PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4310 di Lunedì 17 settembre 2018

A breve disponibile un nuovo protocollo di sicurezza delle reti Wi-Fi

La diffusione crescente delle reti Wi-Fi impone di proteggere in modo adeguato l'accesso a queste reti. Il protocollo ad oggi più diffuso risale a ben 14 anni fa e quindi sembra del tutto logico che esso possa essere sottoposto a tempestiva revisione.

È opportuno tracciare una breve storia sull'evoluzione dei protocolli di sicurezza, applicati alle reti senza fili.

Il primo protocollo applicato aveva il nome WAP 2- *Wi-Fi protected access*, e per 14 anni ha garantito un soddisfacente livello di sicurezza di queste reti.

Tuttavia, con il passare del tempo, hanno cominciato, come è del tutto fisiologico, a manifestarsi alcune debolezze, mentre i criminali informatici studiavano a fondo possibili debolezze di questo protocollo.

Il motivo per cui è recentemente apparso sul mercato un protocollo evoluto, chiamato WAP 3, nasce proprio dalla necessità di mettere sotto controllo queste debolezze.

Il fatto che ancora oggi questo protocollo di sicurezza sia utilizzato a livello mondiale, in milioni di reti, fin dal 2004, dimostra che tutto sommato si tratta di un protocollo soddisfacente. Vediamo adesso quali sono invece i miglioramenti che offre questo nuovo protocollo, che è in corso di sviluppo e per il quale dovrebbero essere emesse le appropriate certificazioni dell'ultimo scorcio del 2018.

Gli esperti affermano che l'utilizzo di questo protocollo avvantaggerà soprattutto i consumatori, più che le aziende, e i miglioramenti saranno tanto importanti, quanto relativamente trasparenti per l'utente.

Un'altra considerazione da non trascurare è legata al fatto che oggi molte reti, messe a disposizione gratuitamente da attività commerciali, non sono protette: l'obbiettivo di questa riduzione sicurezza è quella di facilitare all'utente il collegamento alla rete.

Purtroppo non tutti si rendono conto che questo tipo di collegamento è accessibile a chiunque possa monitorare le onde radio, a meno che non vengano utilizzati dei protocolli particolari di cifratura nel collegamento utilizzato dall'utente con il proprio server, oppure con il server aziendale.

Tuttavia, anche le reti ad accesso protetto utilizzano delle parole chiave di pubblico dominio. In molti alberghi, a tutti i clienti viene consegnata, insieme alla chiave della camera, la informazione afferente alla parola chiave di collegamento alla rete alberghiera.

Il protocollo WAP3 risolvere questo problema basandosi una nuova norma, chiamata Opportunistic Wireless Encryption (OWE). Una rete così protetta si comporta a tutti gli effetti come una rete aperta, ma il traffico viene cifrato con un robusto algoritmo, anche senza dover introdurre una parola chiave.

Chi ha sviluppato questo protocollo ritiene che possa trovare una larghissima applicazione nelle reti pubbliche, ad esempio quelli disponibili presso gli esercizi commerciali o presso i luoghi pubblici di molte città, perché non si richiede nessun intervento da parte dell'utente coinvolto. È così facilmente possibile proteggere reti esistenti senza interventi di grande levatura.

La storia insegna

Per molti anni, i criminali informatici hanno attaccato le reti WPA2-PSK (Pre-Shared Key), vale a dire le reti in cui la parola chiave di accesso è la stessa per tutti gli utenti. Alcune tecniche di attacco si basavano su sistemi ormai ben noti, come gli attacchi con dizionario, che individuano la parola chiave analizzando una moltitudine di chiavi probabili.

Molti strumenti di attacco sono stati specialmente progettati per attaccare reti protette di tipo WPA2-PSK.

Nella seconda metà del 2017 la situazione è rapidamente peggiorata, perché è stato messo a punto un nuovo protocollo di attacco, chiamato. KRACK (Key Reinstallation Attack). Questo protocollo non attacca direttamente la rete via radio, ma sfrutta un errore frequente di installazione, su quale non vale la pena di addentrarci. L'ormai famoso Computer Emergency Response Team degli Stati Uniti (US- CERT) ha illustrato in dettaglio come funziona questo attacco.

Il nuovo protocollo usa un nuovo sistema di autentica, chiamato SAE (Simultaneous Authentication of Equals). Una peculiarità del nuovo protocollo è quella che consente a due parti, che cercano di collegarsi alla rete, di identificarsi rispettivamente, dimostrando di essere a conoscenza della chiave segreta, senza però divulgarla.

Una delle tecniche più comuni per attaccare le esistenti reti senza fili è quella di creare un finto Access point della vicinanza di un'azienda, come ad esempio nel parcheggio aziendale. Questo finto Access point può cercare di collegarsi alla rete, apparendo come utente legittimo. Il nuovo protocollo mette sotto controllo questa possibilità di attacco.

Esistono anche altre versioni ancora più raffinate di questo nuovo protocollo, chiamato WPA3-CNSA (Commercial National Security Agency). Una limitazione di questo nuovo protocollo è legata al fatto che la sua installazione richiede la chiusura della rete per un certo periodo. Ciò non toglie che sia possibile, ad esempio in un giorno festivo, bloccare la rete procedere all'aggiornamento.

Poiché sempre più spesso queste reti vengono utilizzate per trasmettere dati personali, il responsabile della sicurezza informatica devono condurre una valutazione di rischio sull'utilizzo di queste reti e, se del caso, attuare le appropriate e moderne contromisure disponibili.

Adalberto Biasiotti

---

www.puntosicuro.it