PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 715 di lunedì 10 febbraio 2003

Wireless Lan, la sicurezza dell'insicurezza

A cura di Fabio Pietrosanti. Comincia a diffondersi ora in Italia la tecnologia di trasmissione dati senza fili WI-FI. La tecnologia offre livelli di protezione adeguati?

Comincia a diffondersi ora in Italia la tecnologia di trasmissione dati senza fili WI-FI, che significa connessione a 11MBit/s sui 2,4GHz se si utilizzano apparecchiature aderenti allo standard 802.11b e addiritttura 54 MBit/s su 5 GHz con il nuovissimo standard 802.11a; in sostanza si puo' finalmente parlare di connettivita' a larga banda ovunque ci si trovi.

L'attrattiva di tale tecnologia e' rappresentata dall'elevata comodita' di utilizzo unita a un abbattimento dei costi legati al cablaggio (che per alcune tipologie di applicazioni possono essere molto pesanti), inoltre il costo per un kit di collegamento wireless lan (access point e due schede pcmcia) si attesta attualmente intorno ai 350 Euro, una spesa alla portata anche del segmento di mercato SOHO.

Siamo quindi in linea con le previsioni fatte IDC che vedono in 24,6 milioni gli utenti mondiali di tale tecnologia nel 2004, e le proiezioni di Gartner Group che pronosticano la presenza di 38000 gateways wlan nel mondo nel 2006.

Sempre uno studio di Gartner Group indica che entro il 2002 ben il 30% delle imprese che avranno implementato soluzioni wireless lan lo avranno fatto senza prendere debitamente in considerazione le problematiche di sicurezza ad esse connesse (direttamente o indirettamente).

Uno scenario apocalittico? No, anzi forse si tratta di una valutazione ottimistica se si prendono in considerazione i risultati di uno studio effettuato nel cuore di Londra che ha evidenziato come su 5000 reti wireless rilevate, ben il 92% di esse fosse sprovvista di misure di sicurezza anche minimali.

Ci troviamo quindi alle prese con una diffusione capillare e rapidissima di questa tecnologia, ed occorre affrontare in modo proattivo i suoi aspetti di sicurezza, insiti nel protocollo 802.11 ma in parte legati anche alla configurazione degli apparati (access point in primo luogo), che vengono troppo spesso installati nella loro configurazione di base: di facile ed immediato utilizzo, che consente in pochi minuti di collegare senza fili i propri client dalla sala riunioni, dalla stanza di fianco e purtroppo anche dalla strada.

Nasce cosi' tra gli hacker americani, e si diffonde assieme alla tecnologia wifi a livello mondiale, la moda del "wardriving", che consiste nel girare in macchina per le vie della città muniti di portatile (o palmare), scheda wireless e antenne che sporgono dai finestrini, a caccia delle reti wireless sprotette.
In America è diventato famoso il progetto Netstumbler che si prefigge di giungere alla mappatura completa delle reti wifi presenti in tutti gli stati dell'unione.

Sebbene possa essere fastidioso che un hacker curioso e irrispettoso utilizzi la nostra connessione per navigare a scrocco dalla strada sotto il nostro ufficio, questo e' in effetti il problema minore perche' i veri rischi sono dovuti alle falle insite nello standard 802.11.
Bachi e falle del protocollo sono venuti allo scoperto e sono documentati a cura degli hacker curiosi e un po' goliardi che peroò hanno favorito sia la diffusione della "moda" wireless che la focalizzazione sugli aspetti di sicurezza correlati.

Il primo meccanismo di sicurezza creato per proteggere il Wi-Fi dalle intercettazioni e garantire l'accesso alla rete ai soli utenti autorizzati è il WEP (Wired Equivalent Privacy) basato sulla crittografia a chiave simmetrica, con chiave che può essere di

lunghezza 40 o 128 bit.
In entrambe le varianti, la chiave può essere ricavata qualora sia stata acquisita, mediante l'utilizzo di uno sniffer wireless, una sufficiente quantità di dati.
Un altro metodo per aumentare la sicurezza delle reti wifi concedendo accesso solo agli utenti autorizzati è il cosidetto "filtro sui mac address" (ricordiamo che i mac address sono gli indirizzi fisici delle schede di rete), mediante il quale viene mantenuta una tabella delle schede wireless, identificate attraverso appunto il mac address, che possono associarsi all'access point protetto.
Purtroppo anche questo mezzo di protezione ha avuto vita breve, infatti è possibile falsificare con facilità il mac address di una scheda.

Ecco quindi che l'IEEE (Institute of Electrical and Electronics Engineers) responsabile per la definizione dello standard 802.11, rilascia l'802.11x, un nuovo meccanismo di autenticazione per l'802.11b che consente di basare l'accesso alla rete su credenziali decisamente piu' forti del WEP, autenticando
l'utente o attraverso la canonica accoppiata username e password (EAP-MD5) o tramite certificati digitali (EAP-TSL) il cui supporto e' gia' incluso in Windows XP, nonostante sia embedded nei driver dei rispettivi vendor per
tutti gli altri sistemi operativi (Linux incluso ovviamente) .

A questo punto sembrava che il discorso sicurezza degli accessi per il fiwi fosse partita chiusa, ma ecco che dall'universita' del Maryland arriva l'ennesimo smacco per l'IEEE.
Due ricercatori infatti pubblicano una dettagliata analisi di vulnerabilita' del nuovo standard dimostrando la fattibilita' di attacchi "man in the middle" e di "session hijacking" oltre a innumerevoli possibilita' di effettuare Denial Of Service al fine di rendere inutilizzabile l'intera rete wireless oggetto di attacco.

Concludendo non ritengo che gli standard attuali possano garantire livelli di protezione adeguati e quindi consiglio vivamente di considerare almeno i seguenti aspetti se si vuole a tutti i costi implementare una rete wireless:

-Considerare la rete come untrusted e posizionarla in una interfaccia dedicata del firewall.Questa deve avere lo stesso livello di fiducia di un utente collegato in dialup dalla corea.

-Non fidarsi del WEP, utilizzare quindi per tutte le informazioni sensibili connessioni cifratein SSL, e-mail con PGP e quant'altri strumenti di protezione della privacy .Alternativamente e' possibile utilizzare una VPN IPSec per raggiungere dalla rete wireless l'internal networkaziendale.

-Non usare SSID (gli identificativi della rete) con nomi che possano consentire a un wardriver di identificare che la rete appena scoperta in quella via e' proprio la vostra .

-Usare i filtri sui Mac address mantenendo una lista aggiornata delle sole schede abilitate

-Cambiare le chiavi WEP di default e ove possibile usare i nuovi meccanismi di autenticazione basati su EAP

-Disabilitare i Beacon Packets se si dispone di un singolo Access Point. I Beacon Packets sono segnali che vengono inviati ogni pochi millisecondi dagli access point per consentirne il discovery da parte dei client in modo automatico (e quindi anche da parte di un attaccante)

-Posizionare gli access point piu' vicino possibile alle facciate interne degli uffici, lontani dalle finestree, ove possibile, utilizzare antenne direzionali al fine di non irradiare con le microonde anche la strada

-Effettuare regolari assessment wireless delle proprie reti al fine di individuare eventuali access point non autorizzati.

Articolo a cura di Fabio Pietrosanti.