

**Desiderei conoscere il significato dei termini "wardriving" e "warchalking". Grazie.  
(25 agosto 2003)**

I due termini sono entrati già da qualche tempo nel gergo della comunità internazionale che naviga in rete e si riferiscono in particolar modo ai fenomeni di appropriazione e uso di banda ad alta velocità attraverso la rete wireless, ossia attraverso connessione ad Internet tramite radiofrequenza, detta anche WLAN.

L'idea che spinge lo sviluppo di questa soluzione tecnologica è la possibilità di offrire connettività "senza fili", garantendo così la navigazione e l'utilizzo dei servizi in rete mentre ci si trova, ad esempio, all'aeroporto, in stazione, all'ufficio postale, per la strada in automobile. La connessione avviene grazie ad un dispositivo installato sul proprio pc, appostandosi nelle vicinanze dei punti di accesso. L'attività di ricerca, appostamento ed utilizzo indebito della connessione su reti wireless, non adeguatamente protette e configurate, viene denominato "wardriving". Ma come è possibile venire a conoscenza di punti di accesso non messi in sicurezza accuratamente? Il "warchalking" è esattamente quanto serve: con questo termine si intende la pratica di indicare con una serie di simboli lungo le strade e sui muri la vicinanza di un punto di ingresso "wireless" e le relative coordinate di collegamento.

Il fenomeno del "wardriving", rimasto prevalentemente confinato all'interno di sfide di abilità fra i nuovi hackers senza fili, deve far riflettere sulla maggiore debolezza e vulnerabilità delle reti wireless rispetto a quelle via cavo.

Le reti cablate sono per loro natura più sicure: per accedere è necessario un collegamento fisico mediante un cavo. Questo non è vero per le reti wireless: il mezzo fisico di connessione è l'ambiente stesso e non è necessario alcun cavo.

Sono stati sviluppati sistemi di autenticazione fra il terminale che effettua il collegamento e il punto di accesso.

Primo fra tutti il WEP ( Wired Equivalent Privacy ) che, a valle della fase di autenticazione, cripta e decripta tutto il flusso di dati. WEP non ha potuto imporsi dal momento che anche la più piccola perdita di dati, più frequente nella comunicazione senza fili, comporta la perdita dell'intero processo di trasferimento.

Oggi WEP è stato sostituito dal nuovo standard di comunicazione WAP che combina regole di autenticazione con livelli di crittografia, ottenendo un livello di sicurezza decisamente più elevato.

Mario Marangione