

### Sicurezza senza fili, un grande problema per piccole reti (15 Marzo 2004 - Extra Edition)

*Wireless LAN e PMI*

*Tra mancanza di risorse e tecnologie da conoscere, il tema della security wireless impegna più le piccole che le grandi aziende*

Il vostro portatile rileva immediatamente la copertura della Wireless LAN e presenta la finestra di login. Entrate nella rete con l'account di ospite, navigate fra i server, consultate i documenti e dopo un po' decidete di chiudere la connessione. Tutto molto semplice e immediato, proprio come sostengono i fautori delle LAN senza fili. L'ideale? Sembrerebbe, tranne per un piccolo problema: la rete in cui siete entrati non è la vostra e avrebbe dovuto bloccarvi immediatamente.

Episodi come questo si sono verificati con il diffondersi delle WLAN nelle piccole e medie realtà, in cui non ci sono sempre le competenze e il tempo per occuparsi di un problema - la sicurezza degli accessi "fisici" in rete - che le reti cablate non presentano quasi più. La questione è anche infrastrutturale: nelle aziende di dimensioni ridotte mancano quei componenti della sicurezza IT (VPN, server di autenticazione, policy complesse...) che invece sono diffusi nelle grandi imprese. Le PMI non potevano - e ancora non possono - investire in queste soluzioni, quindi hanno dovuto accontentarsi di un livello di security non sempre adeguato alle loro necessità.

#### Una maggiore attenzione

Molti vendor di apparati wireless dedicati al segmento SOHO/PMI vedono le funzioni di sicurezza come elemento opzionale, lasciandole inattive nelle configurazioni standard dei loro dispositivi. Dovrebbero essere gli utenti ad abilitarle secondo le proprie necessità, ma si è visto che gli utilizzatori meno tecnici non badano a questo aspetto e si ritrovano, seppure involontariamente, "aperti" ad accessi non autorizzati. Per evitare questo pericolo, anche i responsabili tecnici o gli amministratori di rete delle piccole e medie aziende devono accertarsi che siano garantite le componenti base della sicurezza di rete wireless e devono mantenersi aggiornati sull'evoluzione dei prodotti e delle tecnologie di sicurezza.

#### Prima e dopo Wep

Il protocollo WEP (Wired Equivalent Privacy) è uno di questi elementi base, anche se è ormai noto che il protocollo è vulnerabile agli attacchi di un hacker evoluto, per due ragioni: ripete abbastanza frequentemente i blocchi di dati usati nel processo di scrambling, che un hacker malevolo può raccogliere per decifrare il traffico, e non cambia automaticamente la chiave condivisa usata da un Access Point e da un gruppo di client, dando agli attaccanti più possibilità di "rompere" il codice. Ciononostante, il Wired Equivalent Privacy è un primo livello di protezione che va comunque abilitato ed è presente in tutti i dispositivi WLAN. Un IT manager deve anche seguire le sue evoluzioni, aggiornando - se serve - il firmware dei suoi dispositivi non appena possibile.

Il primo e più evidente passo in avanti rispetto al WEP è la specifica WPA (Wi-Fi Protected Access), una versione ridotta di ciò che sarà il protocollo 802.11i e destinata proprio al mondo SOHO/PMI. WPA migliora le funzioni di cifratura di WEP perché adotta il protocollo TKIP (Temporal Key Integrity Protocol), che rende più complesso decifrare i dati scambiati tra client e Access Point. Rende inoltre più sicuro il processo di autenticazione dell'utente perché aderisce allo standard 802.1x e utilizza il protocollo EAP (Extensible Authentication Protocol).

In linea teorica, l'autenticazione dovrebbe avvenire utilizzando un server Radius anche nel "modello" WPA, ma nelle piccole-medie imprese è difficile che ci sia un sistema Radius. WPA aggira il problema utilizzando una password condivisa che serve a identificare fra loro tutti i client e l'Access Point. Dopo questa autenticazione si attivano le funzioni di cifratura evoluta di WPA, il cui uso dovrebbe essere semplificato dal fatto che la specifica è integrata in Windows XP.

### Verso 802.11i e oltre

Il dopo-WPA è rappresentato dallo standard 802.11i, che però richiederà aggiornamenti hardware e non solo upgrade software. Lo standard raggiunge livelli più elevati di sicurezza sfruttando la cifratura AES (Advanced Encryption Standard) a 128 bit, che richiede una potenza elaborativa piuttosto consistente. Per questo motivo non è garantito che tutti gli Access Point attualmente in commercio saranno in grado di gestire l'802.11i. Un utente, in poche parole, deve tenere presente che il passaggio alla cifratura AES potrebbe comportare nuovi investimenti e deve regolarsi di conseguenza: verificare se un livello di security più elevato è veramente necessario e, se lo è, capire con il proprio fornitore come far evolvere la sua rete e con che costi.

Con il passaggio allo standard 802.11i si porrà nuovamente il problema dell'interoperabilità fra apparati: i test e le certificazioni saranno compito, come già ora, soprattutto della Wi-Fi Alliance e degli ICSA Labs.

### Standard in conflitto?

Di possibili problemi di interoperabilità si parla anche a proposito di PEAP (Protected EAP), una tecnologia che nasce dalla collaborazione fra Cisco, Microsoft e RSA Security. Si basa sulla creazione, tra client e server, di un tunnel in cui transitano le credenziali dell'utente, ad esempio la password, senza la necessità di avere un certificato digitale sul client. L'idea originaria era integrare PEAP nei dispositivi di rete, nel software client, nei server di autenticazione e nei directory service, in modo da gestire tutto il ciclo di autenticazione di un utente che accede alla rete wireless. Le tre aziende avevano presentato la specifica PEAP all'IETF per farne uno standard, ma Cisco e Microsoft si sono poi trovate in contrasto sull'implementazione di PEAP e ora ciascuna supportano una versione separata della tecnologia.

Secondo Cisco, l'implementazione di PEAP fatta da Microsoft è troppo legata ai suoi prodotti: funziona benissimo con Active Directory e con i domini NT, ma non con LDAP, le directory Novell e con altri approcci

non Microsoft. Opposta la versione di Microsoft, secondo cui l'implementazione PEAP di Cisco non è uno standard aperto.

Altra tecnologia Cisco all'esame dell'Internet Engineering Task Force è EAP FAST (Extensible Authentication Protocol Flexible Authentication via Secure Tunneling). Il protocollo dovrebbe rappresentare un'alternativa a PEAP e utilizza lo stesso approccio con tunnel cifrati, ma l'autenticazione si basa su credenziali che il client di rete scarica automaticamente da un server sicuro.

### Il glossario della sicurezza WLAN

802.1X - E' lo standard IEEE 802.11 per l'autenticazione: supporta diversi modi di autenticazione, tra cui Radius, che possono essere usati in reti wireless e cablate.

802.11i - Il gruppo di standardizzazione IEEE che si è dedicato a risolvere i "buchi" di sicurezza percepiti in 802.1X e WEP.

LEAP - Lightweight Extensible Authentication Protocol: le estensioni proprietarie a 802.1X che Cisco ha usato per lo scambio dei dati di autenticazione tra gli Access Point Aironet e il Cisco Secure Access Control Server.

PEAP - Protected Extensible Authentication Protocol: sviluppato da Microsoft, Cisco e RSA Security, è ora un draft IETF. PEAP usa un metodo di tunneling.

TKIP - Temporal Key Integrity Protocol: sviluppato dal comitato IEEE 802.11i come miglioramento del WEP.

TTLS - Tunneled Transport Layer Security: sviluppato da Funk Software e Certicom, ora è un draft IETF alternativo a PEAP.

WEP - Wired Equivalent Privacy, standard di cifratura wireless sviluppato dal comitato IEEE 802.11.

### Altre strade possibili

Lo scenario è in effetti ancora più complesso. PEAP ed EAP FAST sono nati anche come risposta a una vulnerabilità di un precedente sistema proprietario Cisco: LEAP (Lightweight EAP). Esso poteva essere aggirato catturando parte di una sessione di autenticazione e poi cercando di indovinare la password utente consultando un database di quelle più comuni. LEAP però non è fuori gioco, dato che Cisco continua a consigliarlo per le reti wireless che non hanno bisogno di livelli elevati di sicurezza.

Tra gli standard potenziali c'è anche TTLS (Tunneled Transport Layer Security): disegnato da Certicom e Funk Software, è molto simile a PEAP nel suo utilizzo di tunnel cifrati, ma i suoi sostenitori lo giudicano più flessibile perché si integra con più protocolli di cifratura.