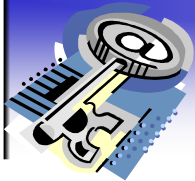


La Sicurezza Informatica

Minacce e vulnerabilità delle Reti WireLess

**Sistemi WI-FI per Radioamatori
Aspetti Legali**

**7° MEETING ARI FIDENZA
29 MARZO 2009**



Chi vi parla?

Nome : Sergio Giuffrida Call: IZ3CNM

Nato a: Verona (ma vissuto a Catania dai 6 ai 19 anni!)

Attuale domicilio: Marcon(Venezia) dal 1984

Stato Civile: Coniugato (+due figli)

Professione: Formatore I.C.T. nella Pubblica
Amministrazione quale addetto al
Centro Addestramento Regionale G. di F. Veneto.

Radioamatore dal 1989 (nominativo IW3HCL)

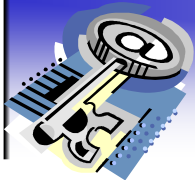
In A.R.I.: dal 1988 al 2001 e dal 1 luglio 2008 al ???

eMail: iz3cnm@tin.it

Cell: 328-0468150

IZ3CNM

Sezione A.R.I. Chioggia-Sottomarina (VE)



Cosa è una violazione

- **Formale**

(violazione di una norma,
prescrizione, Legge)

- **Regole Comuni**

(costumi, consuetudini,
regole civile convivenza)



Perché una persona commette un crimine?

- Non conosce la norma**
- E' sicuro di non essere scoperto**
- Non conosce i danni conseguenti**
- Non valuta la reazione da parte della vittima**
- Stima (o meglio sottostima) le conseguenze penali e sociali**



In base a cosa avviene un crimine?

Criminologia Classica (Marco Strano)

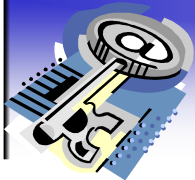
- Vissuto**
- Personalità**
- Socializzazione**
- Genetica (Cesare Lombroso)**
- Apprendimento (livello culturale)**



Quali sono i “Computer Crimes”?

“Nullum crimen, nulla poena sine lege”

- frode informatica,
- falso informatico,
- danneggiamento dei dati e dei programmi informatici,
- sabotaggio informatico,
- **accesso non autorizzato,**
- riproduzione non autorizzata di un programma informatico protetto



Computer Crimes

Violazione dei segreti

Nell'art. 616 del codice penale, il quarto comma recita:

*"Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica **ovvero effettuata con ogni altra forma di comunicazione a distanza**".*



Computer Crimes

Violazione dei segreti

"Art. 617-quater. - (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche). - Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

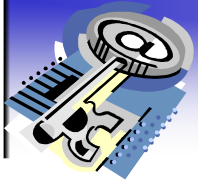
Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo d'informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma...



Computer Crimes

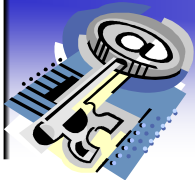
Violazione dei segreti

Art. 617-quinquies. - *(Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche) .- Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma*



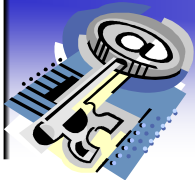
Conseguenze dell'introduzione dei crimini informatici

- Consapevolezza del diritto
- Nuove responsabilità?
 - Assicurare la legittimità del diritto
 - Amministrazione di sistema:
 - Prevenzione o Violazione?
 - Condotta omissiva (Art. 40 c.p.)
 - Culpa in eligendo
 - Culpa in vigilando



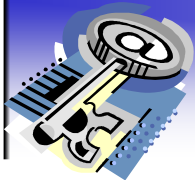
Misure di sicurezza Logica

- Controllo degli accessi alle informazioni
- Sistemi di controllo e mantenimento dell'integrità
- Sicurezza delle trasmissioni
- Protezione degli elaboratori, del software, delle licenze, degli accessi alle reti
- Sicurezza nel processo di sviluppo software, dell'installazione, della configurazione
- Sicurezza dei sistemi di rilevazione e trattamento degli incidenti



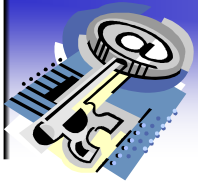
Il Crimine Informatico in Italia

- La legislazione Italiana, dal 1993, ha introdotto tutta una serie di dispositivi che contemplano il crimine cosiddetto informatico.
- L'approccio iniziale è stato di tipo evolutivo, ovvero si è basato sulla modifica di leggi esistenti ricollegando reati "tradizionali" ai nuovi possibili basati su, o condotti contro, strumenti informatici



Reati Penali

- Nel 1993 sono state prodotte le modificazioni al Codice Penale ed al Codice di Procedura Penale relativamente al reato informatico (legge 23 dicembre 1993 n. 547)
- Con le modificazioni, sono stati individuati un certo numero di reati che possono essere apportati contro o mediante strumenti tecnologici informatici



Reati Penali

- Perché reati penali?
 - Agevolare la cooperazione internazionale allineando la normativa italiana a quelle degli altri paesi europei, anch'esse di tipo penale
 - Aderire alla Raccomandazione CEE n. 89/9 del Comitato per i problemi criminali del Consiglio d'Europa
 - Mantenere un approccio "evolutivo" della normativa in merito ai Computer Crimes



Reati introdotti dalla L.23/12/93 n.547

- Tipologie di reati:
 - Esercizio arbitrario delle proprie ragioni con violenza sulle cose
 - Delitti contro l'ordine pubblico
 - Falsificazione di documenti informatici
 - **Accesso abusivo ad un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso, diffusione di programmi diretti a danneggiare od interrompere un sistema informatico;**
 - Violazione dei segreti
 - Delitti contro il patrimonio.



Accesso abusivo a un sistema informatico o telematico (art.615 ter)

- *1. Dopo l'articolo 615-bis del codice penale sono inseriti i seguenti:
"Art. 615-ter. - (Accesso abusivo a un sistema informatico o telematico). - **Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza** ovvero vi si mantiene contro la volontà **espressa o tacita** di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
(...)*



Leggi e Regolamenti per i RadioAmatori



Codice delle Comunicazioni

- Decreto legislativo
1 agosto 2003 nr.259

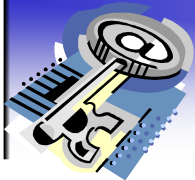
Capo VII° - Radioamatori Art. 134-
144

Allegato 26 - Normativa Tecnica



Codice delle Comunicazioni

- Art. 12, comma 4 – Allegato 26
- “ E' consentita l'interconnessione delle stazioni di radioamatore con le reti pubbliche di comunicazione elettronica per motivi esclusivi di emergenza o di conseguimento delle finalita' proprie dell'attivita' di radioamatore”

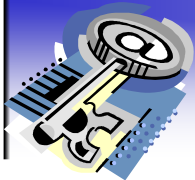


Frequenze di esercizio



Frequenze di esercizio Piano Nazionale di Ripartizione delle Frequenze Decreto 8 luglio 2002

2300-2440	radioamatore	secondario
2440-2450	satellite	secondario
5650-5670	satellite	secondario
5760-5770	satellite	primario
5830-5850	satellite	secondario



Frequenze utilizzabili

Banda 2400

Ch. 1, 2, 3, 2412-2422 MHz

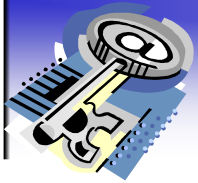
Ch. 4, 5, 6, 2427-2437 MHz

Ch. 7, 8 2442-2447 MHz

Ch. 9, 10, 11 2452-2462 MHz

Ch. 12, 13, 14 2467-2484 MHz

(in rosso le frequenze destinate al servizio satellite)



Progetto di Rete

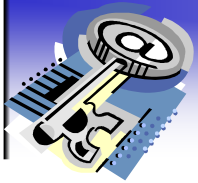
- Scelta del Canale

(Evitare l'interferenza con il servizio satellitare)

- Canali disponibili

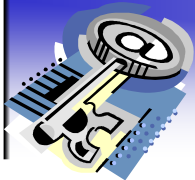
(canali da 1 a 6 degli Access Point)

(Ricordiamo che il canale 6 degli AP e' uno standard!)



Progetto di Rete

- Potenza
(Adeguate ai sistemi RX/Tx)
- Antenne
(Parabole e/o Pannelli)



Frequenze di esercizio

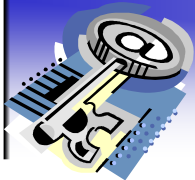
Banda 5600 MHz

5650 – 5670 MHz

5760 – 5775 MHz

5830 – 5850 MHz

(in rosso le frequenze destinate al servizio satellite)



Potenze di esercizio

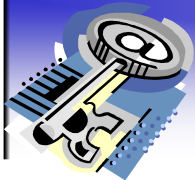
Allegato 26 – Art. 15

“Fatte salve eventuali limitazioni delle potenze riportate dal Piano di ripartizione delle frequenze, le stazioni di Radioamatore possono operare con le seguenti potenze massime:

Classe A*, Fisso o Mobile/portatile: 500
Watt

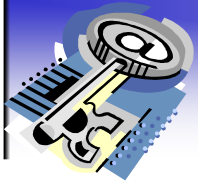
Classe B*, Fisso o Mobile/portatile: 50
Watt

*(adesso classe unica)



Potenze di esercizio

- Stazioni automatiche non presidiate installate fuori dal domicilio
- Art. 10, comma 9, Allegato 26
- “La massima potenza equivalente irradiata (erp) non deve essere superiore a 10 Watt”



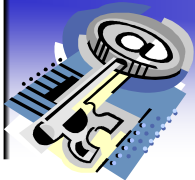
Potenze di esercizio: Lo standard USA

Banda 5600 MHz

5150 – 5350 MHz 200mW indoor

5470 – 5725 MHz 1W in/outdoor

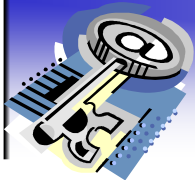
5725 – 5875 MHz 25 mW



Potenze di esercizio

- Art. 10, Allegato 26

Per le stazioni automatiche non presidiate installate fuori dal domicilio, e' necessaria apposita autorizzazione generale, previa presentazione di scheda tecnica



Legislazione

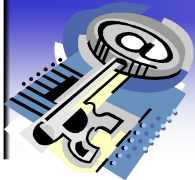
- Fino al 2001 il riferimento legislativo per l'utilizzo delle apparecchiature operanti nelle bande di frequenza da comunemente dette a banda 2.4 GHz e a banda 5 GHz, utilizzate per la trasmissione wireless LAN, era dato dal DPR 447 del 5 Ottobre 2001.

IZ3CNM Sergio Giuffrida
A.R.I. Chioggia - Sottomarina (VE)



Legislazione

- Il decreto stabiliva che tali frequenze potessero essere impiegate solo nell'ambito di LAN ad uso privato, mentre per connettere una WLAN alla rete pubblica occorreva un'autorizzazione generale del Ministero nonché il pagamento di un canone.



Legislazione

- A partire dal gennaio 2002, il regolamento di attuazione dello stesso DPR 447 del 5 Ottobre 2001 consente l'utilizzo di dispositivi di WLAN che operano sulle bande di frequenza appositamente assegnate, senza più la necessità di richiedere alcuna concessione.



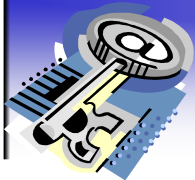
Legislazione

- Il quadro regolamentare definitivo per l'utilizzo della tecnologia Wi-Fi in ambito pubblico è dato però dal cosiddetto decreto Gasparri del 28 Maggio 2003, che regola le condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso Radio-LAN alle reti ed ai servizi di telecomunicazioni.



Legislazione

- La delibera dell'Autorità per le Garanzie nelle Comunicazioni (num. 102/03/CONS) precisa che non è necessario disporre di licenza o autorizzazione per l'erogazione di servizi di connettività di rete nel caso l'attività commerciale non abbia come oggetto sociale principale l'attività di telecomunicazioni (es. bar, alberghi, centri commerciali).



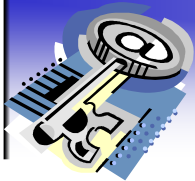
IL DECRETO LANDOLFI

- Il decreto del Ministero delle Comunicazioni liberalizza l'erogazione di servizi Wi-Fi nel territorio nazionale, modificando il precedente decreto Gasparri 28 Maggio 2003.
- L'articolo 1 liberalizza il servizio su tutto il territorio nazionale, eliminando l'obbligo di fornire il servizio in aree a frequentazione pubblica o locali aperti al pubblico.
Inoltre l'articolo 4, riprendendo il decreto legislativo 1° agosto 2003 n. 259, mantiene il regime di autorizzazione generale per i soggetti che vogliono fornire servizi radiolan. Tale autorizzazione è da richiedere alla Direzione generale per i servizi di comunicazione elettronica e radiodiffusione del Ministero delle Comunicazioni.



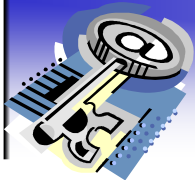
Decreto Legge 27 luglio 2005, n.144

- **Le complicazioni del Decreto Pisanu**
- Con il decreto "*Misure urgenti per il contrasto del terrorismo internazionale*", noto come decreto Pisanu, del 27 luglio 2005, alcune delle norme citate precedentemente sono state variate.
- L'articolo 7, infatti, invalida la delibera dell'Autorità per le Garanzie nelle Comunicazioni (num. 102/03/CONS) precedentemente citata, indicando che è necessario richiedere un'autorizzazione al questore per chi mette a disposizione terminali telematici. L'autorizzazione va richiesta per chi ne fa attività prevalente o esclusiva, o per chi ha più di 3 terminali installati. Inoltre richiede la "*preventiva acquisizione di dati anagrafici riportati su un documento di identità dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando **tecnologia senza fili***".



Legislazione

- I limiti di potenza, secondo le norme ETSI attuali, per i servizi radioWlan sono stabiliti in 100 mW per la banda a 2.4 GHz e 1 W per la banda a 5 GHz.



Conclusioni

- Appare quindi evidente che nella normativa attuale non sussistono necessità di richiesta di autorizzazione nè per uso privato, nè per uso professionale all'interno di uffici o tra differenti uffici appartenenti alla stessa società, a patto che l'accesso non sia pubblico.
- In caso di fornitura di accesso al pubblico è sempre e comunque necessaria una preventiva autorizzazione.



Proposta

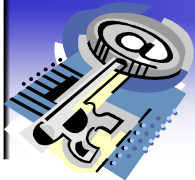
- Sviluppo verso l'uso della banda dei 5600 MHz

IZ3CNM Sergio Giuffrida
A.R.I. Chioggia - Sottomarina (VE)



Perche' i 5600 MHz ?

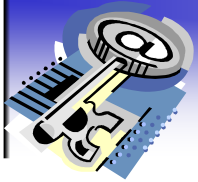
- Forte congestione della banda dei 2400 MHz
- Maggiore potenza (norme nazionali)
- Minore criticita' nel collegamento radio
- Statuto primario



Cosa si dice del WI-FI?

- ***"La connessione web senza cavi ad alta velocità non sarà in concorrenza con la futura offerta UMTS"*** è l'opinione del Dott. R.Ruggero, A.D. di Telecom Italia, Domestic Wireline.

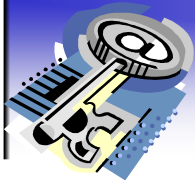
"Il Wi-Fi è una tecnologia interessante, la stiamo sperimentando", dichiarazione di V.Colao, A.D. di Vodafone Omnitel, indicano un netto interesse verso la tecnologia 802.11b anche da parte degli operatori radiomobili, che, inizialmente, apparivano molto scettici, diffidenti, quasi osteggiatori.



Wardriving

La nuova tendenza del wi-fi

- Complice i problemi di sicurezza dello standard 802.11b per le reti wireless è nato negli Stati Uniti il fenomeno di '**wardriving**'. Esso consiste nell'appostarsi nei pressi di un punto di accesso WI-FI e condividere la rete WIRELESS - a radiofrequenza-, per navigare ad alta velocità senza alcuna spesa.
Se l'accesso avviene a piedi, si parla di warwalking.



Wardriving

Cosa dice WikiPedia?

- *""""Il **wardriving** è un'attività che consiste nell'intercettare reti [Wi-Fi](#), in automobile o a piedi con un [laptop](#), solitamente abbinato ad un ricevitore [GPS](#) per individuare l'esatta locazione della rete trovata ed eventualmente pubblicarne le [coordinate geografiche](#) su un [sito web](#). Per una miglior ricezione vengono usate antenne omnidirezionali. È necessario utilizzare un [software](#) specifico, quasi sempre di tipo libero, per diverse piattaforme: [NetStumbler](#) ([Windows](#)), [KisMac](#) ([Macintosh](#)), [Kismet](#) ([GNU/Linux](#)) e [Ministumbler](#) ([PocketPC](#)).""""*

(Fonte WikiPedia.org)



Wardriving

La nuova tendenza del wi-fi

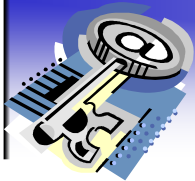
- Wardriving in realtà è l'unione di una sigla *WAR* (Wireless Access Revolution) e *DRIVING* ovvero guidando l'automobile.



Wardriving

La nuova tendenza del wi-fi (2)

- *Il wardriving in sé consiste nel trovare Access Point (AP) e registrarne la posizione. Alcune persone, invece, infrangono le scarse misure di sicurezza tipiche di queste reti per accedere ai file personali e magari distruggerli. Poiché nella maggior parte dei casi le reti wireless sono collegate ad [Internet](#), molte persone si introducono in queste reti solamente per navigare gratis e ad alta velocità.*



Wardriving

La nuova tendenza del wi-fi

- **Le Mappe del Wardriving** (<http://wireless.iport.it/mappe.html>)
- [SDV W-lan](#)
- [WorldWide WarDrive](#)
- [WiFiMaps](#)
- [ZDNet UK's Wifi Map](#)
- [THE PARISIAN ACCESS POINT WIFI MAP](#)
- [WIFI zone](#)
- [Free W-Fi From your iPod](#)
- [802.11 Devices](#)
- [Google Secure Access](#)
- [Free Hotspots in the United States](#)
- [Wi-Fi-FreeSpot Directory](#)
- [Geek Hotspots](#)
- [Geek Hotels](#)
- [Send a Wi-Fi Thank You](#)
- [Add Jwire Hotspot Search](#)
- [Mac OS X Jwire Widget](#)
- [WiGLE.net](#)
- [WiFiMaps.com](#)
- [Plazes](#)
- [Free Hotspots in Southern California](#)
- [Wi-Fi Alliance](#)
- [Yahoo Maps](#)
- [Security in Public Spaces](#)
- [Public Hotspot Security](#)
- [Make your car a Wi-Fi hotspot](#)
- [FreeFi](#)



Clicca per zoom



Clicca per zoom



Clicca per zoom



Clicca per zoom



Clicca per zoom



Clicca per zoom

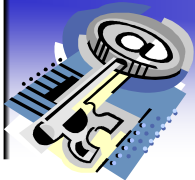


Wardriving

La nuova tendenza del wi-fi

- **I risultati...**

Effettuando un tour abbastanza breve, di circa un'ora, i nostri eroi hanno individuato **18 reti**, di cui **12 senza "protezione"** e **solo 6** con il protocollo di sicurezza attivato...



Wardriving

!!! ATTENZIONE !!!

- Andando a ragionare oltre la moda e l'esaltazione del momento c'è da interrogarsi sulle problematiche legali del wardriving che è **tutt'altro che l'innocente azione di "scroccare" la connessione a Internet del vicino e implica la violazione di più leggi.**

In particolare segnaliamo:

Art 617-quater c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Art 617-quinquies c.p. - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Art 615-ter c.p. - Accesso abusivo a un sistema informatico o telematico

Le rilevazioni effettuate e riportate non devono quindi indurre a fraintendimenti: **il wardriving è un'attività illegale.**



Proposta

- Sviluppo della sicurezza e autenticazione del Radioamatore



Autenticazione del radioamatore

La nostra rete
radioamatoriale deve
necessariamente garantire
l'accesso e l'uso solo da
parte di persone in
possesso di autorizzazione
generale



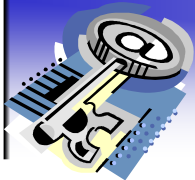
Autenticazione del radioamatore

- Proposta:
Presentazione delle credenziali per ottenere la determinazione da parte dell'Autorità per il rilascio del Certificato di Firma Digitale per i Radioamatori



Autenticazione del radioamatore

- Non dimentichiamo che il nostro Paese e' stato il primo Paese Europeo (e forse al mondo!) ad aver adottato una Legge sulla Firma Digitale:
- LEGGE NR. 59 DEL 1997
- REGOLAMENTO DPR 513 DEL 1997



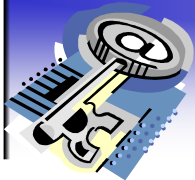
WiMAX ?

- *WiMAX è una tecnologia di rete di area metropolitana (MAN) senza fili che fornirà un'estensione wireless alle connessioni via cavo e xDSL per l'accesso in banda larga del cosiddetto ultimo miglio. Consente la connettività per gli utenti a una stazione base (base station).*
- *Le prime 2 fasi di attivazione del progetto, in Italia, prevedono la realizzazione di collegamenti punto-punto, per servire aree non raggiungibili in altro modo dal collegamento a banda larga o più semplicemente per utilizzare un mezzo trasmissivo alternativo al rame e alla fibra. In questo periodo l'utente finale non avrà quindi alcuna interazione con il sistema WiMAX, accederà alla rete utilizzando le attuali tecnologie ed eventualmente un collegamento Wi-Fi.*



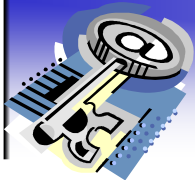
WiMAX ?

- WiMAX non si pone in conflitto con Wi-Fi ma ne costituisce il complemento.



WiMAX ?

- *La tecnologia supporta **velocità di trasmissione di dati condivisi** fino a 70 Mbit/s. Secondo i proponenti di WiMAX questa ampiezza di banda è sufficiente per supportare simultaneamente almeno 40 aziende con connettività di tipo T1 e 70 abitazioni con connettività al livello DSL da 1 Mbit/s.*



WiMAX...ci può interessare?

Le caratteristiche principali del documento approvato dall'IEEE sono le seguenti:

- Frequenze radio utilizzate che coprono le bande dei 2,3 GHz, 2,5 GHz, 3,3 GHz, 3,5 GHz e 5,8 GHz.
- Modalità di modulazione con accesso multiplo in OFDM, che suddivide lo spazio di frequenze disponibili in diversi gruppi di portanti con sottocanali e riduce le interferenze per i terminali con antenna omnidirezionale (tipicamente i terminali mobili).
- Scalabilità dell'occupazione dei canali sulla base della disponibilità di banda.
- Supporto di antenne adattative, ossia con la focalizzazione in ricezione e trasmissione effettuate "formando" il fascio radio con mezzi non meccanici ma elettronici.
- Miglioramento nella gestione dell'hand-over, ossia il passaggio di un terminale da una stazione base a un'altra senza perdita di connessione.
- Gestione del roaming, ossia la possibilità per un abbonato di un gestore di connettersi tramite un altro gestore.
- *Al momento WiMAX è una tecnologia in corso di "sperimentazione" in [Italia](#), dove è utilizzata unicamente alla frequenza di 3,5 GHz (Giga Hertz)?????????.*



La novità...

- Il Garante della Privacy, con provvedimento del 14 gennaio 2009 ha stabilito che agli *"amministratori di sistemi spetta il compito di vigilare sul corretto uso dei sistemi informatici"* ivi inclusi quelli wireless...



Novità....

- Necessita quindi che la rete wifi A.R.I. abbia uno o più amministratori con responsabilità non solo tecniche....
- Domanda...
A chi tocca questa patata bollente?



Istruzioni per l'uso

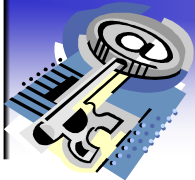
- **FARSI AIUTARE.** Chi ha un problema, spesso si vergogna, teme di essere catalogato come una persona stupida. Ma non è così: lo stesso problema è già capitato a tanti. Quando non si conosce qualcosa bisogna chiedere aiuto. Nessuno ce la fa da solo.



Conclusioni

- **NON DIMENTICHIAMO CHE IL RADIOAMATORE E', PRIMA DI TUTTO, UNO SPERIMENTATORE !!!**

"THE TRUE METHOD OF KNOWLEDGE IS THE EXPERIMENT" (WILLIAM BLAKE, 1788)



La Sicurezza Informatica

Minacce e vulnerabilità delle Reti WireLess

Sistemi WI-FI per Radioamatori

Aspetti Legali

7° MEETING ARI FIDENZA

29 MARZO 2009

Grazie!

IZ3CNM SERGIO

eMail: iz3cnm@tin.it

Cell: 328-0468150