States the law is known as CALEA, in CIS countries as SORM.**
- **With the PSTN, Lawful Interception (LI) is performed by applying a tap on the telephone line of the target in response to a warrant from a Law Enforcement Agency (LEA).**
- **However, VoIP technology has enabled the mobility of the end-user, so it is no longer possible to guarantee the interception of calls based on tapping a physical line.**
- **Whilst the detailed requirements for LI differ from one jurisdiction to another, the general requirements are the same. The LI system must provide transparent interception of specified traffic only, and the subject must not be aware of the interception. The service provided to other users must not be affected during interception.**

L.I.G. Concept



Entities involved in L.I.

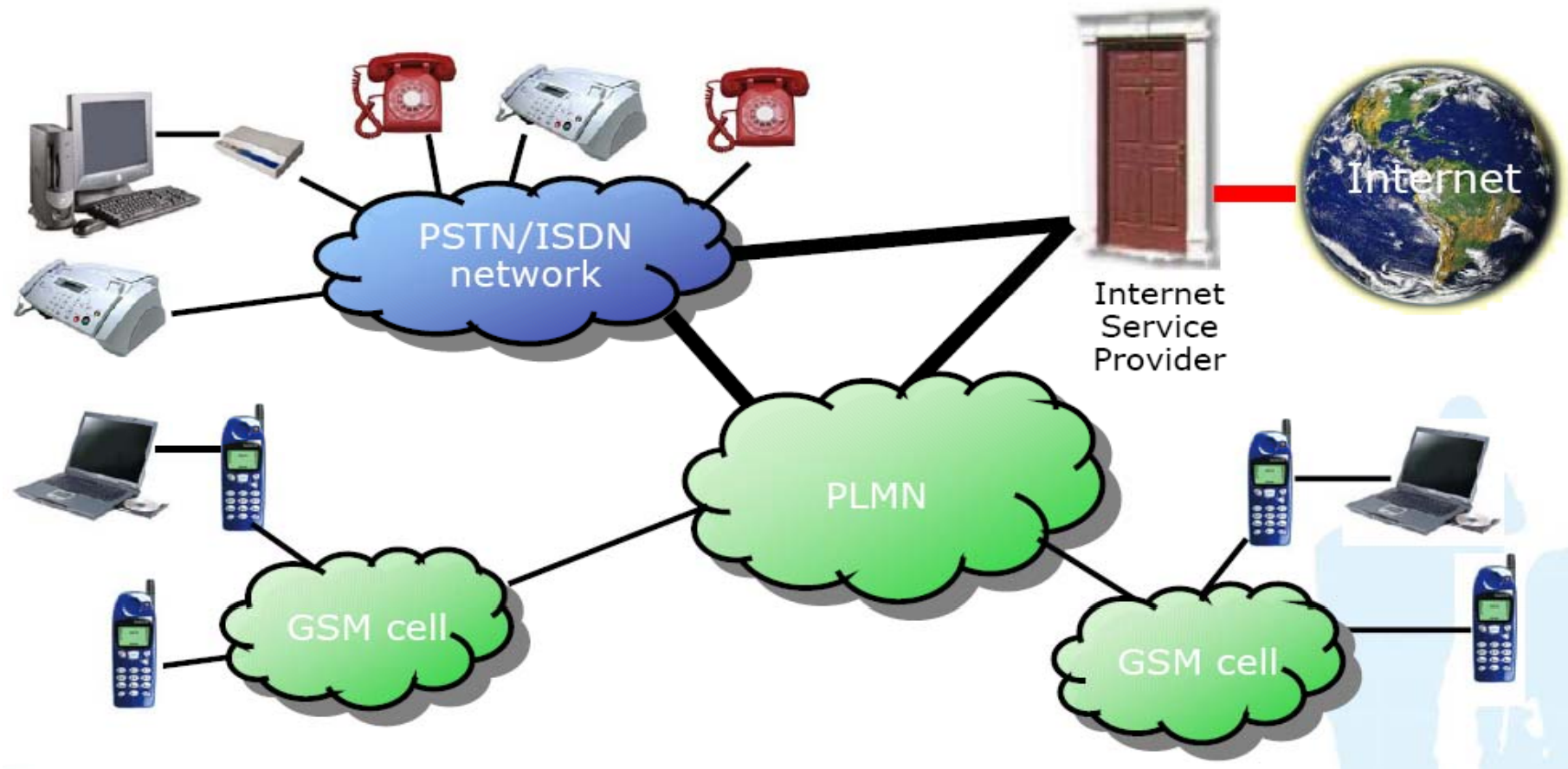
- **Governments**
 - Operates in the interests of the nation
 - Sets the regulatory framework in which Lawful Interception is performed
 - Defines economical parameters for Lawful Interception activities.
- **Operators**
 - Lawfully operate for the sake of their business and profit
 - Withstand rules set by the government in terms of lawful interception as unavoidable
 - Install proper devices to fulfil the relevant obligations
- **Law Enforcement Agencies**
 - Operate in the name of crime fighting and nation security
 - Request lawful interception and define the real targets
 - Receive the communication data extracted by the operators
 - Need proper devices to playback and decode the intercepted traffic

Early Interception

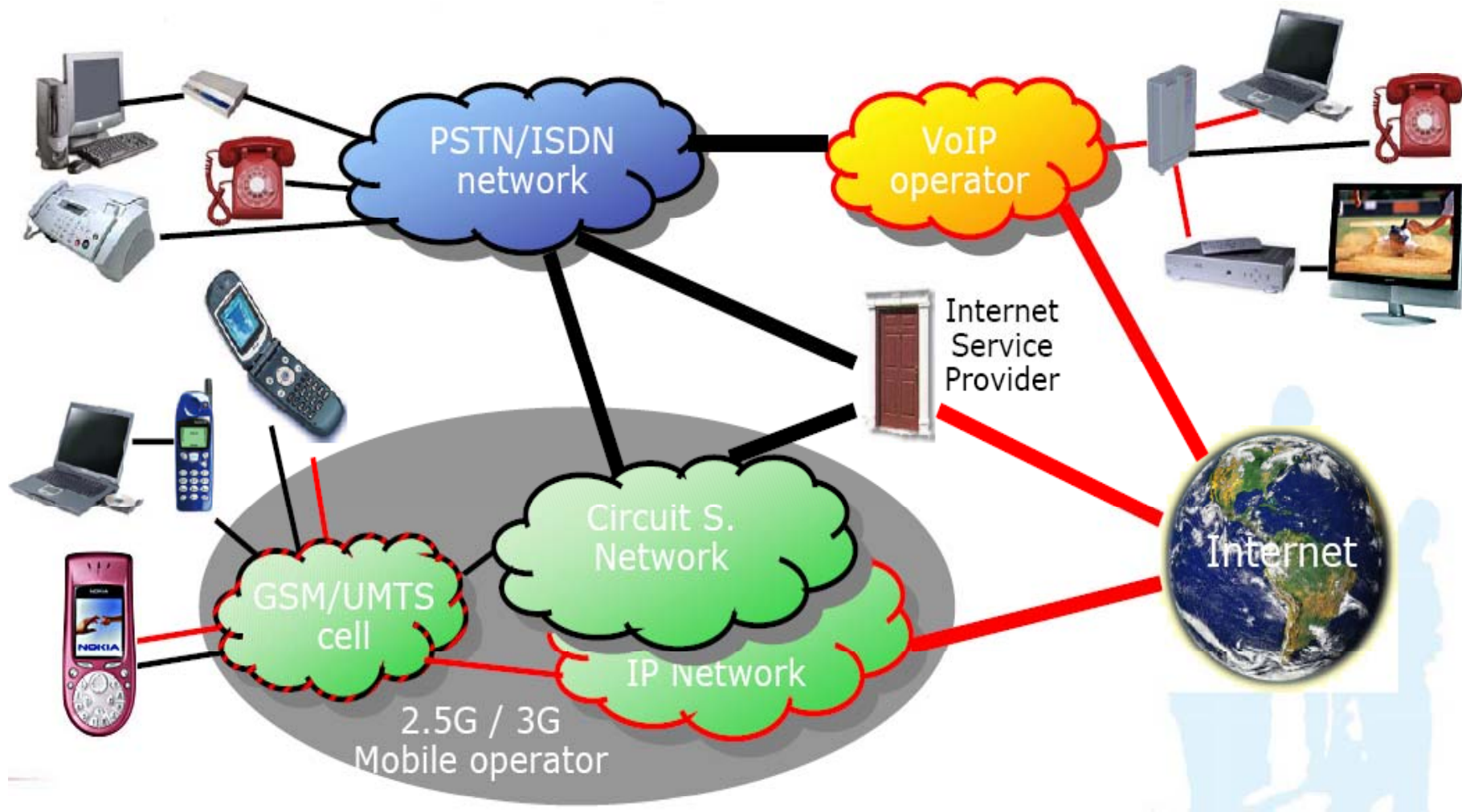
- The mass telecommunications were only bound to the fixed PSTN network
- No additional functionalities were provided by the handsets;
- The transport Network was unique in type and technology, it was based upon Circuit Switching, and the only type of payload transported was VOICE.
- Interception operated over a single network, with good-to-excellent results
- Single type of payload (typically ISDN voice over 64 kbps;
- Due to the circuit switching technology, may be operated in any point of the network between the end points.



Things start to get complicated...



...and turn into a L.I. nightmare !!!



L.I. challenges

- **A lot of mass telecommunication traffic today doesn't traverse any part of the well-controlled Circuit Switched network:**
 - IP multimedia traffic between GPRS/UMTS mobile phones
 - The traffic to and from Internet exchanged on high bandwidth ISPs (ADSL, FTTH, cable...)
 - Telephone traffic between two VoIP terminals, maybe connected to different VoIP operators.
- **Encrypted traffic without key escrow mechanisms**
- **Decentralized Peer to Peer networks**

L.I. & Vodafone Greece scandal

- Ho voluto aggiungere questa sezione perché l'abuso dei sistemi LIG/LIS rappresenta uno dei peggiori incubi ipotizzabili, sia dal punto di vista degli operatori che dell'utente finale (privacy: bye bye!)
- Ora, dopo aver visto queste slide, penso vi sarà più semplice leggere, comprendere ed apprezzare l'articolo "The Athens Affair", del quale consiglio vivamente la lettura a voi tutti:

<http://www.spectrum.ieee.org/jul07/5280/1>

Cosa ci riserva il prossimo futuro ?

What's coming up ?

- **Nel prossimo, immediato futuro, assisteremo a:**
 - **Aumento esponenziale del phishing, il quale si evolverà verso il c.d. “Vishing”, grazie alla fusione di tecniche di Social Engineering, Phishing e VoIP abusing;**
 - **Frodi telefoniche (“scams”) verso utenti finali fissi e mobili (smartphone, PDAs, xDSL+VOIP subscribers);**
 - **Attacchi di medio livello verso operatori di TLC (fisso e mobile) di piccole e medie dimensioni per vulnerabilità web-based;**
 - **Attacchi di medio ed alto livello verso operatori VoIP**
 - **Attacchi di alto livello verso operatori GSM e 3G (CDR, LIG/LIS, SMS, CN)**

Conclusioni

NGN: Next Generation Nightmares

- **3G/NGN/4G/IMS security issues will always be there.**
- **Technical security of NGN systems well designed but likely to suffer implementation problems**
- **Increased connectivity means the security exposure will become more serious and harder to manage**
- **Protocols such as SIP (e.g. in IMS model) likely to be abused by NGP (next generation phreakers)**
- **Business risk due to emergence of alternative technologies e.g. VoIP, Asterisk, SER, WiMAX, etc.**
- **Huge monolithic network operators likely to suffer in the highly competitive deregulated market**

Bibliografia e Riferimenti

Bibliografia / 1

Durante le diverse fasi di ricerca documentale per la stesura di questa presentazione, l'autore ha fatto riferimento (anche) alle seguenti pubblicazioni e risorse on-line:

- Questionari H.P.P. 2004/2005/2006/2007
- Stealing the Network: How to Own an Identity, (AA.VV), Syngress Publishing, 2006
- Stealing the Network: How to Own the Box, (AA.VV.), Syngress Publishing, 2003
- Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier, Suelette Dreyfus, Random House Australia, 1997
- The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Clifford Stoll, DoubleDay (1989), Pocket (2000)
- Masters of Deception: the Gang that Ruled Cyberspace, Michelle Stalalla e Joshua Quinttner, Harpercollins, 1995
- Kevin Poulsen, Serial Hacker, Jonathan Littman, Little & Brown, 1997
- Takedown: sulle tracce di Kevin Mitnick, John Markoff e Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996
- The Fugitive Game: online with Kevin Mitnick, Jonathan Littman, Little & Brown, 1997
- The Art of Deception, Kevin D. Mitnick e William L. Simon, Wiley, 2002
- The Art of Intrusion, Kevin D. Mitnick e William L. Simon, Wiley, 2004
- @ Large: the Strange Case of the World's Biggest Internet Invasion, Charles Mann & David Freedman, Touchstone, 1998
- The Hacker Diaries: Confessions of Teenage Hackers, Dan Verton, McGraw-Hill Osborne Media, 2002
- Cyberpunk: Outlaws and Hackers on the Computer Frontier, Katie Hafner, Simon & Schuster, 1995
- SecurityFocus.com (BugTraq, VulnDev), Mitre.org (CVE), Isec.com (OSSTMM), many "underground" web sites & mailing lists, private contacts & personal friendships, the Academy and Information Security worlds

Bibliografia / 2

Durante le diverse fasi di ricerca documentale per la stesura di questa presentazione, l'autore ha fatto riferimento (anche) alle seguenti pubblicazioni e risorse on-line:

- Emmanuel Gadaix from Telecom Security Task Force (TSTF), various security talks @ Black Hat, RuxCon, Hack in the Box, EUROSEC (2002-2006)
- Compendio di criminologia, Ponti G., Raffaello Cortina, 1991
- Criminalità da computer, Tiedemann K., in Trattato di criminologia, medicina criminologica e psichiatria forense, vol.X, Il cambiamento delle forme di criminalità e devianza, Ferracuti F. (a cura di), Giuffrè, 1988
- United Nations Manual on the Prevention and Control of Computer-related Crime, in International Review of Criminal Policy – Nos. 43 and 44
- Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale, Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001
- Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques, Turvey B., Knowledge Solutions Library, January, 1998
- Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology, Täterpro

Ringraziamenti

- **Telecom Security Task Force: Emmanuel Gadaix, Philippe Langlois, Stavroula Ventouri**
- **CLUSIT: Gigi Tagliapietra, Paolo e Giorgio Giudice, Claudio Telmon**
- **@ Mediaservice.net/Data Security Department staff: Ivan Verri, Marco Ivaldi, Maurizio Agazzini, Lorenzo Migliardi, Carlo Pelliccioni, Claudio Prono, Daniele Poma**
- **Chaos Computer Club (manu, starbug, Lisa, many others)**
- **Hack in the Box – Dhillon, Amy, HITB crew**
- **Mixed: BellUA - Anthony Zboralski, Jim Geovedi; Dino Cosvotos at TelSpace South Africa; The Grugq**
- **The “underground”**

Aderire al CLUSIT

Per ulteriori informazioni, per aderire al
CLUSIT e partecipare alle sue attività:

www.clusit.it

e-mail: info@clusit.it

Grazie per l'attenzione!

Contatti, Q&A

DOMANDE ?

Se invece siete "*troppo timidi*" per farmi domande ora, o volete affrontare tematiche particolari, i miei riferimenti sono:

www.mediaservice.net

www.TSTF.net

rchiesa@CLUSIT.it

rc@TSTF.net