Suggerimenti per gestire la sicurezza nelle wireless LAN

In questa prima parte l'autore offre una serie di consigli utili ed un sintetico riassunto su tutto quello che si deve sapere su WEP. Per gli interessati, la possibilità di approfondire gratuitamente la materia attraverso un draft su PPPoE ed un e-book di ben 140 pagine intitolato "Sicurezza nelle Wireless LAN"

di Giuseppe Paternò

La necessità di mobilità e di copertura in ambienti aperti o difficili da raggiungere tramite cavi (es.: ospedali, aeroporti o palazzi antichi) hanno favorito la diffusione delle tecnologie wireless, una delle quali è proprio IEEE 802.11, detta anche Wireless Ethernet o Wi-Fi (Wireless Fidelity). Stiamo assistendo ad un aumento notevole della loro diffusione negli ultimi mesi presso le aziende e utenze private, data la facilità di installazione, le sue prestazioni (11Mbps o 54Mbps) e la sua flessibilità con costi ridotti. Esistono però dei rischi di sicurezza collegati all'uso delle tecnologie wireless. Alcuni di questi rischi esistono anche nelle reti di tipo tradizionale, ma vengono esasperati dalla tipologia di collegamento senza fili. La trasmissione attraverso onde radio non è confinabile ad uno spazio ben definito, quale può essere quello della trasmissione via cavo: come per l'ascolto di una radio, è possibile per un potenziale intruso avvicinarsi all'esterno del palazzo e "captare" le onde radio. Così come per le reti cablate, attraverso appositi strumenti, è possibile visualizzare i dati che vengono ricevuti e inviati, rendendo disponibile all'eventuale intruso preziose informazioni quali utenze e password, e, in alcune situazioni, addirittura accedere ai database e corrompere i dati.

È bene essere consci di un fattore di rischio molto importante, ma troppo spesso sottovalutato, ovvero che un eventuale intruso non abbia nessun interesse a prendere informazioni sulla rete attaccata, ma voglia utilizzare la rete vittima come "ponte" per attaccare una terza entità, con cui spesso si ha una relazione di fiducia. L'intruso sarà solito usare il "ponte" per offuscare le proprie tracce: da un punto di vista puramente giuridico, l'amministratore della rete wireless violata sarà formalmente responsabile dell'atto di pirateria informatica nei confronti della terza entità, fino a quando le autorità giudiziali non troveranno prova dell'avvenuta intrusione.

Il WEP e la sua insicurezza

La Wireless Ethernet dispone di un sistema di sicurezza che viene chiamato Wired Equivalent Privacy, detto comunemente WEP. Questa specifica, nata per garantire la privacy delle utenze, è basata però su di un sistema di crittografia debole che si è rilevata controproducente: attraverso un'analisi probabilistica di una piccola quantità di dati cifrati, è possibile risalire alla chiave di crittografia e pertanto accedere alla rete. Il rischio principale è che WEP dà una falsa sensazione di sicurezza agli utenti, conseguentemente i dati non cifrati possono essere facilmente catturati da intrusi.

Recenti studi (il più importante dei quali è "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP" di Stubblefield, Ioannidis e Rubin) hanno dimostrato che si può ricavare la chiave di cifratura WEP dall'osservazione del traffico di rete. In dettaglio, la chiave WEP (da 40 o 104 bit) viene concatenata inizialmente ad un vettore di inizializzazione (IV) di 24 bit per formare una stringa da 64 o 128 bit, che sarà data in input all algoritmo RC4 per formare la chiave di cifratura dei dati. Parallelamente i dati da criptare vengono scomposti in blocchi e concatenati con i bit di checksum (ICV) per formare una stringa della stessa lunghezza della chiave RC4. Infine viene effettuato lo XOR tra la chiave RC4 e i blocchi dati ottenendo il testo cifrato, a cui viene aggiunto il vettore di inizializzazione.

Proprio l'uso di quest'ultimo ha determinato la maggior debolezza del protocollo WEP: infatti l'algoritmo RC4 risulta vulnerabile se vengono utilizzate le chiavi più di una volta. Questo è esattamente quello che accade con il WEP: il vettore di inizializzazione è lungo soltanto 24 bit, quindi ammette uno spazio di 16777216 combinazioni (2^24). In aggiunta, il protocollo WEP prevede la reinizializzazione del IV ogni qual volta si origini una collisione nella trasmissione dei pacchetti dati. In una rete di medie dimensioni e con un discreto volume di traffico sono sufficienti pochi minuti affinché vengano riutilizzate le stesse chiavi di cifratura. Tramite meccanismi di criptoanalisi differenziata si può risalire in poco tempo alla chiave WEP e decifrare tutto il traffico tramite la chiave individuata. Oltre alle debolezze intrinseche del WEP, bisogna riscontrare che lo standard IEEE 802.11 non fornisce alcun meccanismo sulla custodia e configurazione delle chiavi WEP. Nei casi peggiori alcuni produttori hanno optato nel conservare la chiave WEP nel registro dei sistemi Windows o in un file di testo in Linux, completamente in chiaro; solo in pochi produttori hanno custodiscono la chiave WEP nel firmware della scheda di rete. È da

sottolineare che la configurazione delle chiavi WEP è manuale, con un notevole sforzo da parte degli amministratori di sistema che sono costretti ad impostare la chiave WEP su ogni singola stazione wireless e punto di accesso. Questo implica una scarsa variazione nel tempo delle chiavi WEP, che è una delle cause principali di penetrazione nei sistemi per i motivi sopra discussi.

Il meccanismo WEP, quindi, dà una falsa sensazione di sicurezza all'utente finale, pertanto tutti i dati non criptati, ad esempio attraverso SSL, possono essere facilmente intercettati da eventuali intrusi.

Hardening degli Access Point

La configurazione standard delle case produttrici sono uno dei maggiori fattori di rischio per la sicurezza delle Wireless LAN. Gli amministratori di rete, molto spesso per mancanza di tempo, non configurano gli Access Point in maniera dettagliata: le password degli Access Point, gli SSID e le chiavi WEP di default sono pertanto facile preda di potenziali aggressori.

Una corretta configurazione degli apparati è un buon inizio per proteggere la rete wireless. Grazie ad alcuni semplici accorgimenti, è possibile "sviare" un eventuale intruso nascondendo dettagli preziosi e rendendo più difficile l'identificazione della rete su cui si sta collegando. Vediamone brevemente alcuni

- Cambiare il Service Set Identifier (SSID) di default.

- Utilizzare SSID non descrittivi facilita il compito di un eventuale intruso nell'individuare luoghi o aziende. Si consiglia di utilizzare nomi anonimi come "AC01MLX" o "MI3AP".

- Disabilitare il Broadcast SSID. Gli AP mandano ad intervalli regolari Beacon Frames per la sincronizzazione con i client, i quali contengono il SSID. Queste frames servono ai client per configurarsi automaticamente la rete di accesso, ma servono anche a potenziali aggressori durante la ricerca delle reti wireless. È auspicabile disabilitare il Broadcast SSID qualora l'AP supporti questa opzione. Il client dovrà essere configurato manualmente con il SSID corretto per poter accedere alla rete.

- Cambiare le password di default degli Access Point.

- Aggiornare il firmware. Nella scelta di un Access Point, è preferibile orientarsi verso un apparato che abbia la possibilità di aggiornare il suo firmware e allinearlo all'ultimo livello.

- Chiavi WEP. Anche se è stato dimostrato che WEP non è adeguato a proteggere una rete wireless, rappresenta comunque un deterrente per gli intrusi occasionali. Bisogna prima catturare dai 100 Mb a 1 Gb di traffico per provare a ricavare la chiave WEP, pertanto l'aggressore deve essere ben motivato per tentare l'intrusione. Cambiare spesso le chiavi WEP di crittografia sugli AP fa in modo che una rete compromessa, non lo sia a tempo indeterminato.

- Abilitare il MAC filtering. Molti produttori includono nei loro Access Point la possibilità di abilitare filtrare le schede di rete che vi accedono tramite il loro MAC address. È necessario però comprendere che il MAC address di una scheda può essere facilmente cambiato, pertanto il MAC filtering non può essere usato come solo metodo di protezione.

- Spegnere l'AP quando non serve. Sembra banale, ma gli intrusi agiscono solitamente durante la notte e il fine settimana, pertanto sarebbe interessante collegare gli Access Point ad un timer, in modo da spegnerli quando non vengono utilizzati.

- Minimizzare l'intensità del segnale. Gli intrusi sfruttano il fatto che le onde radio non si possono limitare a dei luoghi ben definiti, ma riescono ad espandersi fuori dalle mura perimetrali dall'ufficio. Da qui la definizione del nome "parking lot attack", o più semplicemente attacchi provenienti dal parcheggio. È pertanto importante scegliere un'adeguata collocazione dell'Access Point all'interno dell'edificio, in modo che il segnale sia sufficiente a garantire il collegamento solo ed esclusivamente alla zona interessata.

- Cambiare le community di default di SNMP. Su molti AP risulta installato un agente SNMP (Simple Network Management Protocol). Se la community password non risulta correttamente configurata, un aggressore può leggere e scrivere dati di configurazione sull'AP, in maniera analoga ad altri sistemi che supportano SNMP.

- Limitare il traffico di broadcast. I messaggi di broadcast (ad esempio il NetBIOS su TCP/IP) contribuiscono ad incrementare il valore IV del sistema WEP, minimizzando per un intruso i tempi di raccolta dei dati per ricavare la chiave WEP, pertanto è consigliabile limitare il traffico di broadcast quando possibile, ad esempio disattivando il protocollo NetBIOS su TCP/IP dal binding con la scheda di rete Wireless.

- Protezione del client. Alcuni attacchi sono mirati ai client wireless in quanto vengono usati come ponte per entrare nella rete interna e per ricavare preziose informazioni. È preferibile usare un personal firewall sui client in modo da ridurre i rischi di attacchi.

- Non utilizzare il DHCP. È consigliabile non utilizzare il DHCP per l'assegnazione dinamica degli indirizzi, ma considerare l'utilizzo di IP statici.
- Uso di una VLAN separata. È consigliabile utilizzare una Virtual LAN separata per il traffico wireless, separandola dalla rete intranet. Esistono varie metodologie, ad esempio il PPPoE che vedremo in seguito, per unire in maniera sicura le due LAN.

In ambienti SOHO (Small Office, Home Office) dove la protezione della rete non rappresenta un problema, queste semplici regole potrebbero essere sufficienti a proteggere l'accesso wireless. Uno dei punti negativi di WEP è che non può essere usato come metodo di autenticazione degli utenti: WEP infatti è un metodo di crittografia che si applica ad un "segmento" wireless e non al singolo utente, non potendolo identificare univocamente. In alcuni casi è importante anche autenticare ed autorizzare un singolo utente, anche banalmente con username e password, e applicare delle regole al singolo utente, ad esempio assegnando IP address statici e creando Access Lists o regole di firewall (iptables sotto Linux) in modo che l'amministratore delegato possa accedere a tutto, mentre il commerciale solo alla posta.

Nella seconda parte di questo articolo, che verrà pubblicata nel prossimo numero, l'autore offrirà una serie di consigli utili ed un sintetico riassunto su tutto quello che si deve sapere sull'autenticazione degli utenti e sul PPPoE. Per gli interessati, come meglio specificato nel box a latere, c'è la possibilità di approfondire gratuitamente questa materia sia attraverso un draft su PPPoE e sia tramite un e-book di ben 140 pagine intitolato "Sicurezza nelle Wireless LAN".

L'autore
Giuseppe Paternò, autore di questo articolo, ha conseguito la certificazione CCNP ed è membro di IEEE e della Italian Linux Society. La sua passione per le nuove sfide tecnologiche lo ha spinto ad esplorare fin da giovanissimo tutti i settori dell'informatica, con particolare riguardo al settore della sicurezza e delle reti. Attualmente lavora presso Sun Microsystems occupandosi di architetture di network e security, ma nel suo passato spiccano esperienze di lavoro stimolanti, tra cui con IBM e Infostrada. In quasi due anni di ricerche sulle Wireless LAN, Giuseppe ha prodotto un Internet Draft dal titolo "Using PPP-over-Ethernet (PPPoE) in Wireless LANs" e un e-book dal titolo "Sicurezza nelle Wireless LAN". Entrambi questi documenti sono utilissimi per approfondire le tematiche trattate on questo articolo e sono disponibile gratuitamente sul suo sito personale: http://www.gpaterno.com

Altri articoli pubblicati da Linux Journal sulle Wireless LAN

A Guided Tour of Ethereal
Learn exactly what's in all those packets flying by on your network with this essential development and administration tool.
by Brad Hards
www.dossier.duke.it, Codice Documento: L118-6842

Laptopia
Will your next laptop "just work" with Linux? And when will you be able to buy a major-label laptop without a proprietary OS anyway?
by Doc Searls
www.dossier.duke.it, Codice Documento: L117-7198

Secure Mail with LDAP and IMAP
Set up a secure, scalable mail system that uses your existing LDAP server to authenticate IMAP users connecting from anywhere.
by Mick Bauer
Part I - www.dossier.duke.it, Codice Documento: L115-6998
Part II - www.dossier.duke.it, Codice Documento: L117-7191

Building a Linux IPv6 DNS Server
A tutorial on building a DNS server node that provides IPv6 name resolution, with examples of some useful IPv6 applications.
by David Gordon and Ibrahim Haddad
www.dossier.duke.it, Codice Documento: L114-6541

Discovering Wireless Networks
Does anyone nearby have an access point you can use? Find out quickly.
by Tony Steidler-Dennison
www.dossier.duke.it, Codice Documento: L113-6861

Linux-Powered Wireless Hot Spots
Put a convenient authentication system on your access point with free software.
by Mike Kershaw
www.dossier.duke.it, Codice Documento: L113-6887

Suggerimenti per gestire la sicurezza nelle wireless LAN Parte 2

In questa seconda parte l'autore offre una serie di consigli utili ed un sintetico riassunto su tutto quello che si deve sapere su PPPoE. Per gli interessati, la possibilità di approfondire gratuitamente questa materia attraverso un draft su PPPoE ed un e-book di ben 140 pagine intitolato "Sicurezza nelle Wireless LAN"

di Giuseppe Paternò

Mentre nella prima parte dell'articolo, pubblicata nel precedente numero di marzo, sono state approfondite le tematiche del WEP, in questa seconda parte vogliamo focalizzarci sugli standard dell'autenticazione ed in particolare sull'uso di PPPoE nell'ambito wireless.

Come noto, lo standard per autenticare un utente in un ambiente wireless è IEEE 802.1x, che è basato Extensive Authentication Protocol Over Lan (EAPOL) e nato per l'identificazione e l'autorizzazione dell'utente su reti wireless (più in generale sulle reti ethernet). Sebbene questo protocollo sia l'ideale per riconoscere un utente e dare l'accesso alla rete, si possono evidenziare tre sue implicazioni. La prima è che IEEE 802.1x non definisce un sistema di crittografia: questo protocollo si limita ad autenticare l'utente, anche se è in grado di "integrarsi" con WEP. Il secondo problema è che molti degli Access Point esistenti non dispongono di 802.1x. Quegli AP che non dispongono della possibilità di essere aggiornati via software devono essere sostituiti. Inoltre è probabile che i futuri AP a basso costo, tipicamente pensati per l'utenza domestica e piccoli uffici, non disporranno di 802.1x, che necessita comunque di una infrastruttura RADIUS. Infine solamente alcuni sistemi operativi, ad esempio Windows 2000 e Windows XP, supportano nativamente IEEE 802.1x. I sistemi Apple con MacOS prima della versione 10.3 "Panther" e chi dispone di sistemi Windows 95/98/ME/NT devono acquistare un client compliant con IEEE 802.1x, con costi aggiuntivi. Il costo potrebbe rappresentare un problema minore per una azienda con un numero definito di utenti, ma potrebbe essere un rischio di business per un ISP o un operatore mobile che decidesse di offrire accesso Wireless. Con il Point-to-Point Protocol over Ethernet (PPPoE), questo problema non esiste: tutti gli OS sono dotati di software per l'accesso PPPoE in quanto si tratta della stessa tecnologia usata nell'ADSL e nei Cable Modems (usati all'estero per veicolare Internet sulla TV via cavo).

PPPoE è paragonabile all'uso di IEEE 802.1x a livello autenticazione, ma offre alcuni vantaggi, ad esempio non richiede l'uso di indirizzamenti a livello 3 (esempio IP) direttamente sulla ethernet, offuscando di fatto la topologia della rete interna, ed inoltre non richiede una infrastruttura PKI per l'autenticazione dell'utente. PPPoE, di contro ha un problema relativo alla lunghezza dei pacchetti trasmessi, chiamata Maximum Transmission Unit (MTU). In pratica la lunghezza dei pacchetti non può superare i 1492 bytes, causando problemi di performance su una grossa mole di dati trasmessi.

L'uso di PPPoE richiede che una macchina, sia essa un router od un server (vedremo un esempio con Linux), funga da collegamento tra la rete interna e la rete Wireless (pertanto necessita di due schede di rete). Questa macchina, denominata Access Concentrator, avrà il compito di autenticare e autorizzare in primo luogo l'utente, successivamente di codificare e decodificare il protocollo PPPoE.

È bene ricordare che durante la configurazione dell'Access Concentrator, lo scambio delle password tra il server e il client non deve essere di tipo Password Authentication Protocol (PAP), in quanto le password vengono scambiate in chiaro, ma si suggerisce l'uso di CHAP o MS-CHAPv2.

È noto a tutti quanto le onde radio siano difficili da controllare e quanto sia facile per un intruso intercettarle. Il protocollo PPP e di conseguenza PPPoE, offre un'architettura di crittografia chiamata Microsoft Point-To-Point Encryption Protocol (MPPE). Questa estensione del Compression Control Protocol (CCP) è stata introdotta da Microsoft per applicare la sicurezza nel protocollo di VPN chiamato Point-to-Point Tunneling Protocol (PPTP). È abbastanza semplice introdurre l'uso di MPPE su collegamento basato su PPPoE, anche se non tutte le piattaforme supportano l'uso congiunto delle due tecnologie. PPPoE con l'estensione MPPE può essere un modo semplice per affrontare il problema di sicurezza in ambito wireless, attribuendo a ciascun client una crittografia in base all'utente.

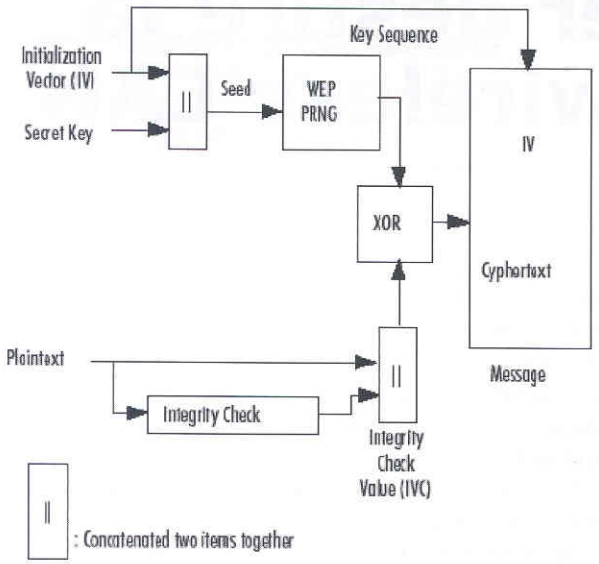

Fig. 4.7 - Query dei sevizi PPPoE disponibili

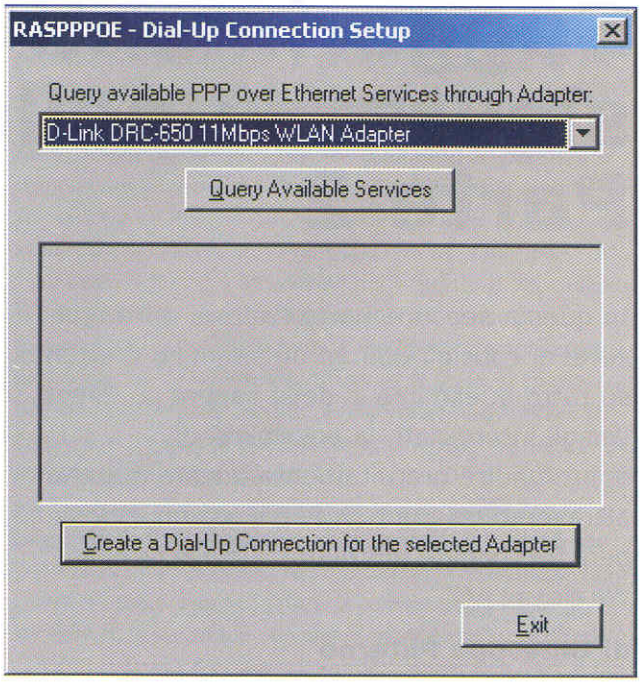

Fig. 4.8 - Selezione della cifratura MPPE

Installare un Access Concentrator

Precedentemente abbiamo parlato dell'Access Concentrator (AC) che funge da concentratore di accessi tra la rete wireless e la rete cablata, in maniera simile a quanto faccia un concentratore di accessi per i modem. Per creare un AC con Linux è necessario disporre di un computer con almeno due schede di rete, una attestata sulla LAN interna con il proprio IP address, l'altra senza IP address (ma in stato "up") e con un cavo cross-ethernet (o un hub/switch) su cui attestare uno o più Access Point. Come software useremo Roaring Penguin PPPoE, di solito contrassegnato come rp-pppoe e installato quasi in tutte le distribuzioni. Qualora la distribuzione non abbia a disposizione il software, è possibile scaricare i binari ed i sorgenti dal sito http://www.roaringpenguin.com/pppoe.

È necessario inoltre scaricare le patch del kernel e le patch di PPPD 2.4.1 per abilitare l'uso del protocollo MPPE e, successivamente, applicarle. L'URL da cui si possono scaricare tali patch è http://public.planetmirror.com/pub/mppe/. Alcune distribuzioni forniscono il programma PPPD e il kernel con queste feature abilitate: si consiglia di verificare con il manuale o con le FAQ della propria distribuzione.

In seguito è sufficiente configurare il file /etc/ppp/pppoe-server-options in maniera simile a quanto segue:

```
debug
name *
lock
mtu 1490
mru 1490
proxyarp
auth
+chap
+chapms
+chapms-v2
ipcp-accept-local
ipcp-accept-remote
lcp-echo-failure 3
lcp-echo-interval 5
deflate 0
mppe-128
mppe-40
mppe-stateless
```

Poi configurare il file /etc/ppp/pppoe-server-pool-ip con un intervallo di IP address da assegnare agli utenti wireless, e configurare il file /etc/ppp/chap-secrets. Per eseguire il server PPPoE su Linux, eseguire il seguente comando:

```
pppoe-server -I ethX -C ACNAME-l 192.168.0.1 -p
/etc/ppp/pppoe-server-pool-ip
```

dove ethX è l'interfaccia collegata alla rete Wireless, ACNAME è il nome dell'Access Concentrator e 192.168.0.1 è l'IP address da assegnare al server, che deve essere congruente con quanto specificato in /etc/ppp/pppoe-server-pool-ip. Dopo aver provato la soluzione, è necessario configurare gli script di partenza/arresto per il server PPPoEll client PPPoE

È da notare che il supporto PPPoE client è molto più diffuso rispetto alla funzionalità di Access Concentrator, però

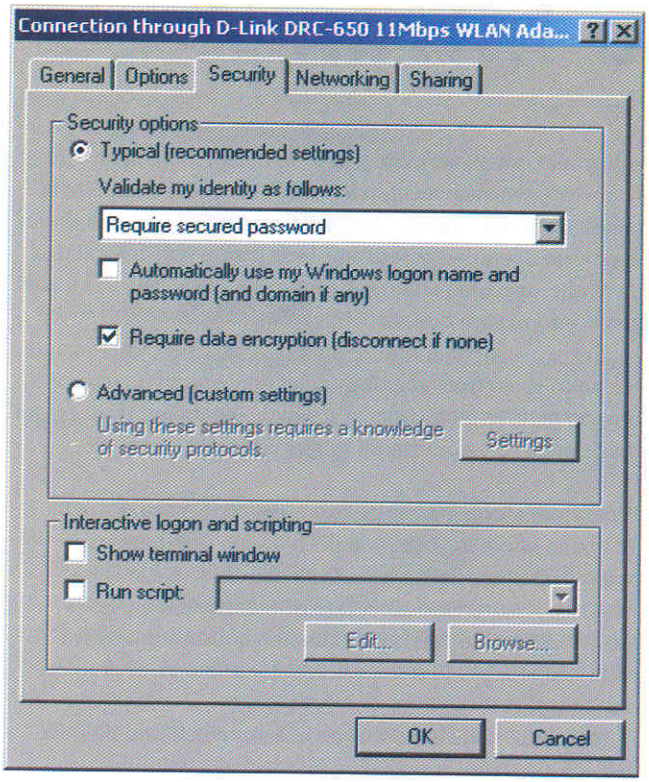

Figura 3

non tutte le implementazioni client PPPoE accettano anche l'estensione MPPE per la crittografia: i software selezionati in questo articolo sono stati testati dall'autore con la funzionalità di MPPE.

Esempio con Windows 2000

La configurazione è stata realizzata attraverso il programma RASPPPOE di Robert Schlabbach disponibile al sito Internet http://www.raspppoe.com/, da cui si può scaricare il driver. Durante questa fase verrà installato il driver Point-to-Point over Ethernet sul sistema, configurandolo nella scheda di rete collegata verso la rete wireless.

- Scompattare il file ZIP del driver PPPoE in una directory temporanea
- Nel pannello Network and Dial-Up Connections aprire la proprietà della scheda di rete collegata verso la rete wireless e premere sul pulsante Install
- Nella finestra Select Network Component selezionare Protocol e premere il pulsante Add
- Nella finestra Network Protocol selezionare Have Disk
- Nella finestra Install From Disk selezionare la directory temporanea in cui si è scompattato il driver e premere Ok
- Selezionare PPP over Ethernet Protocol e premere Ok
- Durante l'installazione del protocollo verranno presentate diverse finestre con il messaggio Digital Signature Not Found: premere sempre i pulsanti Yes o Continue Anyway
- Ritornati alla finestra delle proprietà della rete, togliere i checkbox a tutti i protocolli con l'esclusione di PPP over Ethernet Protocol

A seguito di questa fase è suggerito effettuare un riavvio manuale del sistema, nel caso in cui non venga proposto da Windows: un boot sotto Windows non si nega a nessuno :-) Successivamente, premere Start, selezionare Run, inserire il programma RASPPPOE e premere Ok.

- Verrà presentata una finestra di dialogo. Selezionare la scheda di rete wireless dall'opzione Query available PPP over Ethernet Services through Adapter qualora si abbiano più di una scheda di rete installata dalla macchina
- Premere il pulsante su Create a Dial-Up Connection for the selected Adapter
- Verrà creata un'icona chiamata Connection through "Nome Adattatore" nel pannello Network and Dial-Up Connections
- Selezionare la nuova icona e premere Properties.
- Nella sezione Security, selezionare Required secured password e selezionare Require data encryption
- Nella sezione Networking, selezionare unicamente il protocollo TCP/IP
- Premere O per eseguire la connessione, fare click due volte sulla nuova icona e fornire username e password, come definito sul server. È possibile configurare client con altre versioni di Windows con lo stesso driver PPPoE: è bene sempre leggere il file di documentazione readme9x.htm per Windows 95/98/ME e readment.htm per Windows NT.

Esempio con Linux

Il PPPoE client per Linux è lo stesso usato anche per l'Access Concentrator: infatti il software Roaring Penguin PPPoE contiene sia la parte "server"che "client". Anche in questo caso è necessario modificare il kernel di Linux e il programma PPPD per abilitare MPPE (rif. Access Concentrator). Successivamente è necessario modificare il file /etc/ppp/pppoe.conf per riflettere i parametri di configurazione utente, in particolare il campo USER, che deve contenere un utente valido, e PPPD_EXTRA="mppe-128 mppe-stateless require-chapms-v2". È necessario anche modificare il file /etc/ppp/chap-secrets per inserire la coppia username e password. Il comando per avviare la connessione è adsl-start ed analogamente adsl-stop per terminarla.

L'Autore
Giuseppe Paternò - http://www.gpaterno.com