PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4428 di Lunedì 18 marzo 2019

WAP3: l'evoluzione della protezione delle reti WiFi

Un'evoluzione dei protocolli Wi-Fi che utilizza un sofisticato algoritmo per garantire un più elevato livello di autentica e verifica di integrità del messaggio.

Credo che oggi non passi più di un'ora, senza che un utente di servizi di comunicazione o di apparati informatici non abbia occasione di connettersi ad una rete senza fili. L'utilizzo crescente di queste reti ha reso necessaria la introduzione di protocolli di comunicazione protetti, per evitare che chiunque potesse intercettare chiunque altro. La prima norma che prese in considerazione la sicurezza delle trasmissioni Wi-Fi è stata chiamata **Wired Equivalent Privacy (WEP**).

L'evoluzione delle tecniche di attacco ha messo presto in evidenza alcune limitazioni, caratteristiche di questo protocollo di comunicazione, ed ecco perché l'ormai famosa Wi-Fi Alliance, che produce normative afferenti all'uso di questi sistemi di comunicazione, mise a disposizione un algoritmo più sofisticato, che garantiva un più elevato livello di protezione crittografica ed un più elevato livello di autentica delle controparti. Questa norma è stata ratificata da IEEE nel 2004 ed è contrassegnata dalla sigla 802.11i.

Il nome commerciale è **Wi-Fi Protected Access (WPA**). Un grande vantaggio di questa evoluzione normativa era legato alla retro-compatibilità con il protocollo precedente.

Poco dopo è stato messo a punto un nuovo protocollo, **WAP2**, che utilizza un sofisticato algoritmo, chiamato Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), per garantire un più elevato livello di autentica e verifica di integrità del messaggio.

Anche questo protocollo ha delle debolezze legate alla possibilità di accessi non autorizzati a reti aziendali ed ecco perché è stato introdotto un nuovo protocollo, chiamato WAP3.

Vediamo di analizzare un poco più in dettaglio questo protocollo, che ormai acquisterà una posizione di assoluta preminenza, rispetto agli altri già sviluppati.

È il terzo protocollo sviluppato dalla Wi-Fi Alliance. Come accennato in precedenza, questo protocollo offre un livello di sicurezza molto più elevato, rispetto ai protocolli precedenti. È bene ricordare che gli utenti che desiderano migrare a questa nuova tecnologia di protezione devono acquistare dei nuovi router in grado di supportare questo applicativo di cifratura o sperare che il fornitore dell'apparato di cui oggi dispongono possa mettere a disposizione l'aggiornamento.

Le caratteristiche migliorate di questo protocollo sono appresso illustrate.

- Innanzitutto, viene creato uno scambio di dati fra i due apparati connessi tramite rete Wi-Fi, che verifica ed autentica la connessione. Anche se la parola chiave scelta dall'utente è debole, il protocollo provvede a rinforzarla in modo appropriato.
- Quando ci si collega su una rete pubblica, il protocollo registra un nuovo apparato usando un sistema di controllo, che migliora in modo significativo il livello di protezione del collegamento.
- Come ulteriore misura di sicurezza, viene usato un applicativo criptografico assai più sicuro, in quanto a 256 bit, rispetto al precedente protocollo a 128 bit.
- Infine questo protocollo offre una protezione contro tentativi di individuare la password con sistemi di "brute force", in quanto consente all'utente un solo collegamento per avviare la procedura di verifica delle parole chiave. Questo è motivo per cui precedente protocollo WAP2 poteva essere violato con attacchi di forza bruta.

Adalberto Biasiotti

www.puntosicuro.it