Ci sono sin da subito alcune cose da sapere:

- **gli apparati wireless vengono venduti con tutte le misure di sicurezza disattivate, per cui chiunque può collegarsi a scrocco e/o far danni: è necessario l'intervento dell'utente per attivare le protezioni**
- **la sicurezza delle reti wireless è molto più debole di quanto ammettono i produttori di questi dispositivi senza fili**
- **le prestazioni reali sono di gran lunga inferiori a quelle pubblicizzate**
- **però tutto sommato la tecnologia funziona; basta conoscerne e rispettarne i limiti**

Ho realizzato la mia rete wireless usando dispositivi che seguono lo standard **802.11g**, per cui questi appunti si limitano alle apparecchiature che rispettano questo standard. Non ho materialmente il tempo di scrivere un trattato valido per tutte le varianti possibili delle connessioni senza filo.

Questa miniguida non pretende di realizzare una rete impenetrabile. La sicurezza assoluta non esiste. Però si può ambire a una sicurezza *ragionevole*, ossia sufficiente a scoraggiare gran parte degli intrusi e dei vandali, che andranno a cercarsi bersagli più facili, che vi assicuro non mancano.

La maggior parte delle informazioni riportate qui è **indipendente dal sistema operativo**. Vale quindi sia che usiate Windows, sia che usiate Linux, sia che usiate il Mac o qualsiasi altro computer e sistema operativo.

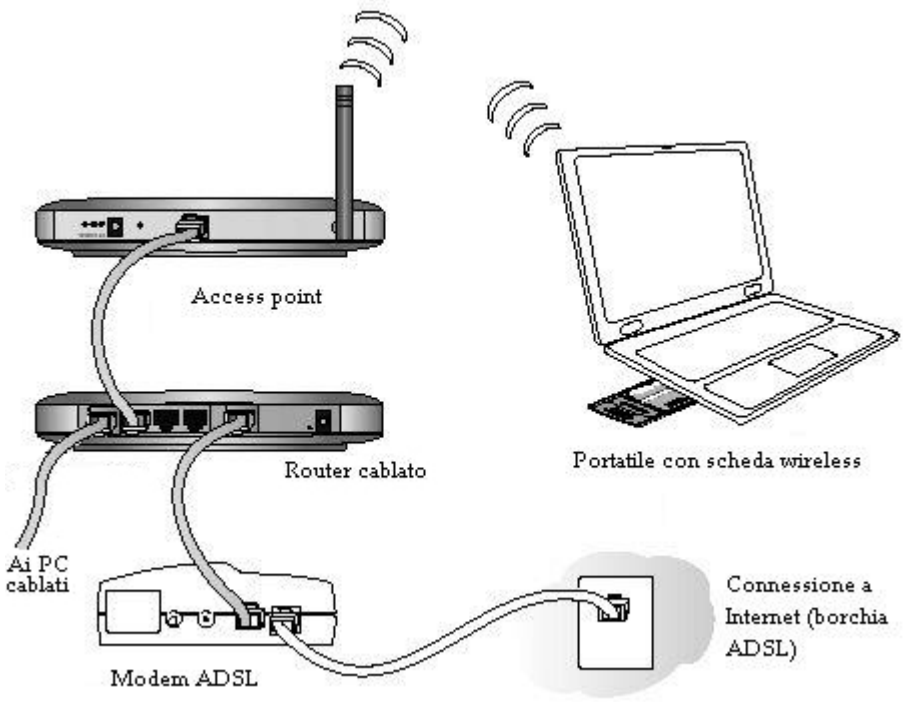
Parte di quello che ho scritto è tratto da un ottimo articolo di Ars Technica. Eventuali errori di interpretazione tecnica, ovviamente, sono colpa mia.

Ingredienti

Per creare una rete wireless di solito si usa una configurazione "a stella": ciascun computer si collega a un unico punto centrale, denominato *access point*. Ci sono anche altri gingilli wireless di nome *router* e *bridge*, che hanno funzioni simili, ma per semplificare li indicherò tutti genericamente come *access point* (gli esperti non mi mandino troppi accidenti). L'access point è poi collegato alla rete cablata e/o a Internet. Ci sono vari altri modi di collegare i computer con schede wireless, ma non me ne occupo qui.

Per esempio, nel mio piccolissimo caso, ho un portatile dotato di schedina wireless, che collego alla rete degli altri miei computer attraverso un access point, che a sua volta è attaccato a un router, al quale sono collegati via cavo gli altri computer. Il router è collegato a Internet tramite una connessione ADSL.

Lo schema è grosso modo quello mostrato nel manuale dell'access point NetGear che ho usato qualche tempo; lo riporto (con qualche modifica) qui sotto:



La rete wireless è una gran comodità: mi permette di lavorare in giardino o di acciambellarmi sul divano a rispondere alla posta o scrivere pagine Web come questa, mi evita di cablare l'intera casa per collegare i vari computer, e mi consente di andare su Internet e di stampare documenti da qualsiasi stanza della casa e con qualsiasi computer della rete.

Limiti

La connessione wireless, però, è **più lenta** di quella cablata.

- Le schede wireless che seguono lo standard 802.11g arrivano a 54 megabit al secondo in condizioni ottimali, mentre la connessione cablata normalmente ha una capacità di 100 megabit al secondo.
- Il guaio è che le "condizioni ottimali" sono molto rare. Basta che ci siano di mezzo un paio di muri e la qualità del segnale degrada e di conseguenza la connessione rallenta drasticamente. Rimane sufficiente per navigare in Internet, ma non certo per trasferire grandi file da un computer all'altro.

L'altro problema è la **portata limitata**.

- I manuali dei produttori parlano di portate massime di 150 metri al coperto (è il caso del manuale NetGear), ma in realtà ho trovato difficile collegare un computer situato in una stanza collocata a dieci metri di distanza dall'access point. Il segnale non copre neppure tutto il mio giardino: arriva a cinque-sei metri fuori dal perimetro di casa, e poi si deteriora al punto di essere inutilizzabile. Tuttavia altri apparecchi sono evidentemente più potenti, dato che se giro per le città tenendo attivo un programma di monitoraggio apposito, trovo il segnale forte di moltissimi dispositivi wireless.
- La portata viene inoltre penalizzata dal fatto che quasi tutte le attuali schede wireless lavorano a 2,4 GHz, che è la stessa frequenza sulla quale lavorano molti telefoni cordless e i forni a microonde. Se accendete uno di questi apparecchi, l'interferenza è tale che la connessione rallenta o addirittura cade.
- Due apparecchi che si sono rivelati fonte inaspettata di disturbi sono le **palle al plasma** (quegli oggetti ornamentali costituiti da una sfera di vetro dentro la quale si formano dei piccoli fulmini), che hanno fatto collassare *completamente* la connessione wireless (segnale a zero), e la lavastoviglie: quando il suo motore è in funzione, la portata del segnale precipita

a sei-sette metri dall'antenna dell'access point.

Tuttavia, se si rispettano e accettano questi limiti, la rete wireless è appunto una gran comodità.

Pericoli

Il guaio è che **questa comodità comporta anche dei rischi**. In ossequio alle leggi della fisica, il segnale radio della rete si diffonde per qualche decina di metri *in ogni direzione*, quindi anche fuori dalle mura domestiche, e quindi è intercettabile.

Con una connessione wireless, un intruso può entrare nella mia rete senza neppure prendersi il disturbo di entrarmi in casa. Si siede in macchina nella strada accanto, con un comune computer portatile e il software giusto (facilmente scaricabile da Internet), e si collega ai miei computer, legge i miei dati e scrocca la mia connessione a Internet. So che è così perchè l'ho fatto in diverse occasioni. E' il delitto perfetto.

Soluzioni di sicurezza

Il segnale della rete wireless si può proteggere mediante la **cifratura**. Infatti i produttori hanno dotato le schede wireless di un sistema di cifratura denominato *WEP*. Il guaio è che le schede vengono vendute con il WEP **disattivato**: sta all'utente attivarlo. Bella furbata. Non che serva a molto, comunque, perché il WEP, spacciato per ultrasicuro, **si "buca" in meno di un quarto d'ora**.

Questo non vuol dire che ci si debba mettere alla mercé del primo aspirante intruso che passa. C'è una serie di misure per ridurre notevolmente il rischio di intrusioni.

Cambio dell'indirizzo IP dell'access point

Gli access point hanno di solito un indirizzo IP predefinito in fabbrica. Gli intrusi conoscono questi indirizzi IP standardizzati e pertanto possono andare a colpo sicuro nel cercare di accedere al vostro access point. Per questo **conviene cambiare l'indirizzo IP dell'access point.**

Controllo del MAC address

Ogni scheda di rete (wireless o meno) ha un proprio "numero di serie", che si chiama *MAC address*. Gli access point possono essere impostati in modo da accettare connessioni soltanto dalle schede che hanno un certo MAC address. Questo rende molto difficile all'intruso penetrare nella rete, perché deve prima scoprire uno dei MAC address autorizzati. Non è impossibile, ma è una scocciatura che scoraggia buona parte degli aggressori.

Pertanto conviene assolutamente **attivare il controllo del MAC address**.

Niente DHCP

Il DHCP è un sistema che semplifica la gestione di una rete assegnando automaticamente un indirizzo IP a ogni macchina che si collega alla rete. Questo è comodo in un ambiente cablato, ma è **pericoloso** in un ambiente wireless, perché assegnerebbe automaticamente un indirizzo IP anche a un intruso.

Bisogna quindi **disabilitare il DHCP** sull'access point e assegnare manualmente gli indirizzi alle singole schede wireless.

Tenete presente, comunque, che un intruso abbastanza furbo è in grado di aggirare questo ostacolo (gli basta indovinare la gamma di indirizzi IP che usate, tipicamente *192.168.0.**). Ma è proprio questo il concetto: creare una serie di ostacoli che singolarmente sono superabili, ma

cumulativamente sono una tale pena che l'intruso cambia aria.

Cambio dell'SSID

La rete wireless ha un suo identificativo, chiamato *SSID,* che le schede wireless devono conoscere per potervisi collegare. Anche l'intruso ha bisogno di conoscerlo per fare il suo sporco mestiere. Il guaio è che **conoscerlo è facilissimo:** la maggior parte dei dispositivi wireless è impostato in fabbrica in modo da usare, come SSID, **il nome del fabbricante**. Altra bella furbata. Siccome i fabbricanti non sono poi tanti, è banale per l'intruso tentarli uno per uno.

Quindi un altro bastone da mettere tra le ruote dell'intruso è **cambiare l'SSID**, assegnandone uno poco intuitivo. Ricordate che dovete cambiare l'SSID su tutte le schede della rete e nell'access point, e che comunque l'SSID rimane intercettabile, anche se più faticosamente, quindi non usate come SSID una vostra password o altre informazioni delicate. Non usate come SSID il vostro nome o il nome della ditta.

WEP? Ma sì, male non fa

Il WEP è un colabrodo, ma nel suo piccolo è comunque **un ostacolo in più** da frapporre fra la rete e gli intrusi. Va quindi attivato **insieme a tutte le altre contromisure**, e al massimo livello possibile (di solito 128 bit), ma attenzione: **non si devono usare eventuali chiavi predefinite**.

Queste chiavi predefinite, infatti, sono uguali per tutti i dispositivi wireless dello stesso produttore e quindi sono conosciutissime. Se le usate, per l'intruso (che le conosce) è un gioco da ragazzi entrare.

Alcuni dispositivi wireless permettono di scegliere fra WEP facoltativo e WEP obbligatorio, ossia di accettare sia connessioni cifrate, sia connessioni non cifrate oppure accettare soltanto quelle cifrate. Se avete quest'opzione, **scegliete il WEP obbligatorio**, che rifiuterà tentativi di connessione da schede wireless senza WEP.

Spegnere quando non serve

Può sembrare un consiglio abbastanza banale, ma è una di quelle contromisure così ovvie che raramente vengono prese in considerazione: **spegnete la rete wireless quando non la state usando.** Se la rete wireless non è in funzione, l'intruso non ha modo di usarla e ha meno tempo per tentare di entrarvi quando è accesa.

Un esempio tipico è il mio caso: il portatile di solito se ne sta sulla scrivania, e in tal caso è collegato alla rete locale via cavo. La rete wireless è accesa soltanto quando prendo il portatile e vado in un'altra stanza o in giardino. Quando non uso il portatile, spengo la rete wireless (le altre macchine di casa sono cablate).

Questo ha anche il vantaggio secondario di ridurre la propria esposizione alle onde radio emesse da ogni dispositivo wireless. Non risulta alcuna prova seria del fatto che questi campi elettromagnetici siano nocivi, ma nel dubbio, se si possono evitare è meglio.

Condivisioni di Windows

Se usate Windows, vi conviene **mettere una password sulle risorse condivise**. Le password di condivisione di alcune versioni non patchate di Windows (95, 98 e ME, per esempio) sono "bucabili" abbastanza facilmente, come descritto in un mio articoletto, ma costituiscono comunque un ostacolo in più.

Sicurezza fisica

Questo è un aspetto regolarmente trascurato della sicurezza delle reti wireless. **E' importante fare in modo che il segnale radio esca il meno possibile dall'edificio.** Se non c'è segnale fuori dall'edificio, l'intruso non solo non ha nulla a cui attaccarsi: non può neppure sapere che avete una rete wireless.

Non è difficile bloccare il segnale radio quanto basta per renderlo inutilizzabile dall'esterno. La prima cosa da fare è **collocare l'access point al centro della zona da coprire** e **il più lontano possibile dai muri esterni**. La seconda è **schermare l'access point nelle direzioni che non vi interessa coprire.** Per esempio, se dovete collocare un access point vicino a un muro esterno, mettete un foglio metallico fra l'access point e il muro (anche vicino all'access point, a mo' di paravento): rifletterà il segnale radio e gli impedirà di dirigersi verso l'esterno dell'edificio.

Infine, **non dimenticate la terza dimensione.** Il segnale radio non si diffonde soltanto orizzontalmente, ma anche verticalmente. Chi abita o lavora al piano superiore o inferiore è lontano, in linea d'aria, solo pochi metri dal vostro access point, e quindi ne riceve benissimo il segnale. Anche qui, il rimedio è schermare, schermare, schermare.

Trucchi evoluti

Quello che ho descritto fin qui è un approccio di base alla sicurezza delle normali reti wireless domestiche, ma si può fare molto di più. Mi limito a un breve accenno:

- si può **separare la rete cablata dalla rete wireless**, interponendo fra le due reti un firewall hardware o software. Il firewall consente poi alle macchine wireless di accedere a quelle della rete cablata soltanto a determinate condizioni, che potete impostare a vostro piacimento: per esempio, potete permettere di accedere via wireless a Internet o al server Web della vostra rete cablata, ma non alle risorse condivise (dischi e stampanti).
- si può **usare una gamma di indirizzi IP non standard**. Normalmente, le reti locali usano gli indirizzi della gamma *192.168.1.x*, dove *x* è compreso fra 0 e 254 (ci sarebbe anche il 255, ma è riservato). L'intruso lo sa, e imposta la propria scheda wireless in modo da usare la medesima gamma. Se però voi usate un'altra gamma, l'intruso è spiazzato (non in eterno, ma quanto basta per rendergli la vita difficile). Attenzione: se la vostra rete locale è connessa a Internet, non potete usare una gamma di indirizzi qualsiasi, perché andreste in conflitto con gli indirizzi usati dal resto di Internet. Le alternative ammesse sono *192.168.x.x*, *10.x.x.x*, e da *172.16.0.0* a *172.31.255.255*.

Note

Lo standard 802.11g è diventato ufficiale il 12/6/2003, come segnala (The Register).

Esiste anche un'alternativa al WEP, chiamato *WPA (Wi-Fi Protected Access),* che dovrebbe offrire maggiore sicurezza sulle connessioni wireless. Da settembre 2003, tutti i dispositivi wireless che aspirano al marchio Wi-Fi devono rispettare gli standard WPA; i dispositivi già in commercio prima di quella data dovrebbero essere aggiornabili tramite l'installazione di nuovo *firmware*. Trovate maggiori dettagli presso http://www.wi-fi.org.

Domande frequenti

Paolo, ho un problema con il mio wifi, mi aiuti?

No. Mi spiace, non posso: fare queste cose senza essere sul posto è difficilissimo se non impossibile

e richiede un'infinità di tempo. Chiedete aiuto a qualcuno sul posto: a un amico esperto oppure a un tecnico informatico.

Devo collegare computer situati a due piani differenti e il segnale è debole

Lo spessore di muri e solai attenua molto il segnale radio. Vi servirebbe un dispositivo con un'antenna più sensibile. Purtroppo è difficile avere questi dati prima dell'acquisto, a meno di andare su apparecchi costosi dotati di antenna esterna.

Potete provare ad orientare l'antenna del trasmettitore in modo diverso, per esempio coricandola in modo che sia orizzontale o inclinata: di norma, infatti, questi apparecchi diffondono il segnale principalmente su un piano perpendicolare all'asse della loro antenna.

In alternativa, vi serve un altro modo di trasmettere il segnale. Ci sono degli apparecchi *powerline* o *a onde convogliate*, che usano la rete elettrica normale: basta infilarli nelle prese elettriche. Se sono sotto lo stesso contatore funzionano benissimo. Ne ho parlato per esempio in questo articolo.