



Wireless Fidelity

R e d a t t o d a

S t e f a n o Q u i n t a r e l l i

Indice

Premessa	3
Cosa è il WiFi	3
Standard e frequenze	6
Le disposizioni normative	8
<i>La discussione sulla normativa</i>	9
La questione della sicurezza	10
<i>Policy di sicurezza</i>	10
<i>Autenticazione e Riservatezza</i>	11
NOTE SUL DOCUMENTO	13
<i>Informazione sul copyright</i>	13
<i>Riproduzione parziale</i>	13
<i>Riproduzione integrale</i>	13
<i>Altri usi</i>	13
<i>Informazioni sull'Autore</i>	13

Premessa

A partire dalla fine maggio 2002, si è verificata una esplosione di comunicazione su tutti i media relativamente ai sistemi di tipo WiFi; questa comunicazione è stata spesso imprecisa, talvolta errata, certamente sempre confusa.

Ad aggravare la confusione nei lettori sono stati anche i numerosi articoli e comunicazioni apparsi su quasi tutta la stampa a commento di offerte commerciali di alcuni operatori telefonici che, unitamente ai propri servizi di telecomunicazione (in genere Internet), offrivano ai clienti pacchetti hardware comprendenti Access Point WiFi.

Cosa è il WiFi

WiFi è un marchio che designa gli apparati "Wireless Fidelity": dispositivi hardware che consentono di effettuare comunicazioni digitali wireless secondo lo standard 802.11b, standard anche noto con il nome di "Wireless Ethernet".

Se consideriamo un normale scenario di rete locale in un ufficio troviamo alcuni personal computer, ciascuno contenente una scheda di rete Ethernet a 10MHz o a 100MHz (gergalmente ma impropriamente dette a 10 o 100 Mbps); i personal computer sono collegati con dei cavi di rete ad un Hub (talvolta ad uno switch) il quale a sua volta viene connesso ad un router sul quale viene attestato il collegamento esterno alla rete locale. (cfr. Fig. 1), sia esso permanente (con un Circuito Diretto Numerico o accesso xDSL) o temporaneo (con un accesso ISDN o analogico).

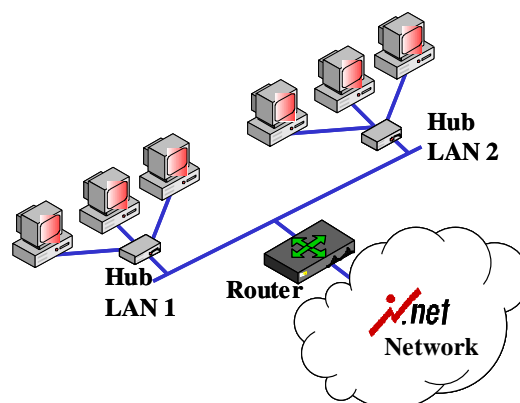


Fig. 1

Due LAN tradizionali collegate ad Internet

A fine del 1999 hanno cominciato a diffondersi sul mercato dispositivi che consentivano di sostituire un hub tradizionale e le corrispondenti schede di rete inserite nei personal computer con dei sistemi wireless consentendo quindi la creazione di reti locali anche in contesti in cui la stesura del cablaggio risultasse costosa o difficile; in presenza di reti locali cablate si usa il termine LAN; nel caso di reti locali Wireless si usa il termine "BSS". (Fig. 2). Si noti che nel caso della LAN più computer sono collegati ad un HUB; gli Hub Wireless sono più propriamente dei Bridge e vengono comunemente chiamati Access Points.

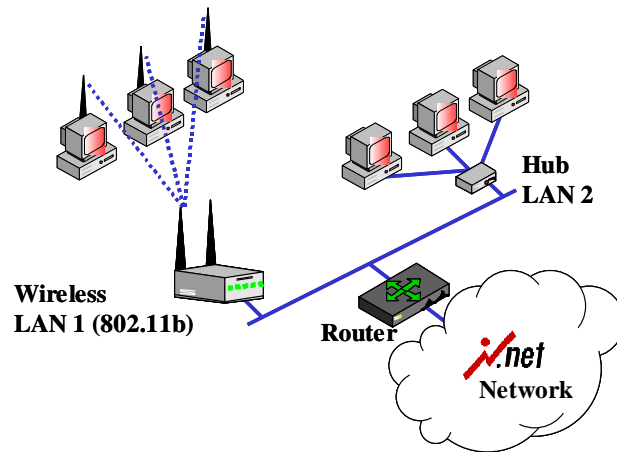


Fig. 2

Due LAN collegate ad Internet, una Wireless ed una cablata

Un BSS o “Basic Service Set” è un insieme di due o più nodi wireless (o “stazioni”: STA) che si sono identificate reciprocamente ed hanno stabilito una comunicazione. Nella forma più basilare di comunicazione, le STA possono comunicare direttamente tra loro in modalità peer-to-peer. Questo tipo di rete si forma in genere in modo temporaneo (ad esempio quando un insieme di colleghi si trova in una sala riunioni) e viene chiamato “Ad Hoc Network” o, più semplicemente “modalità Ad Hoc”, o anche “Independent Basic Service Set” (IBSS). In Fig. 3 è illustrato un esempio di IBSS.

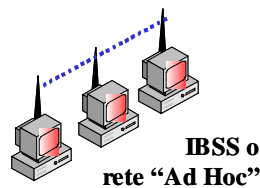


Fig. 3

Rete operante in modalità Ad Hoc

Nella maggioranza dei casi le BSS contengono un Access Point la cui funzione, come detto in precedenza, è fungere da Bridge tra reti wireless e reti cablate. Un AP è analogo ad una Base Station (BS) di una rete telefonica cellulare. In presenza di un AP, le STA non comunicano in modalità peer-to-peer; tutte le comunicazioni che avvengono tra STA e tra una STA e la rete fisica passano attraverso l'AP. Gli AP non sono mobili e formano parte della infrastruttura fisica della LAN; un BSS in questa configurazione si dice che opera in modalità “infrastructure”.

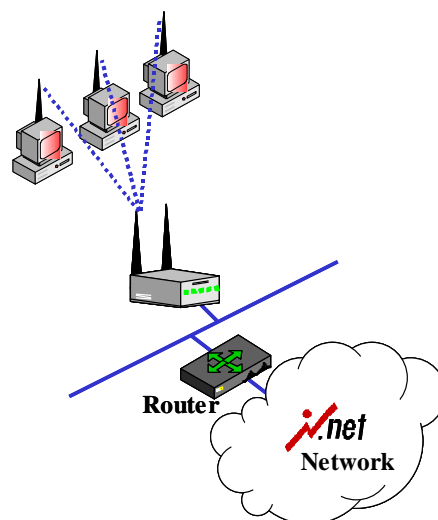


Fig. 4

Rete operante in modalità Infrastructure

In una LAN con cablaggio tradizionale, un repeater è un dispositivo che consente di “leggere” il segnale elettrico trasportato su uno spezzone di una LAN e di “trasferirlo” su un altro spezzone di LAN in modo tale da potere, di fatto, estendere una LAN oltre il limite fisico di rete Ethernet pari a 500m (se i cavi sono di tipo STP: Shielded Twisted Pair o Doppino Schermato).

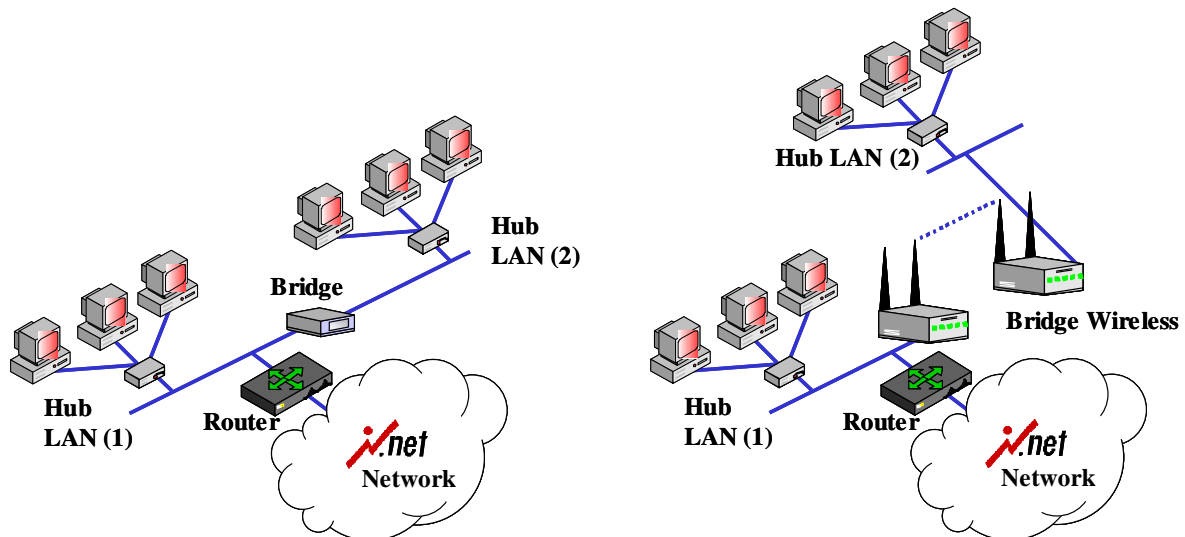


Fig. 5

Due spezzoni di LAN connessi, a sinistra con un Bridge ed a destra con un Access Point

Mentre in presenza di un Bridge per LAN fisiche, generalmente si possono solamente unire solo due spezzoni di rete realizzando una sorta di collegamento “punto-punto”, nel caso di Access Point wireless, si possono effettuare dei collegamenti “punto-multipunto”, come esemplificato in Fig. 6.

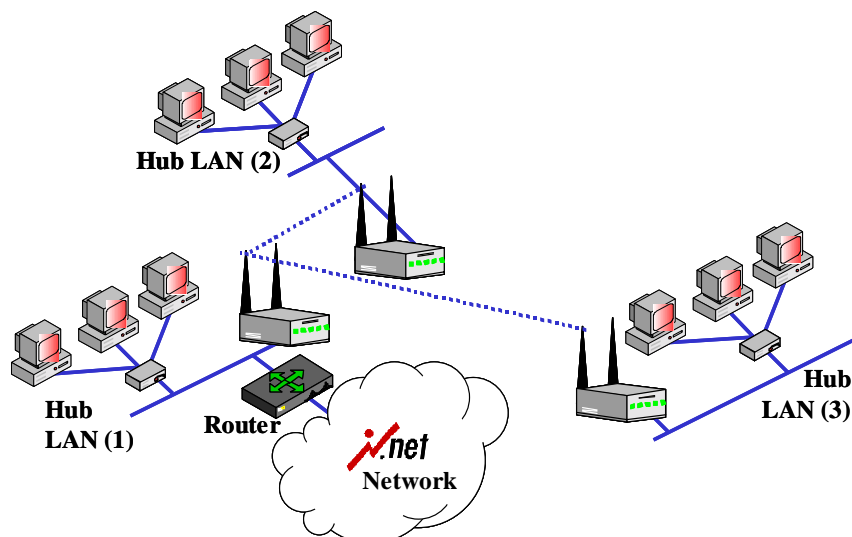


Fig. 6

L'Access Point dello spezzone di LAN (1) sta operando in modalità punto-multipunto.

Naturalmente, in questo scenario, le prestazioni dei due collegamenti wireless sono inferiori a quelle di un singolo collegamento in quanto condividono lo spettro e si contendono le risorse.

Standard e frequenze

Il Wireless Fidelity o WiFi rivela già dal proprio nome l'intenzione di marketing di costituire un prodotto di elettronica di consumo per realizzare piccole LAN domestiche senza la necessità di intervenire sulle strutture delle abitazioni.

Lo standard 802.11b prevede la trasmissione in uno spettro di frequenza compreso, in Italia così come in altri paesi, tra i 2,4GHz e i 2,4835GHz. Vale la pena di ricordare qui che i telefoni cellulari GSM operano su frequenze comprese in un intorno di 0,9GHz e 1,8GHz. Il WiFi pertanto opera appena al di sopra di queste bande regolamentate.

La banda citata di 2,4GHz infatti non è soggetta a licenze in molti paesi del mondo tra cui l'Italia e può essere utilizzata da chiunque nell'ambito però di severi limiti di emissione di potenza; il limite di emissione in Italia è pari a 100mW.

Gli elementi che possono condizionare, limitandola, l'efficacia di un collegamento wireless si chiamano in gergo "Clutter" e riguardano la densità di edificazione, la presenza di interferenze elettromagnetiche, la densità di fogliame, la copertura di visibilità ottica, ecc.

Con questo livello di potenza, nella maggior parte delle situazioni, è possibile realizzare una rete locale wireless entro una distanza dai 50 ai 100 metri con un Access Point installato internamente ed in un contesto con molto Clutter, e fino a circa 400 metri in un contesto con poco Clutter ed un Access Point collocato in luogo elevato e visibile.

In questo spazio di frequenze vengono definiti 13 canali logici per cui, se opportunamente configurati, è possibile utilizzare 13 collegamenti wireless con un minimo degrado del tasso di trasferimento dati (throughput).

Va ricordato che il protocollo di accesso al mezzo fisico da parte delle reti Ethernet è il CSMA/CD: Carrier Sense Multiple Access with Collision Detection. Questo meccanismo prevede che chiunque debba trasmettere, proceda nel seguente modo: prima di trasmettere deve ascoltare la portante per rilevare se qualcun altro sta trasmettendo; qualora nessuno stia impegnando il mezzo trasmissivo si può effettuare la trasmissione, dopo aver trasmesso si deve ascoltare la trasmissione al fine di rilevare se altri abbiano trasmesso contemporaneamente causando collisioni. Se si è verificata una collisione che non ha consentito l'invio corretto dei dati, sarà necessario attendere un breve lasso di tempo prima di ritentare la trasmissione.

Questo protocollo di accesso CSMA/CD, caratteristico di tutte le reti Ethernet, siano esse Wireless o via cavo, fa sì che il throughput (quantità di dati effettivamente trasferiti per unità di tempo) sia sempre molto inferiore alla velocità nominale.

Il tasso di trasferimento nominale di un collegamento WiFi è di 11 Mbps; qualora un solo personal computer stia comunicando con un Access Point e la qualità del collegamento wireless sia buona (scarse interferenze, buona visibilità, assenza di ostacoli), le collisioni saranno assai contenute ed il throughput potrà essere anche superiore a 6 Mbps; qualora numerosi personal computer comunichino con un Access Point (nelle medesime condizioni), il throughput sarà simile a quello riscontrabile in una Ethernet a 10MHz ovvero intorno ai 3Mbps.

Va notato che, dato che le frequenze sono liberamente utilizzabili ed il costo dei dispositivi hardware negli ultimi 3 anni si è ridotto quasi di un ordine di grandezza, in contesti densamente popolati di sistemi informatici, quali ad esempio i centri uffici, stante il limitato numero di canali ed il limitato throughput per canale, la capacità del sistema tende ad essere massimizzata molto in fretta e gestire interferenze con altri utenti può risultare molto complesso.

La maggior parte dei Bridge 802.11b usano una tecnologia chiamata DSSS (Direct Sequence Spread Spectrum) che è abbastanza robusta alle interferenze elettromagnetiche; gli standard 802.11a ed 802.11g utilizzeranno una tecnica denominata OFDM (Orthogonal Frequency Division Multiplexing) che si ritiene offrirà livelli di robustezza ancora maggiori.

Per migliorare le prestazioni, qualora possibile, è consigliabile usare delle antenne direzionali che consentono di focalizzare maggiormente la potenza nell'area di copertura riducendo nel contempo le interferenze in aree adiacenti.

Ciò consente di ridurre e gestire le interferenze con altri dispositivi che utilizzano lo stesso spettro di frequenze quali i telefoni cordless o DECT, forni a microonde, dispositivi Bluetooth, apriporta, radiogiocattoli, radiomicrofoni, telecomandi, ecc...

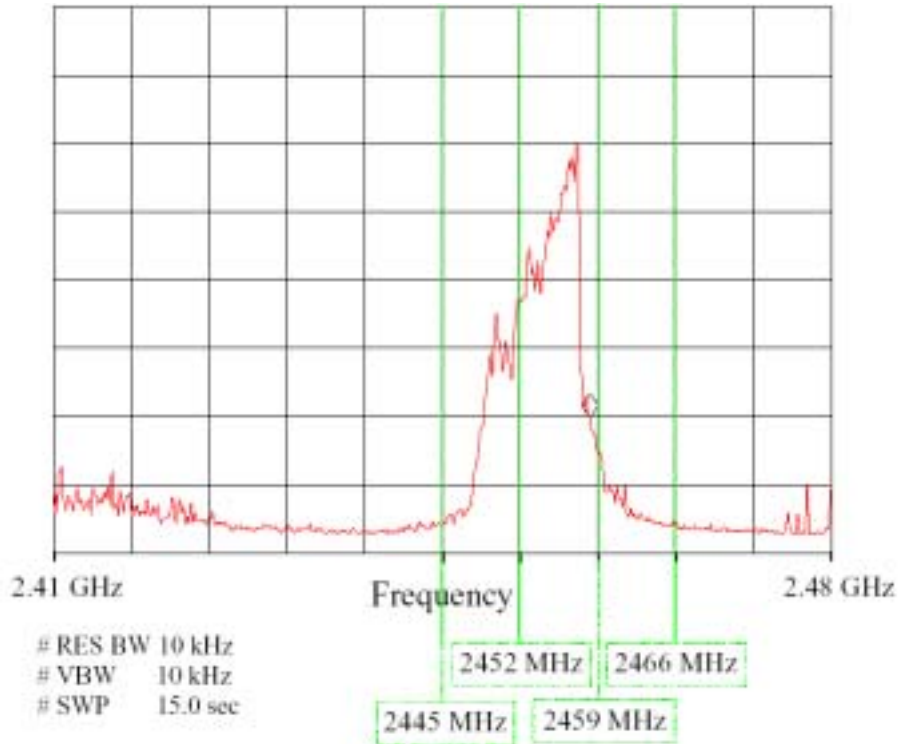


Fig. 7

Spettro di un forno a Microonde ad uso domestico
 (Fonte: "Microwave Oven Interference on Wireless LANs
 Operating in the 2.4 GHz ISM Band" – Lucent Technologies)

Con il proliferare delle reti wireless, in special modo nei centri uffici e nelle abitazioni residenziali, gli aspetti di interferenza diverranno sempre più problematici.

L'industria sta rispondendo con l'introduzione di due soluzioni come accennato sopra: gli standard 802.11a ed 802.11g.

In particolare, l'802.11a prevede di utilizzare uno spettro intorno ai 5GHz, cosa che lo renderà intrinsecamente più resistente alle interferenze, sarà possibile avere un numero di reti che condividono la frequenza almeno 5 volte superiore a quanto possibile con apparati 802.11b sebbene, a parità di potenza di emissione, coprirà una distanza inferiore agli apparati 802.11b. Lo standard 802.11g è ancora a livello embrionale, prevede di essere compatibile sia con gli 802.11a che con gli 802.11b.

L'arrivo sul mercato di apparati in standard 802.11a sarà evidente in quanto verranno designati con la sigla "WiFi 5" per indicare appunto che operano a 5GHz.

Le disposizioni normative

Come già accennato, la banda di 2,4GHz non è soggetta a licenze in molti paesi del mondo tra cui l'Italia e può essere utilizzata da chiunque nell'ambito però di severi limiti di emissione di potenza; il limite di emissione in Italia per apparati a "bassa potenza" è pari a 0,1W/mq per la potenza dell'onda piana equivalente (più diffusamente noto come limite di 100mW), come stabilito dal decreto ministeriale 381/98 all'articolo 4, comma 2.

La regolamentazione applicata alle attività di telecomunicazioni è quella prevista nel decreto del Presidente della Repubblica n° 447 del 5 ottobre 2001 disponibile all'indirizzo http://www.comunicazioni.it/normativa/teleco/tel_dpr447-01.htm

All'articolo 4 si specifica che:

1. **Una licenza individuale è necessaria** nel caso di installazione di una o più stazioni radioelettriche o del relativo **esercizio di collegamenti di terra e via satellite richiedenti un'assegnazione di frequenza**, con particolare riferimento a: sistemi:

a) fissi, mobili terrestri, mobili marittimi, mobili aeronautici;

[omissis]

All'articolo 5 si specifica che:

1. **Un'autorizzazione generale** è necessaria nel caso di:

[omissis]

b) **installazione o esercizio di sistemi che impiegano bande di frequenze di tipo collettivo:**

[omissis]

2) senza alcuna protezione, **mediante dispositivi di debole potenza**, compresi quelli rispondenti alla raccomandazione CEPT/ERC/REC 70-03.

[omissis]

2.2) di installazione o **esercizio di reti locali radiolan e hiperlan**, ad eccezione di quanto disposto dall'articolo 6, comma 1, lettera b);

[omissis]

All'articolo 6 si specifica che:

1. Sono di **libero uso** le apparecchiature che impiegano frequenze di tipo collettivo, senza alcuna protezione, **per collegamenti a brevissima distanza** con apparati a corto raggio, compresi quelli rispondenti alla raccomandazione CEPT-ERC/REC 70-03, tra le quali rientrano in particolare:

[omissis]

b) **reti locali di tipo radiolan e hiperlan nell'ambito del fondo**, ai sensi dell'articolo 183, comma secondo, del decreto del Presidente della Repubblica n. 156 del 1973; sono disciplinate ai sensi dell'articolo 5 le reti hiperlan operanti obbligatoriamente in ambienti chiusi o con vincoli specifici;

Per "fondo" in materia di telecomunicazioni si richiama la legge del 1973 all'articolo 183 che recita:

Nessuno può eseguire od esercitare impianti di telecomunicazioni senza aver ottenuto la relativa concessione o, per gli impianti di cui al comma secondo dell'art.1, la relativa autorizzazione.

Tuttavia **è consentito al privato di stabilire, per suo uso esclusivo**, impianti di telecomunicazioni per collegamenti a filo **nell'ambito del proprio fondo** o di più fondi di sua proprietà, purché contigui, ovvero nell'ambito dello stesso edificio per collegare una parte di proprietà del privato con altra comune, **purché non connessi alle reti di telecomunicazione destinate a pubblico servizio.**

Parti dello stesso fondo o più fondi dello stesso proprietario si considerano contigui anche se separati, purché collegati da opere permanenti di uso esclusivo del proprietario, che consentano il passaggio pedonale.

[omissis]

Questo articolo vieta l'erogazione di servizi a terzi pur anche nell'ambito del proprio fondo, ed in particolare vieta esplicitamente l'interconnessione della BSS ad una rete pubblica (Internet).

Riassumendo, il decreto del 5 ottobre 2001 prevede tre categorie di utilizzo:

- Licenza individuale
- Autorizzazione Generale (in questo caso sono dovuti dei contributi per ogni sede e per ogni variazione)
- Uso libero

La licenza individuale riguarda i soggetti cui viene assegnato un insieme di frequenze quali radio, televisioni, operatori telefonici mobili.

L'autorizzazione generale riguarda i soggetti che offrono servizi di telecomunicazioni all'esterno del fondo

L'uso libero può essere effettuato all'interno di un fondo.

E' comunque vietata espressamente l'interconnessione a fini commerciali di sistemi radiolan a reti pubbliche di telecomunicazioni quali Internet e la rete telefonica.

La discussione sulla normativa

Molti ritengono che i bassi limiti di emissione imposti per legge a 100mW non siano giustificati dato che, di per sè, la tecnologia è in grado di rendere possibili comunicazioni su distanze anche dell'ordine di una decina di chilometri. Molti ritengono che il regime di Autorizzazione generale che prevede la dichiarazione dei siti ove sono collocate antenne ed un contributo annuale dovuto per ogni installazione e variazione sia un freno alla diffusione della tecnologia.

Infine, molti ritengono che il divieto di interconnessione a reti pubbliche sia un limite allo sfruttamento commerciale a tutela degli operatori che hanno acquisito frequenze in regime di Licenza Individuale investendo enormi quantità di denaro a beneficio dell'erario.

Molti sostengono che lo spirito dell'impianto normativo sia quello di consentire l'utilizzo di sistemi in radiofrequenza ad uso domestico o comunque privato in luoghi ristretti, aumentando le garanzie per gli utenti sia per quanto concerne gli aspetti legati alla salute, sia per quanto concerne le interferenze.

Si ritiene infatti che, qualora fosse possibile sfruttare commercialmente questo spettro di frequenze vi sarebbe una enorme proliferazione di dispositivi, praticamente incontrollabili in termini di potenze di emissione e di interferenze a nocimento di tutto il sistema (un po' come avvenne intorno a fine anni 70 con la proliferazione delle radio libere che richiese un intervento regolatore successivo).

La questione della sicurezza

La questione della sicurezza logica dei dati trasmessi e del controllo degli accessi ai sistemi connessi ad una BSS è certamente enorme.

I due problemi fanno riferimento in modo predominante a tre aspetti della sicurezza in ambito wireless : le policy aziendali di sicurezza con relativa verifica con attività di Asset Auditing, l'AAAA (Autenticazione, Autorizzazione, Accounting, Auditing degli accessi alle BSS autorizzate), la riservatezza dei dati trasmessi mediante l'utilizzo di tecniche di cifratura.

Policy di sicurezza

Il primo aspetto è quello che riveste la criticità maggiore. Un Access Point wireless è estremamente attraente in termini di funzionalità offerte ad un utente. Alcuni anni fa, con i primi accessi ad Internet, alle LAN aziendali erano sovente connessi dei modem direttamente da parte degli impiegati senza che i responsabili dei sistemi ICT ne fossero a conoscenza.

Un Access Point può essere acquistato a basso costo presso un qualunque negozio di elettronica di consumo o, ancora più semplicemente, essere ottenuto da un fornitore di accesso ad Internet che, al fine di affittare più hardware al cliente, lo inserisce in pacchetti bundle.

L'installazione di un Access Point e di una scheda PCMCIA wireless è talmente semplice che chiunque può estrarre gli oggetti dalla scatola ed installarli con successo in pochi minuti; il processo è ancora più semplice di come era installare un modem nel 1997.

L'utente così sarà libero di muoversi in ufficio con il proprio portatile e quindi di partecipare a meeting in sale riunioni non cablate restando collegato alla propria LAN interna senza dover litigare con assegnazione di indirizzi IP, hub scollegati ed altri problemi tipici.

E' una prospettiva indubbiamente assai attraente, si aggiunga poi che i computer portatili di nuova costruzione, così come hanno incorporato un po' alla volta le schede di rete tra le componenti standard, oggi via via incorporeranno le schede di rete wireless la cui abilitazione richiederà solo qualche clic (o nemmeno quello, se il sistema si accorge automaticamente che è disponibile un Access Point appena tirato fuori dalla scatola e collegato alla presa di rete in ufficio!)

Il problema è che le configurazioni standard degli apparati appena estratti dalle scatole, non prevedono alcuna password di autenticazione ed alcun sistema di cifratura dei dati; in questo modo chiunque entri con un portatile dotato di una scheda di rete wireless nell'area di copertura dell'Access Point "aperto" avrà accesso alla LAN interna dell'organizzazione (che, ironia della sorte, magari investe enormi quantità di danaro per proteggere mediante sistemi firewall e di Intrusion Detection i varchi "ufficiali")

La BBC titolava "Welcome to the era of drive-by hacking" nel suo servizio (http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_1639000/1639661.stm) in cui raccontava l'esperienza di un giro in auto a Londra con un PC con scheda wireless fatto a novembre del 2001 che mostrava come su 12 reti wireless individuate, solo quattro avessero qualche meccanismo di protezione abilitato.

A fine marzo del 2002, nell'articolo "Wireless London is wide open" (http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_1892000/1892510.stm), ovvero meno di 5 mesi dopo, la stessa BBC pubblicava un altro articolo in cui presentava i dati di una ricerca durata sette mesi e finanziata dalla Camera di Commercio Internazionale che mostrava che su 5000 reti wireless rilevate in centro a Londra, ben il 92% di esse non aveva preso misure basilari di protezione atte a proteggere le LAN da attacchi casuali.

A completare il quadro si consideri che, a differenza dei famosi *hacker* esperti, geni del computer come vengono presentati generalmente dai media, il livello di competenze necessarie a collegarsi su una LAN interna sfruttando una BSS non protetta è praticamente nullo, estendendo così la popolazione dei possibili "aggressori" di vari ordini di grandezza, e persino a persone che non sanno bene cosa stanno facendo !

Il problema si presenta anche a livello domestico. L'abbonamento ADSL può essere utilizzato in modo banale da ogni vicino, se al router o network terminator ADSL viene connesso un Access Point per cui non vengono configurati sistemi di sicurezza; sfogliando le risorse di rete è possibile visitare gli hard disk dei vicini, ecc.

A livello aziendale si intuisce l'importanza di vietare in modo categorico l'utilizzo di Access Point non esplicitamente autorizzati e controllati ma questo divieto, soprattutto per le realtà più grandi e più diffuse sul territorio è generalmente insufficiente ed è perciò necessario dotarsi di sistemi o servizi di Asset Auditing che consentano di tenere sotto controllo tutti i dispositivi connessi alla rete fin nella più remota filiale.

Più in generale l'accelerazione con cui le Wireless LAN stanno invadendo il mercato rendono la questione della sicurezza logica sempre più attuale e contribuiranno ad accelerare una tendenza in atto di prevedere dei budget specifici, tipicamente all'interno dei budget dei responsabili ICT.

Autenticazione e Riservatezza

Esistono quattro meccanismi base di autenticazione e riservatezza utilizzabili in una BSS:

- Autenticazione basata sui MAC Address
- Cifratura con chiavi WEP statiche
- Autenticazione WEP/EAP
- VPN IPSEC con Strong Authentication

Autenticazione basata sui MAC Address

Un MAC address è un numero che identifica univocamente al mondo una scheda di rete ed è cablato nell'hardware; viene altrimenti detto "indirizzo fisico".

L'autenticazione basata sui MAC Address è disponibile nella grande maggioranza dei bridge 802.11; in questo scenario sull'Access Point viene configurato l'elenco dei MAC address delle schede wireless installate nei personal computer che possono accedere a detto Access Point.

Sebbene questo schema di protezione consenta di negare l'accesso ad un dispositivo il cui MAC address non sia stato esplicitamente previsto a priori, le trasmissioni tra l'Access Point ed un STA lecitamente connesso, avviene in chiaro, e quindi uno sniffer configurato correttamente potrà osservare e registrare tutto il traffico transitante sul collegamento wireless. All'interno di questo traffico sarà possibile determinare quindi un MAC address valido e, mediante una tecnica di falsificazione di identità (MAC spoofing) sarà possibile ottenere l'accesso alla BSS.

Wireless Encryption Protocol

WEP, o Wireless Encryption Protocol è uno standard che è stato definito con il fine di rendere un collegamento wireless sicuro come un collegamento via cavo. Secondo questo protocollo sia sull'Access Point che sulla STA vengono preconfigurate delle chiavi a 40 o 128 bit utilizzate da un algoritmo implementato sui due estremi che cifra tutto il traffico in transito.

Di recente sono stati documentati dei casi di violazione dell'algoritmo mediante analisi di un numero significativo di pacchetti di dati trasferiti tra AP e STA.

Si noti che l'algoritmo cifra il traffico con determinate chiavi preconfigurate dall'amministratore del sistema; l'algoritmo è un codice che deve essere eseguito in tempo reale su grandi quantità di dati trasmessi e ricevuti; l'algoritmo deve essere implementato su chip a costo molto basso per mantenere accessibile il prezzo degli apparati. Va da sé che il problema esisterà sempre, ovvero dato un costo del componente x (con x piccolo), esisterà sempre un altro componente o sistema dal costo Nx (con N grande) che consenta di decifrare il traffico sulla base di violazione dell'algoritmo esaminando un sufficiente quantitativo di dati trasmessi.

E' bene osservare che, comunque, una cifratura WEP, per quanto violabile da un intruso ben informato, è meglio di nessuna cifratura.

Extensible Authentication Protocol

Un modo per rinforzare il WEP è quello di variare frequentemente le chiavi utilizzate, in modo tale da rendere il lavoro di decifratura più complesso. Questa è la direzione in cui va il protocollo EAP (Extensible Authentication Protocol) usato con cifratura WEP; gli AP e le STA dialogano con diversi sistemi di autenticazione di backend (tipicamente RADIUS) per autenticarsi all'inizio di ogni comunicazione (in modo analogo a quanto avviene per il logon ad una rete) e generano delle chiavi che verranno utilizzate per cifrare il traffico solo per la sessione corrente.

Anche per questo tipo di protezione esistono delle vulnerabilità caratteristiche che lo rendono preferibile ad un semplice WEP ma meno preferibile rispetto a soluzioni più evolute.

VPN IPSEC con Strong Authentication

Il modo più sicuro per comunicare su una Wireless LAN è utilizzare una VPN (Virtual Private Network) appoggiando uno strato sicuro realizzato in standard IPSEC con 3DES (il 3DES o triplo DES è uno standard di cifratura che cifra i dati 3 volte utilizzando 3 chiavi differenti) su un collegamento wireless 802.11 in chiaro.

Anche qui l'autenticazione è determinante ed il modo di presentazione delle credenziali degli utenti non dovrebbe essere statico e basato solo su informazioni (username e password) che, essendo informazioni sono replicabili, ma bensì su sistemi di autenticazione forte (Strong Authentication) nei quali le credenziali che identificano gli utenti sono composte da informazioni e da oggetti fisici (ciò che "ho" e ciò che "so") in modo analogo a quanto avviene con le tessere bancomat nel sistema bancario.

NOTE SUL DOCUMENTO

Informazione sul copyright

Il presente documento è Copyright (2002) di I.NET Spa – BT Ignite; è stato redatto da Stefano Quintarelli; è stato concesso in distribuzione gratuita a CLUSIT- Associazione Italiana per la Sicurezza Informatica. Tutti i diritti riservati.

Il documento può essere richiesto in formato elettronico a CLUSIT- Associazione Italiana per la Sicurezza Informatica all'indirizzo di posta elettronica info@clusit.it

Riproduzione parziale

Porzioni del presente documento possono essere riprodotte liberamente esclusivamente in presenza della INFORMAZIONE SUL COPYRIGHT riportata al paragrafo precedente e dei loghi di I.NET Spa all'interno dei grafici.

Riproduzione integrale

Può essere ridistribuito liberamente in forma cartacea integrale, forma elettronica integrale e può essere riprodotto integralmente liberamente esclusivamente in presenza della presente nota sul Copyright.

Altri usi

Altri usi possono essere concessi previa autorizzazione esplicitamente concessa e da richiedersi all'indirizzo di posta elettronica comunicazione@inet.it

Informazioni sull'Autore

Stefano Quintarelli (s.quintarelli@inet.it) è Socio Fondatore e Direttore Commerciale di I.NET SpA (parte di BT Ignite), Socio fondatore di CLUSIT – Associazione Italiana per la Sicurezza Informatica

Si è occupato di sicurezza informatica a partire dal 1987 quale consulente di grandi aziende ed istituti bancari, come promotore e coordinatore di vari gruppi di lavoro in tema di sicurezza presso l'Università degli Studi di Milano.

E' stato "Assistant Sysop" dell'allora Bulletin Board di John McAfee, ha collaborato con Steve Chang fondatore di Trend Micro; si è quindi occupato di Network Security, fino alla fondazione di I.NET Spa.

Ha partecipato, coordinato, organizzato numerosi corsi, convegni e seminari sulla sicurezza informatica sia in ambito nazionale che internazionale; è autore di libri e pubblicazioni specialistiche.