PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4270 di Lunedì 02 luglio 2018

Da WEP a WAP3: l'evoluzione della protezione delle reti WiFi

La crescente diffusione delle reti senza fili impone la adozione di protocolli di sicurezza più stringenti: ecco l'evoluzione di questi protocolli.

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.

Queste reti sono destinate ad una crescita esponenziale, in relazione all'utilizzo crescente di apparati Internet of Things - IoT, che per poter funzionare hanno bisogno di essere collegati alle reti senza fili.

La architettura di rete più frequentemente utilizzata è chiamata Wi-Fi ed è stata resa disponibile agli utenti in due bande di frequenza, di cui la prima ormai sovraccarica e la seconda in continua espansione.

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.

WPA è stato reso disponibile sia in una versione per gli utenti professionali, sia per usi personali. Nella versione per usi professionali, chiamata WPA-EAP, sono stati usati dei protocolli di autentica più rigidi, utilizzando l'ormai famoso Extensible Authentication Protocol (EAP). Nella versione per uso personale, WPA-PSK, vengono usate delle chiavi di più semplice utilizzo. L'applicazione principale di questo protocollo è appunto per applicazioni domestiche piccoli uffici.

I professionisti della sicurezza di rete furono in grado di introdurre la architettura WPA su precedenti architetture WEP, grazie all'utilizzo di semplici aggiornamenti nel firmware. Anche se questa nuova versione indubbiamente aveva migliorato in modo significativo il livello di sicurezza della comunicazione, vi erano tuttavia delle debolezze in fase di autentica.

Ecco perché 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.

Ma non è finita.

Anche questo protocollo ha delle debolezze legate alla possibilità di accessi non autorizzati a reti aziendali. È ben vero che questo tipo di attacco richiede un impegno notevole da parte dell'attaccante, utilizzando computer di ultima generazione, ma in linea teorica non è possibile negare che tale evento possa verificarsi.

Naturalmente questi attacchi possono essere indirizzati anche a reti domestiche od a piccoli uffici, soprattutto quando vengono usate delle parole chiave di basso livello.

Ecco perché è stato introdotto un nuovo protocollo, chiamato WAP3.

Tanto per cominciare, ho già accennato al fatto che gli esperti prevedono che più di 30 miliardi di apparati saranno collegati a Internet nel 2020. La necessità di rendere sempre più elevato il livello di sicurezza della connessione diventa pertanto un'esigenza primaria.

Ad oggi, anche il protocollo sino ad adesso più avanzato, WAP2, è stato messo appunto ben 14 anni fa e tutti sappiamo quanto i malviventi siano rapidi nel mettere a punto nuove tecniche di attacco.

Il nuovo algoritmo utilizza una architettura di cifratura a 196 bit, ed è pienamente conforme con la nuova piattaforma di protezione approvata dalla commissione dei sistemi di sicurezza nazionale, come parte della National security agency. Questa architettura si chiama Commercial National Security Algorithm Suite.

Il vantaggio di questa nuova architettura sta nel permettere la cifratura automatica di tutto il traffico tra un apparato ed il punto di accesso Wi-Fi utilizzando una unica chiave, che non deve essere precedentemente impostata dall'utente.

Viene inoltre introdotta una procedura di autentica assai più robusta, quando l'apparato si collega ad un altro apparato Wi-Fi, accrescendo così il livello di protezione nel collegamento con apparati che non dispongono di parole chiave sufficientemente protette contro un attacco con la tecnica del dizionario.

Un'altra tecnica di attacco che venne messa in evidenza nel 2017 viene contrassegnata dalla sigla WPA2 KRACK, e venne scoperta da uno specialista, che immediatamente diffuse la notizia.

Il nuovo algoritmo di protezione introduce una semplice ma efficace difesa contro questo attacco, perché impedisce che una parola chiave errata venga più volte digitata, fino a trovare quella giusta.

Questo protocollo di protezione da questi tentativi di attacco per dizionario è già oggi utilizzato in molte architetture di sicurezza, laddove tre digitazioni consecutive di una parola chiave errata portano al blocco del sistema.

Infine, un altro vantaggio di questo nuovo protocollo sta nel fatto che, grazie ad esso, è possibile configurare apparati Wi-Fi privi di tastiera e di schermo, anche se i dettagli su questo argomento ancora non sono stati diffusi.

Per poter essere certi di disporre di un algoritmo di comunicazione sufficientemente sicuro, è bene che i lettori, quando effettuano l'analisi di rischio, si accertino che l'algoritmo utilizzato sia stato certificato dalla Wi-Fi Alliance.

Adalberto Biasiotti
