
Wireless (In)Security
Giuseppe Augiero

Obiettivo del Talk

- Lo scopo di questo seminario e' sensibilizzare gli utilizzatori della tecnoligia Wireless ad un uso più oculato di essa.

- Si vuole anche dimostrare che spesso coloro che effettuano il design di una rete Wifi credono in falso senso di sicurezza.

La tecnologia

Wireless

- Il termine **wireless** (dall'inglese **senza fili**) indica i sistemi di interconnessione tra dispositivi che non fanno uso di cavi. I sistemi tradizionali basati su connessioni cablate sono detti wired.

- Il mezzo di trasporto dell'informazione può essere un segnale radio, la luce infrarossa o un fascio laser.

Wifi

- Il principale standard di riferimento del mondo wireless è il protocollo 802.11.
- L'infrastuttura **Wifi** utilizza il suddetto protocollo per creare una rete senza fili .
- Il sistema wifi produce campi elettromagnetici a 2.400 Mhz. (microonde) con misurazione di 0,5 V/m alla distanza di 150/200 cm

Protocollo 802.11

	802.11a	802.11b	802.11g
Ratifica Standard	2002	1999	2003
Banda /Modulaz.	5GHz / OFDM	2.4GHz / DSSS	2.4GHz / OFDM
Velocità	Fino a 54Mbps	Fino a 11Mbps	Fino a 54Mbps
Copertura	Fino a 50 Metri	Fino a 100 Metri	Fino a 100 Metri
Vantaggi	Minori possibilità di interferenze con le frequenze radio Buon supporto x applic. multimediali e ambienti con alto n° di utenti	Compatibilità certificata Wi-Fi Il sistema oggi più largamente sviluppato; prezzi convenienti	• Compatibile con 802.11b • Alta velocità ed elevata copertura
Svantaggi	Richiede modifica hw Minore area di copertura	bassa velocità	

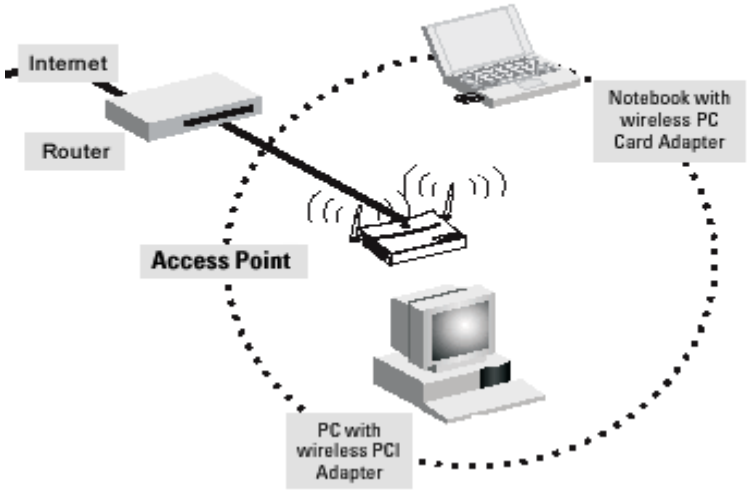
In corso di definizione

- **802.11d** – Definisce i requisiti del livello fisico che soddisfano le richieste di quei paesi che non hanno ancora legiferato in merito a 802.11 WLANS .
- **802.11e** - Opera su 802.11MAC per incrementare la QoS ed assicurare il supporto alle applicazioni audio/video.
- **802.11f** – Migliore la gestione del roaming per mantenere stabile una connessione WLAN tra apparati diversi che afferiscono a segmenti di rete diversi (IAPP).
- **802.11h** – Incrementa il controllo sulla potenza trasmissiva e il suo dosaggio sui canaliadibiti a portare 802.11a. Questo standard è espressamente dedicato a soddisfarele obiezioni avanzate da ETSI in merito alle interferenze su canali RADAR.
- **802.11i** – Implementa 802.1x come base per tutti gli sviluppi in termini diautentificazione.
- **802.11j** – Si preoccupa di armonizzare due standard diversi come 802.11a e HiperLAN2 totalmente in da renderli coesistenti.

Ad-hoc Wlan

- Non prevede un nodo centrale di smistamento.
- Ogni apparato si appropria di un canale.
- Ogni nodo fa da instradatore per gli altri client.

Wlan strutturate



- Lo smistamento dei dati e' affidato all'Access Point
- Ogni nodo comunica solo con l'AP
- L'Ap può estromettere alcuni client dalla comunicazione.

Beacons

- L'Access Point segnala la sua presenza attraverso speciali pacchetti chiamati **Beacons**.
- I Beacons sono inviati ad intervalli regolari.

Associazione

- Il client wireless riconosce l'Access Point e richiede il collegamento alla rete da esso gestita, comunicando i suoi parametri di collegamento.

Autenticazione

- L'Access Point può accettare o rifiutare il client a seconda dei parametri connessione forniti e in base al mac address del client.
- Se autenticato, il client viene ammesso nella rete e avviene lo scambio delle chiavi crittografiche.

Wep

- La chiave wep deve essere conosciuta a priori dal client e dall'access point.
- La chiave e' limitata in lunghezza.
- L'algoritmo in se e la sua applicazione sono poco sicuri.

Sicurezza

Sicurezza vò cercando

- **Le connessioni Wireless hanno bisogno di un grado di attenzione maggiore rispetto a qualsiasi altro tipo di connessione.**

Insicurezze

- La tecnologia Wireless non ha confini fisici.
- L'associazione ad un AP e' spesso invisibile.
- Pochissime persone usano il Wep o il Wpa.
- Chi certifica l'Access Point.

Il nemico invisibile

- Un attacco wireless e' spesso difficile da riconoscere in quanto spesso e' quasi invisibile.

- Policy:
  - Chi e' il vostro attacker.
  - Cosa dovete proteggere?

Possibili utilizzi

- Uso non autorizzato.
- DOS.
- Intercettazioni.
- Manipolazione.
- Mascheramento.

Note legali

- Associarsi a un Access Point non nostro è violazione di domicilio informatico.
- Pensateci bene prima di rischiare.
- Accedere a un AP significa violare la legge:
  - Art. 617 quater cp Intercettazione, impedimento o interruzione comunicazioni informatice.
  - Art 617 quinquies cp Installazione di apparecchiature atte ad intercettare comunicazioni informatiche.
  - Art 615 ter cp Accesso abusivo a un sistema informatico o telematico

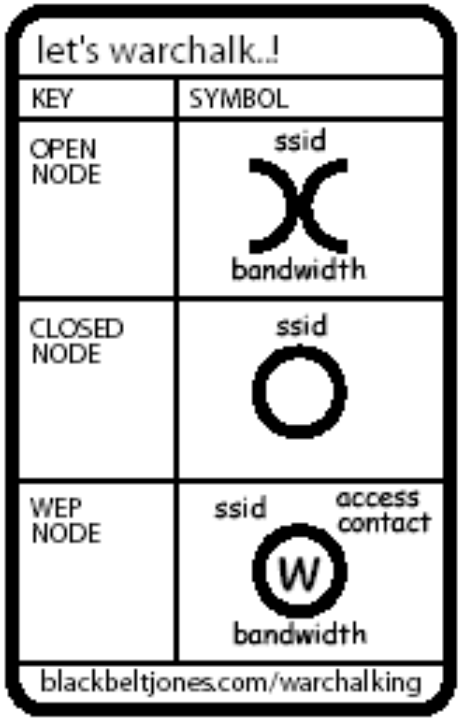
Moda del momento

Wardriving

- E’ quasi diventato un fenomeno di costume viaggiare in macchia con un pda o un notebook e ricercare di reti wireless presenti sul territorio.
- L’attività di wardriving non richiede elevate conoscenze tecniche.

Warchalking

- Segnalazione di reti wireless attraverso segni comuni.



Un caso reale

Pisa

- Pisa, città all'avanguardia tecnologia e popolata da un moltissimi studenti.
- Sul territorio Pisano sono presenti numerosi HotSpot, di alcuni W-ISP.
- Topologia particolare.

Censimento e Leggi

- E' una semplice ricerca a scopo di censimento.
- Non essendoci l'intenzione fraudolenta nell'analizzare i dati passanti sui 2.4 ghz e non andando mai in nessum modo a controllare il contenuto dei pacchetti in transito, siamo al riparo dall'infrangere leggi sulle intercettazioni.
- Inoltre, non essendoci mai associati agli access point rilevati, non ci siamo mai abusivamente introdotti in un sistema informatico mettendoci al riparo dal violare l'Art. 615 cp.

Strumenti per il censimento

- Per effettuare il censimento si e' adoperato:
  - Portatile (Linux Debian)
  - Sk wireless ipw2200 integrata nel sistema
  - Dongle Bluetooth integrato nel sistema
  - Gps

Software per il censimento

- Per il censimento sono stati utilizzati:
  - Kismet
  - Gpsd
  - GpsDrive
  - Mysql
  - Scritpt di conversione xml - kml
  - Google Earth

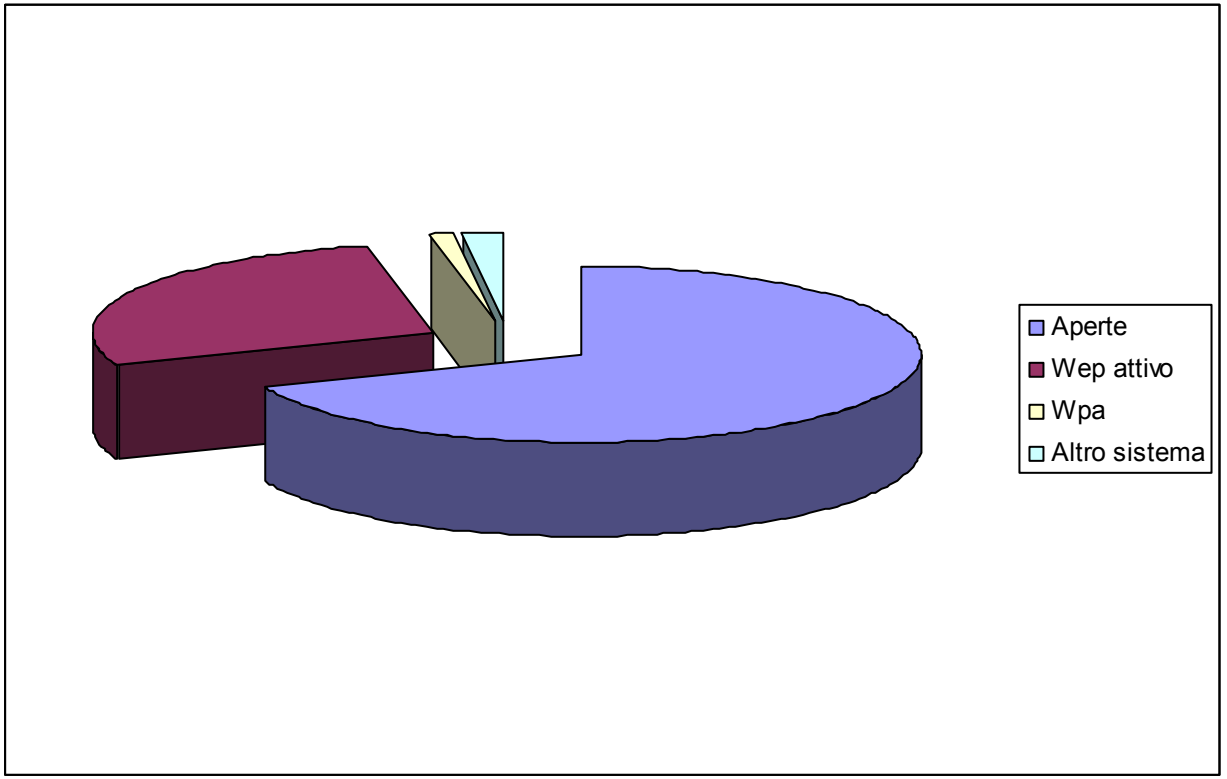
Tecniche di censimento

- Beacon attivi.
- Ricerca passiva.
- No antenne extra.

- No dump traffico.
- No accesso all’AP.
- No attività di analisi.

Risultati

Sicurezza Pisa



Soluzioni

La filosofia sicura

- **La sicurezza dei protocolli nasce da un buon design.**
- La ricerca e' l'unica via.
- Falso senso di sicurezza.

Crittografia

- Utilizzare sempre Wep o Wpa.
- Introdurre altri standard per la crittografia e l'autenticazione.
- Utilizzare protocolli che usano la crifratura (SSH, SSL, TLS).
- Utilizzare Vpn.

SSID

- Ssid non prevedibile.
- Broadcast Ssid non abilitato.

Mac Address

- Implementare il blocco dell'associazione ai mac address non conosciuto.
- Nel caso di molti AP da gestire utilizzare un server Radius.

Collocazione AP

- Il posizionamento dell'Access Point deve avvenire in modo accurato all'interno della rete.
- Le policy di sicurezza devono considerare l'Ap come un nodo untrusted.

Utenti

- **Educare gli utenti del servizio.**

Eap (I)

- Extensible Authentication Protocol (Rfc 2284) e' una estensione di PPP, adottato dal protocollo 802.1x.
- Consente di autenticare l'utente su un server esterno.
- Supporta differenti meccanismo di autenticazione.
- L'Access Point fa solo da tramite per consentire il dialogo di autenticazione.
- L'autenticazione e' centralizzata.

Eap (II)

- Prevede la distinzione degli apparati in:
  - Supplicant: la parte di autenticazione che opera sul client (Client).
  - Authenticator: l'apparato di rete a cui il supplicant deve agganciarsi (AP).
  - Authentication server: la risora centrale a cui gli authenticator si rivolgono per avere conferma dell'autorizzazione. (Server Radius).

Eap (III)

- Scegliere la soluzione migliore:
  - Eap-MD5
  - Eap-TSL
  - Eap-TTSL

Soluzioni proprietarie:

  - Leap
  - Peap

Vpn & PPPoE

- Ottima soluzione per collegare due reti wired via wireless.

Confondiamo le idee

- FakeAP si limita a generare falsi pacchetti di advertisement creando false reti e falsi Access Point sulle varie frequenze.
- In questo modo, l'unico modo per attaccanter, per capire quale sia la rete corretta, è associarsi a tutte e capire quale sia quella reale.

Domande?