Scusa, ti ho bucato per sbaglio

Wireless [in]security

Guido Bolognesi

Network Security Manager

guido@kill-9.it

I.Net S.p.A.

Sommario

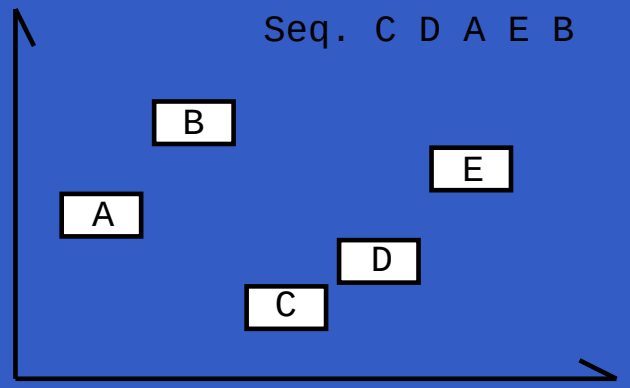
Le reti wireless attualmente diffuse hanno grossi problemi di sicurezza.
In molti casi è possibile penetrare all'interno di queste reti addirittura in modo inconsapevole, magari a causa di un sistema operativo troppo zelante...

Nelle prossime slide cercheremo di capire come e perchè.

Il “vecchio” 802.11b

Utilizza segnali radio nella banda dei 2.4GHz

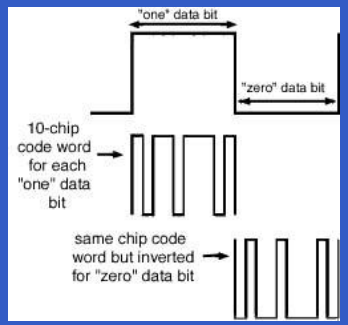
- 1 o 2 Mbit/s
- Usa 23 canali
- Richiede un rapporto S/N di 18dB
- Modulato in FHSS, *Frequency Hopping Spread Spectrum*...



Il “vecchio” 802.11b

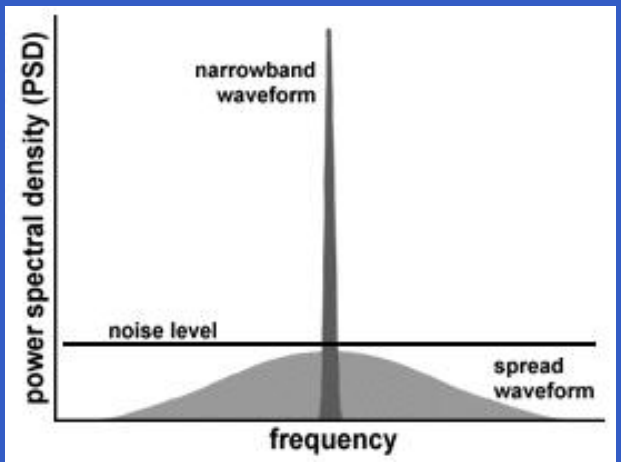
Utilizza segnali radio nella banda dei 2.4GHz

- 1 o 2 Mbit/s
- Usa 23 canali
- Richiede un rapporto S/N di 18dB
- ... o in DSSS con CCK *Complementary Code Keying*



L’ 802.11b “contemporaneo”

- 5.5 o 11 Mbit/s
- usa 11/14 canali sovrapposti
- Richiede un rapporto S/N di 12dB
- Modulato in HR-DSSS, *High Rate Direct Sequence Spread Spectrum*



Come è fatto 802.11b (cont.)

- Uno spreading code comune a sender e receiver
- CSMA/CA *(Carrier Sense Multiple Access, Collision Avoidance)*: al contrario di Ethernet 802.3, *prevede* quando è probabile che avvenga una collisione ed evita di trasmettere

802.11a, il futuro

- 5GHz, con 300MHz di “spazio di segnalazione”
- 50mW max (ricordiamo $d_{(P,F)} = \frac{PF}{d} = k$)
- OFDM *Orthogonal Frequency Division Multiplexing*
- Fino a 54 Mbit/s (38 reali)
- Problemi di standardizzazione in Europa: TPC *(Transmit Power Control)* e DFS *(Dynamic Frequency Selection)* nella banda dei 5GHz

Perchè è interessante?

- La strumentazione costa abbastanza poco
- È compatibile con moltissimi device
- In Europa è ancora in diffusione
- La legislazione è ancora abbastanza indietro (art. 615 *ter* c.p.)
- Ci sono vulnerabilità algoritmiche insite nel WEP
- Molte reti non utilizzano nessun tipo di autenticazione
- Non c'è confinamento fisico

Sistemi di autenticazione

Wi-fi è una radio, quindi se c'è chi trasmette, c'è chi ascolta...

Nessuno: c'è anche questo :)

WEP: *Wired Equivalent Privacy*,

EAP: *Extensible Authentication Protocol*, (RFC2284) ed

EAP-TLS: *EAP-Transport Level Security*, (RFC2716)

LEAP: *Lightweight EAP*, proprietario Cisco – fondamentalmente radius over EAP.

Autenticazione: nessuna

- Nessun controllo sul client
- Spesso un server dhcp assegna automaticamente un indirizzo valido per la rete
- Sono molto diffuse, non solo in Italia: dis.org
  - 60% nella configurazione di default
  - 85% non utilizzano wep
  - 7% usano WEP... nella configurazione di default

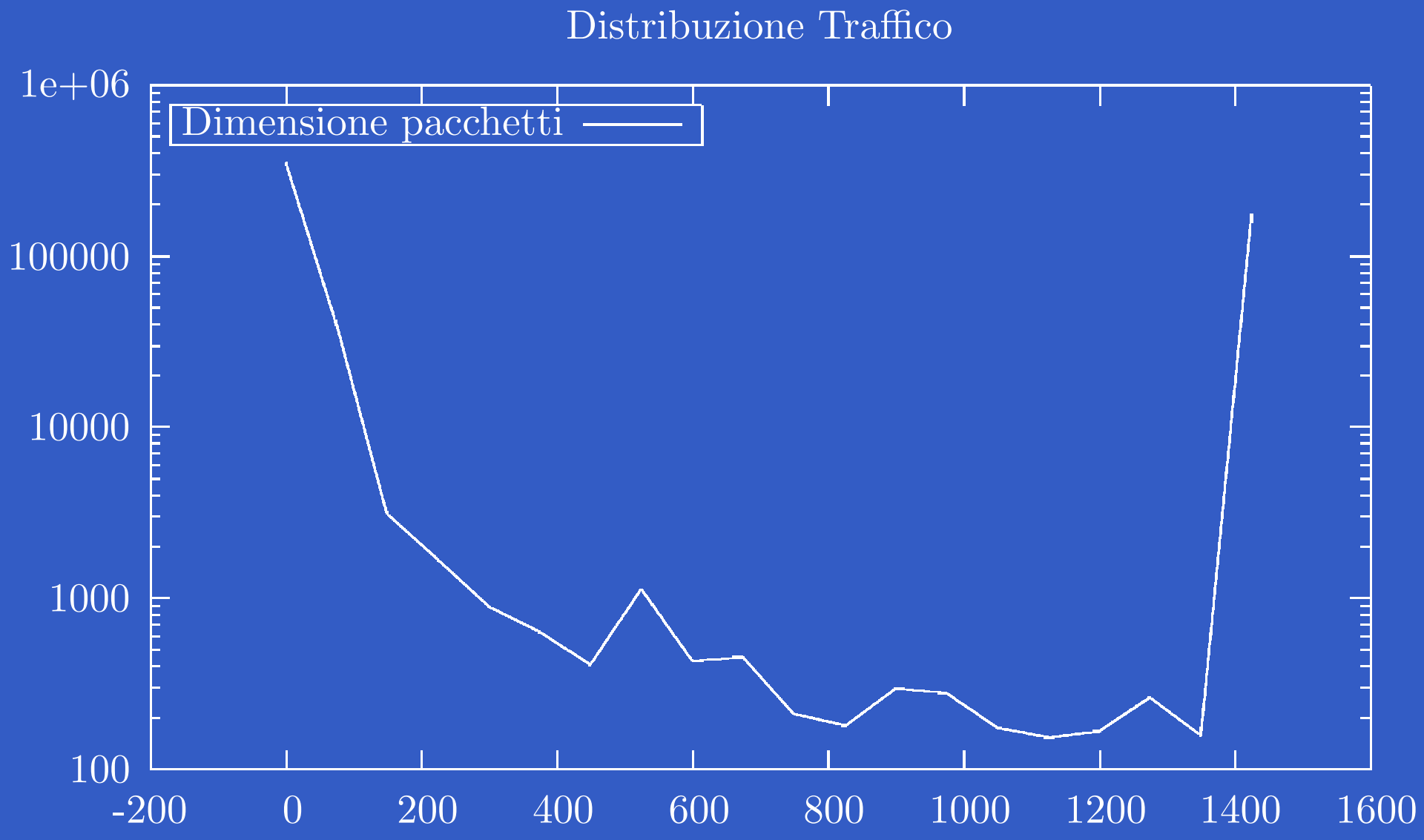
Autenticazione: WEP

- Si basa su una preshared secret K, da 40 o 104 bit (128) e un Initialization Vector IV da 24bit
- Il pacchetto cifrato C viene generato in questo modo:

$$keystream_{[RC4]}(IV, K) \oplus$$
$$(Plaintext + IntegrityCheck_{[CRC32]}) \rightarrow C$$

- Si ricorda che RC4 è uno *stream cypher*, e quindi la perdita di un solo bit invalida lo stream

Distribuzione Traffico



Autenticazione: WEP (2)

- Nella peggiore delle ipotesi:

$$\frac{1500byte}{11Mbps} \cdot 24bit = \frac{1500bit \cdot 8}{(11bit \cdot 10^6) \cdot sec^{-1}} \cdot 2^{24} = \tilde{}18000\ sec$$

  ovvero 5 ore
- IV passa in chiaro verso il ricevente
- Mediamente, la probabilità di riutilizzo della chiave è il 50% dopo 5000 pacchetti
- 40bit: bruteforce. basta confidare nel riutilizzo del keystream

Autenticazione: WEP (3)

- WEP suggerisce un IV diverso, ma non è detto che l'implementazione lo onori
- byte flipping sullo XOR? :)
- AP con e senza WEP: il pacchetto in chiaro passa anche in cifra
- Driver fallati: stesso IV ad ogni tempo t_0 (Lucent)

Autenticazione: EAP

- È un'estensione di PPP
- Permette di autenticare l'utente su un server esterno (Radius, ma anche Kerberos, OTP, Smart Card)
- Può essere utilizzato per autenticare, ma non per lo scambio di chiavi
- EAP-TLS, EAP-SRP, EAP-GSS, EAP-AKA sono estensioni ad EAP che permettono anche di ottenere chiavi da riutilizzare per altre suite di cifratura

Autenticazione: LEAP

- Creato da Cisco per contrastare i problemi di WEP
- Permette un’autenticazione reciproca Client-Network (Radius Cisco ACS)
- Permette la derivazione delle chiavi
- Usa chiavi WEP dinamiche, un Init Vector diverso per ogni pacchetto...
- ...ma funziona *solo con apparati Cisco*
- ...comunque c’è una patch per ethereal (incorporata nella 0.9.3)

Strumenti e tecniche

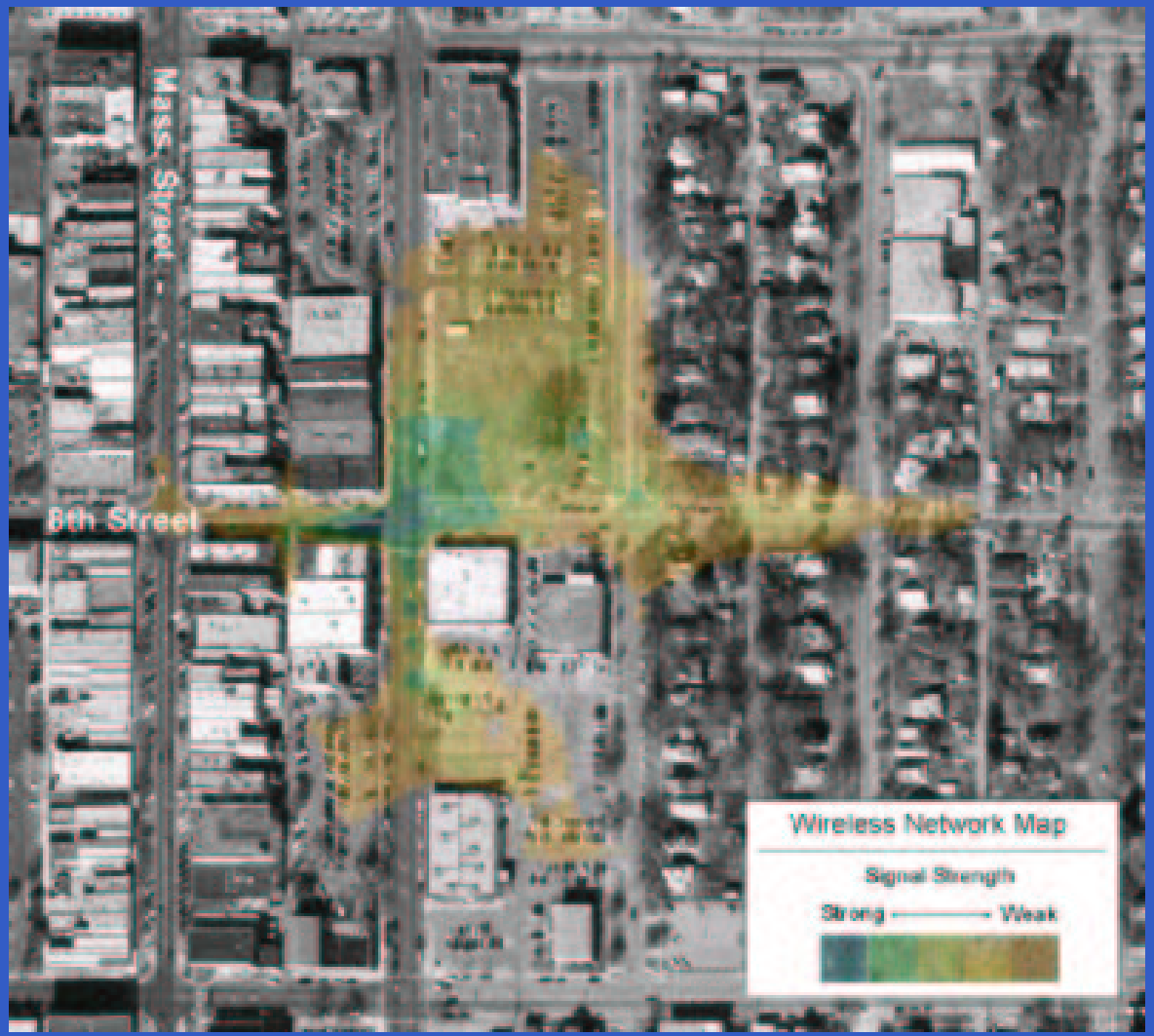
Hardware:

- Un portatile, o
- Un palmare con uno slot PCMCIA (iPaq)
- Una scheda PCMCIA 802.11b

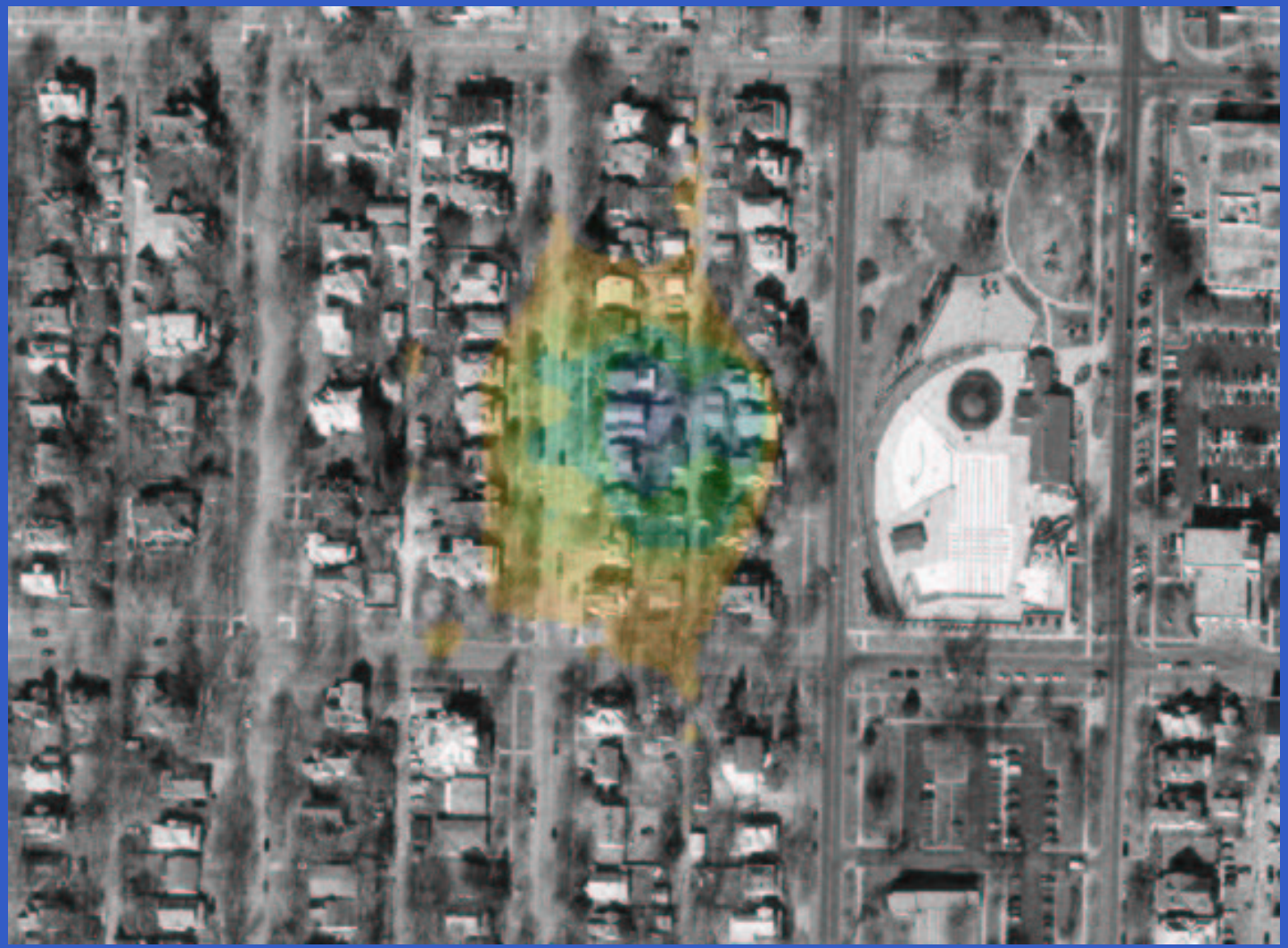
e magari

- Una periferica GPS
- Un’antenna, (omni)direzionale
- Un inverter

Il gps aiuta...


Mass Street
8th Street
Wireless Network Map
Signal Strength
Strong
Weak

Il gps aiuta...



Strumenti e tecniche

Software:

- Un sistema operativo (meglio OpenSource)
- uno o più a scelta tra kismet, wavemon, airtraf, WellenReiter, AirSnort, WepCrack, BsdAirTools, THC-WarDrive, NetStumbler...
- più il solito: tcpdump, ethereal, dsniff, ettercap, samba

e la voglia di fare war[driv|walk|bik|chalk]ing

Una piccola nota

I chipset delle schede wireless...

- Intersil PrismII (Es. DLink)
- Cisco (AiroNet 340/350)
- Orinoco (Lucent WaveLan)

...e la questione pratica dei canali e delle antenne

Un’antenna omnidirezionale da 10dB di guadagno (1mt), ha un raggio di 1.9Km. Una veicolare da 5dB (25cm), ha un raggio di 500mt.

Vi piacciono le Pringles?

http://www.turnpoint.net
http://www.oreillynet.com/cs/weblog/view/wlg/448
Quasi al costo di un tubo di Pringles ($6.45)...
è possibile costruire una direzionale da +10dB

Top 3 tools

IMHO:

- wavemon
- airtraf
- kismet

Milano, senza antenna, Aironet 340.
1 ora, 8 reti, 1 con WEP.

Tenendo presente che sono tutti software più o meno beta...

wavemon

Ottimo per il dettaglio del livello 1.
È particolarmente utile per monitorare

- Intensità e storico del segnale
- Livello di rumore

per fare tuning di antenne, o cercare posizioni migliori

airtraf

Simile ad iptraf, da cui il nome, è utile per i livelli 2-4. Offre breakdown statistico dell'utilizzo della banda

- Frame di management e controllo
- Traffico IP
- Traffico TCP/UDP
- Livello di rumore

Aiuta a capire se vale la pena di usare AirSnort/WepCrack.

kismet

Forse lo strumento più versatile, con una interfaccia unificata per

- Livelli di segnale della scheda wireless
- Discovery dell'indirizzamento via ARP o IP
- visualizzazione di stringhe dal traffico
- approfondimento delle informazioni sull'AP
- ha persino un'interfaccia a festival... :)

Dumpa il traffico su disco in formato tcpdump, per analisi posteriore

Sviluppi ulteriori

- arp spoofing sulla rete wired agendo da 802.11
- iniettare pacchetti (CDP, 802.1d)

Una comunità italiana sul wireless?

wifi@kill-9.it

Rimedi

- Se dovete usare WEP, almeno da 128bit
- Controllo sui MAC Address (ma si cambiano)
- Cifratura del Plaintext (IPSec, CIPE) o almeno a livello applicativo (SSH, SSL)
- Limite Orario
- Access Point almeno in DMZ

Ringraziamenti

- vi, LaTeX, Gimp, gnuplot e la comunità OpenSource
- www.ittc.ku.edu/wlan
- www.seattlewireless.net
- sikurezza.org