SICUREZZA DELLE RETI WIRELESS: ANALISI DEI RISCHI E DELLE CONTROMISURE

Roberto Bernazzani (roberto.bernazzani@unicatt.it)
CRATOS (http://cratos.pc.unicatt.it) - Università Cattolica del Sacro Cuore di Piacenza

Il fenomeno WLAN

Le Wireless LAN (WLAN) rappresentano una delle tecnologie emergenti degli ultimi tempi. Questo dato, oltre che facilmente percepibile dagli addetti ai lavori, è confermato anche da numerosi studi; tra le analisi più autorevoli possiamo citare quella condotta da IDC, secondo la quale il valore complessivo delle vendite di componenti hardware di reti wireless era di 1,45 miliardi di dollari nel 2001, anno in cui le WLAN hanno iniziato a prendere piede, e raggiungerà i 3,72 miliardi di dollari nel 2006.
Le ragioni alla base di questo boom stanno essenzialmente nella convenienza e relativa semplicità ed economicità di realizzazione di questo tipo di reti. Si tratta, in altri termini, di una tecnologia che può essere utilizzata indistintamente in ambiente enterprise, SOHO (Small Office/Home Office) e home senza sostenere costi particolarmente elevati e anche non possedendo competenze specifiche nel campo del networking.
Se da un lato questo è da ritenersi un fenomeno positivo in quanto ha consentito a molti di godere della mobilità garantita dalle WLAN, d'altro canto ha avuto come risultato non voluto quello di far nascere un numero elevato di reti gestite da persone spesso non dotate delle competenze necessarie per comprendere la delicatezza del problema della sicurezza in reti di questo tipo.

Il lato oscuro: la sicurezza

L'aspetto della sicurezza, cruciale per qualsiasi tipo di rete, diventa determinante trattando di reti wireless per le quali possiamo individuare i seguenti rischi:

- violazione dell'integrità, autenticità e riservatezza dei dati che transitano sulla rete, rischi tipici anche delle reti tradizionali;
- che la rete wireless diventi, una volta violata, un ponte per l'accesso alla rete wired, vanificando in tal modo le (costose) misure solitamente adottate per rendere sicura quest'ultima;
- che la nostra rete si trasformi in "hotspot pubblico involontario", consentendo ad altri di sfruttare indebitamente la nostra rete per accedere ad Internet.

Quest'ultimo è un fenomeno noto con il termine di "war driving" e consiste nell'individuare WLAN non adeguatamente protette e sfruttarne la connessione per la navigazione Internet o, nei casi peggiori, per accedere a dati privati o per sferrare attacchi informatici verso altri obiettivi (c.d. bounce attack).
Numerose statistiche dimostrano che le reti non protette in alcun modo e in quanto tali bersaglio preferito delle attività di war driving rappresentano addirittura l'80-90% delle WLAN private.
Si tratta di dati, a parere di chi scrive, sufficienti a far comprendere come chiunque decida di adottare una WLAN debba anche preoccuparsi di predisporre le opportune misure di sicurezza.

Le contromisure

Le soluzioni di security applicabili ad una WLAN possono essere divise in due macro-categorie in base alla finalità che si prefiggono: da un lato abbiamo gli interventi che mirano ad impedire che il segnale irradiato dai nostri access point (AP) venga captato all'esterno dell'area che intendiamo coprire; dall'altro le soluzioni che puntano a predisporre quelle barriere che ostacolino accessi non autorizzati.

Gli interventi del primo tipo si concretizzano nel disporre gli AP e nel scegliere le antenne di irradiazione del segnale in modo che quest'ultimo venga convogliato solo dove necessario, ossia all'interno dell'area che si intende dotare di rete senza fili.
E' evidente come si tratti di una pratica complessa, dal momento che le onde radio, per loro natura, sono difficilmente convogliabili in una direzione voluta. Conviene pertanto rivolgersi a soggetti specializzati nella conduzione delle cosiddette "site survey", quell'attività che, dopo un attento studio dell'area da coprire, genera un progetto di rete in grado di raggiungere l'obiettivo enunciato.

Analizziamo ora gli interventi che mirano a impedire che soggetti in grado di captare il segnale emesso dagli AP di nostra proprietà possano utilizzarlo per accedere alla rete Internet, dando vita al fenomeno che abbiamo sopra definito war driving.
Per evitare questa pratica sono sufficienti solo pochi accorgimenti che tuttavia, come dimostrano le statistiche richiamate in precedenza, non vengono seguiti dalla maggior parte di titolari di reti wireless.
Il primo di questi interventi ha per oggetto il SSID (Service Set Identifier), il nome che viene associato ad una WLAN configurandolo in ogni access point che la compone. Un minimo livello di sicurezza richiede di cambiare il valore di default assegnato dal produttore degli access point e di disabilitare il c.d. SSID broadcasting, ovvero la funzione attraverso la quale un AP trasmette il proprio SSID (e di conseguenza fornisce l'accesso alla rete) a tutti i client in grado di captare il segnale dotati di una scheda wireless e di un sistema operativo che supporta questa procedura (es. Windows XP).
Attraverso queste prime semplici accortezze l'accesso alla rete wireless sarà consentito esclusivamente a chi conosce l'SSID della rete, ponendo una prima barriera all'ingresso.
Un altro accorgimento da adottare consiste nel disabilitare sugli AP predisposti a questo il protocollo DHCP (Dynamic Host Configuration Protocol), il quale consente agli AP di attribuire in modo automatico un indirizzo IP ai terminali che ne fanno richiesta. Se da un lato il ricorso a tale protocollo semplifica notevolmente il compito degli amministratori di rete, dall'altro riduce drasticamente la possibilità di monitorare quali wireless terminal accedono alla propria rete.
L'amministratore oculato dovrà quindi disabilitare il DHCP sui proprio AP e procedere alla configurazione manuale dell'indirizzo IP sui client ai quali intende fornire l'accesso wireless.
Un metodo ancora più sicuro per evitare che terminali non autorizzati accedano alla nostra rete wireless è il filtraggio degli indirizzi MAC (Medium Access Control). Il MAC è un indirizzo che caratterizza in modo univoco e permanente qualsiasi scheda di rete (NIC), sia wired che wireless. Il MAC filtering consiste nel fare in modo che un AP garantisca l'accesso solo alle NIC (e quindi ai terminali) il cui MAC è contenuto in un'apposita lista che il system administrator avrà provveduto a stilare.

Le misure di sicurezza analizzate finora, pur avendo il vantaggio di essere semplici ed efficaci allo stesso tempo, sono insufficienti a garantire un buon livello di sicurezza dal momento che un hacker di medie capacità, grazie anche ad appositi tools facilmente reperibili sulla rete, può essere in grado di aggirare queste protezioni.
Sorge dunque la necessità di ricorrere ad un apposito protocollo che, attraverso meccanismi di crittografia, consenta di garantire integrità, autenticità e riservatezza dei dati che sulla rete wireless viaggiano. Nell'ambito delle reti basate sullo standard 802.11, il protocollo originariamente dedicato a questo scopo prende il nome di WEP (Wired Equivalent Privacy).

Il protocollo WEP
WEP è il protocollo che si occupa di cifrare il traffico di dati trasmesso tra AP e client in entrambe le direzioni.

A questo scopo WEP utilizza l'algoritmo di cifratura simmetrico RC4 con una lunghezza complessiva delle chiavi che va dai 64 bit della versione base di WEP ai 256 bit di versioni di WEP proprietarie, cioè sviluppate dai produttori di hardware per reti wireless.
Le chiavi sono statiche, nel senso che la stessa chiave viene utilizzata da tutti i soggetti connessi alla rete wireless almeno fino a quando non verrà cambiata manualmente.

Analizzando le caratteristiche del WEP risulta evidente come questa soluzione di security sia affetta da numerosi difetti; citiamo i principali:

- le chiavi non sono sufficientemente lunghe, specialmente nella versione "base" di WEP nella quale la chiave è di soli 64 bit; si tratta di un problema grave se consideriamo una delle regole base della crittografia secondo la quale la probabilità di decifrare un messaggio è inversamente proporzionale alla lunghezza della chiave utilizzata per cifrarlo;
- non supporta le chiavi dinamiche: la chiave rimane invariata fino a che non viene cambiata manualmente dall'amministratore di rete in tutti gli AP ed i client; è chiaro che un compito di questo genere diventa molto oneroso in reti di medie dimensioni e addirittura proibitivo in reti enterprise di grandi dimensioni;
- non supporta l'autenticazione degli utenti, mentre è garantita un'autenticazione dei device molto debole essendo basata sulla chiave: tutti i dispositivi che possiedono la chiave comune sono automaticamente autorizzati ad accedere alla rete wireless. Questo è il motivo per il quale questo tipo di autenticazione viene spesso integrata con la pratica del MAC filtering;
- cripta il frame ma non l'header dei pacchetti TCP/IP scambiati tra AP e wireless terminal: ciò significa che un hacker che si pone in ascolto del traffico wireless può essere in grado di ottenere, in un tempo relativamente breve, sufficienti informazioni sulla chiave per accedere alla rete.

Dall'analisi di questi difetti risulta chiaro come il WEP sia assolutamente insufficiente a garantire un adeguato livello di sicurezza in una WLAN, come d'altronde è stato dimostrato da diversi studi condotti da università, enti di ricerca ed aziende specializzate in sicurezza delle reti.
Questa affermazione deve tuttavia essere interpretata nel modo corretto. Affermare che il WEP non garantisce un sufficiente livello di sicurezza non significa sostenere la sua assoluta inutilità. I difetti che abbiamo elencato lo rendono vulnerabile agli attacchi portati da hacker dotati di competenze e capacità elaborative ben lontane da quelle dell'utente medio di Internet.
La pratica, più volte citata, del war driving non ha preso diffusione per il fatto che chiunque sia in grado di violare WEP, quanto piuttosto perché nessuna delle reti violate era stata protetta, cioè il WEP non era nemmeno stato attivato. Ciò significa che il fenomeno del war driving potrebbe essere drasticamente ridotto se solo gli amministratori delle reti avessero l'accortezza di attivare sugli AP e sui terminali il tanto criticato protocollo WEP.
Per spiegare meglio il concetto possiamo ricorrere ad una semplice quanto efficace metafora: tutti noi lasciamo normalmente la nostra auto aperta? Sicuramente no; sicuramente quando abbandoniamo la nostra auto ci assicuriamo di aver chiuso a chiave le portiere e, probabilmente, adottiamo anche altre misure di sicurezza come antifurti di ogni genere. Sappiamo che queste misure non danno la sicurezza assoluta che la nostra auto non verrà rubata, ma almeno terranno alla larga i ladri dilettanti.
Lo stesso vale per le reti wireless: WEP ha sicuramente numerosi difetti, tuttavia attivarlo non costa nulla, se non una riduzione della throughput, e tiene alla larga dalla nostra WLAN gran parte dei malintenzionati. Possiamo andare oltre affermando che la soluzione WEP può essere ritenuta sufficiente per le applicazioni che trattano dati non sensibili e in generale per l'ambiente SOHO.
Il mondo delle grandi aziende ha invece reagito all'inadeguatezza di WEP facendo pressioni sull'IEEE affinché sviluppasse il prima possibile un protocollo di sicurezza più evoluto. Il risultato è stato il rilascio, nell'Aprile 2003, del protocollo noto con il nome WPA (Wi-Fi Protected Access).

Il protocollo WPA
WPA è stato sviluppato con l'intento specifico di risolvere tutte o quasi le vulnerabilità di WEP. Si tratta di un sottoinsieme di un protocollo ancora più ampio, l'802.11i (noto anche con il termine di WPA2) che dovrebbe essere rilasciato nel primo quarto del 2004 e che conterrà una soluzione complessiva per la sicurezza delle WLAN.

WPA si distingue da WEP prevalentemente per i seguenti motivi:

- le chiavi hanno una lunghezza di 128 bit;
- le chiavi sono dinamiche, cioè sono diverse per ogni utente, per ogni sessione e per ogni pacchetto inviato;
- le chiavi vengono distribuite in modo automatico, non richiedendo nessun intervento manuale da parte dell'amministratore di rete;
- prevede un meccanismo di autenticazione degli utenti.

Nel dettaglio, WPA basa il proprio funzionamento su tre componenti fondamentali:

- TKIP (Temporal Key Integrity Protocol) come algoritmo di crittografia;
- 802.1X/EAP (Exstensible Authentication Protocol) come schema di autenticazione;
- MIC (Message Integrity Check) come strumento per garantire l'integrità dei messaggi scambiati.

Analizziamo separatamente, ma senza entrare nel dettaglio tecnico, ognuno di questi componenti.

TKIP utilizza chiavi a 128 bit e sostituisce le chiavi statiche di WEP con chiavi dinamicamente generate e distribuite dal server di autenticazione. A questo scopo, TKIP si serve del framework di autenticazione 802.1X/EAP. Quest'ultimo prevede la presenza all'interno della rete di un server di autenticazione il quale, dopo aver verificato le credenziali dell'utente che tenta di connettersi alla rete wireless, genera una "master key" che TKIP distribuisce a tutti gli AP ed ai client.
La master key è utilizzata per generare, attraverso una complessa funzione matematica, le chiavi che verranno a loro volta sfruttate per cifrare i singoli pacchetti di dati trasmessi sulla rete Wi-Fi. Si ottiene in tale modo quel processo di generazione dinamica delle chiavi che permette a WPA di raggiungere una prevedibilità delle chiavi decisamente inferiore rispetto a WEP.
L'ultimo componente di WPA che ci resta da analizzare è il MIC, il quale si occupa di applicare una complessa funzione matematica al messaggio scambiato. Questa operazione viene compiuta sia dal mittente che dal ricevente: se il MIC calcolato da entrambi non coincide, significa che il messaggio è stato modificato nel transito e quindi viene scartato ed inviato nuovamente. Il tutto avviene ovviamente in modo trasparente all'utente finale.

Abbiamo esaminato a grandi linee il funzionamento di WPA, dando finora per scontato che la rete wireless fosse connessa ad un server di autenticazione. Questa situazione è verosimile in ambiente aziendale, mentre in ambiente SOHO si tratta di uno scenario piuttosto improbabile. I creatori di WPA hanno affrontato questo problema prevedendo due modalità di funzionamento del protocollo: una per l'ambiente enterprise ed una per quello SOHO. Analizziamo le due modalità distintamente.

In aziende di medio-grandi dimensioni, WPA si basa sull'autenticazione 802.1X utilizzando una delle applicazioni del protocollo EAP (Exstensible Authentication Protocol). Quest'ultimo è in grado di autenticare gli utenti in base alla presentazione di credenziali sotto forma di certificati digitali, coppia di username e password, smart card ed altre.
Quando un utente chiede di avere accesso alla rete wireless, il proprio client invia le credenziali al server di autenticazione attraverso un access point. Se il server accetta le credenziali dell'utente, TKIP invia la master key sia al dispositivo client che a tutti gli AP. Seguirà un processo detto di

“four-way handshake”, durante il quale client ed AP si autenticano a vicenda ed installano la chiave inviata loro dal server di autenticazione.

In ambiente SOHO ed a maggior ragione in quello home, dove tipicamente mancano le competenze e le risorse economiche per installare e mantenere un server centrale di autenticazione, WPA funziona in modo leggermente diverso utilizzando una “pre-shared key” (PSK).
Il nome di chiave “pre-condivisa” dipende dal fatto che essa deve essere settata manualmente su tutti gli AP ed i client e successivamente verrà utilizzata per la loro autenticazione. Si passa dunque da un’autenticazione degli utenti del caso precedente ad una (meno sicura) autenticazione dei device.

Se volessimo riassumere schematicamente le caratteristiche del protocollo WPA potremmo affermare che esso è:

- un upgrade software/firmware da effettuare sugli AP e sulle NIC wireless;
- non costoso, sia in termini economici che di tempo necessario per la sua implementazione;
- retrocompatibile con WPE e compatibile con il futuro WPA2;
- compatibile con i dispositivi prodotti da qualunque vendor certificati dalla Wi-Fi Alliance;
- adatto per reti di tutte le dimensioni: enterprise, SOHO e home.

Il futuro: il protocollo WPA2
Come accennato in precedenza, WPA rappresenta un’anticipazione del protocollo 802.11i che IEEE, in collaborazione con la Wi-Fi Alliance, sta sviluppando ed intende rilasciare a breve.
Il funzionamento di 802.11i sarà sostanzialmente lo stesso di WPA (da qui il nome di WPA2) con una sola novità di rilievo: un nuovo schema crittografico noto con l’acronimo AES (Advanced Encryption Standard) che utilizzerà chiavi di 128, 192 o 256 bit in base alla versione scelta, aumentando così ulteriormente il livello di protezione.

Conclusioni
In questo documento si è voluto sottolineare come il valore aggiunto fornito da una wireless LAN sia strettamente correlato al proprio livello di sicurezza. In altri termini, una WLAN viene totalmente svuotata di valore se è vulnerabile dal lato della sicurezza e quindi potenzialmente attaccabile dall’esterno.
Sorge dunque la necessità di proteggere la nostra rete con le modalità descritte in precedenza: dalla semplice disabilitazione del SSID broadcasting, all’adozione del protocollo WEP, certamente “bucabile” ma adatto a realtà di piccole dimensioni, fino ad arrivare al più completo WPA e al nascituro WPA2.
L’adozione di queste misure di sicurezza si rivelerà tuttavia inutile se non sarà accompagnata da una vera *security policy* compresa e applicata da tutti coloro che utilizzano la rete aziendale.
Se potessimo ipoteticamente stimare con un valore l’attenzione alla sicurezza posta dai vari utenti di una rete, potremmo affermare che la sicurezza globale del sistema non è data dalla media di tali valori, bensì dal valore più basso assegnato.
In termini concreti, i nostri sforzi per rendere sicura la rete saranno vanificati se, ad esempio, un dipendente mantiene per pigrizia e comodità la propria password uguale allo username. Un potenziale attaccante sfrutterà di certo questa vulnerabilità per avere accesso alla nostra rete, rendendo inutile ogni altra misura di security.

FONTI:

AA.VV., “Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks”, Wi-Fi Alliance, http://www.weca.net/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf , novembre 2003

AA.VV., “Cisco Wireless Security”, Cisco Systems, http://searchnetworking.techtarget.com/searchNetworking/Downloads/chapter08.pdf, novembre 2003

Geier J., “802.11 WEP: Concepts and Vulnerabilities”, http://www.wi-fiplanet.com/tutorials/article.php/1368661, ottobre 2003

Miller S.S., Wi-Fi Security, 2003, McGraw-Hill, London

Moran J., “Wireless Home Networking, Part III – Wi-Fi Security”, http://www.wi-fiplanet.com/tutorials/article.php/1495811, ottobre 2003

Simon M., “Wireless Security Notes: A Brief Analysis of Risks”, Fluke Networks white papers

Stallings W., Comunicazioni e reti wireless, 2003, McGraw-Hill, Milano