WPA, generalità e principi di funzionamento.

Baglieri Eugenio
Matricola: A40/000047
Sicurezza dei Sistemi Informatici 2
C.d.S in Informatica Applicata
Facoltà di scienze MM.FF.NN.
Università degli Studi di Catania

Indice:

1. Introduzione.

Oggi le reti wireless godono di alto livello di diffusione grazie alla semplicità con cui possono essere realizzate, al basso costo, (si pensi infatti al costo da dover affrontare per il cablaggio di un vecchio edificio sprovvisto di impianti elettrici adeguati) e alla semplicità di accesso. Quest' ultima caratteristica però ha portato in primo piano i problemi relativi alla sicurezza di queste perché la semplictà di accesso disponbile ad un utente autorizzato, è altrettanto disponbile ad un possibile attaccante. C'è pertanto bisogno di un sistema i cui scopi principali siano l'autenticazione e la privacy. L'autenticazione assicura che solo gli utenti autorizzati siano in grado di accedere alla rete, mentre la privacy garantisce che i dati trasmessi nella rete non siano disponibili ad utenti non autorizzati.

Nel tentativo di soddisfare i bisogni delle reti Wi-Fi venne introdotto lo standard 802.11b meglio conosciuto come WEP (Wired Equivalent Privacy) che provava ad assicurare segretezza autenticità e integrità nelle comunicazioni senza fili. Tuttavia questo protocollo si rivelò debole e quindi facilmente attaccabile. A fronte dell'inaffidabilità del WEP il gruppo Wi-Fi Alliance, consorzio di fornitori Wi-Fi, elaborò un nuova specifica per la sicurezza delle reti Wi-Fi per garantire un maggior livello di protezione. Il protocollo si chiama WPA (Wireless Protected Access) e rappresenta solo alcune delle funzioni presenti nello standard IEEE 802.11i. WPA può essere utilizzato in due modalità, Personal ed Entrprise la prima appropriata per piccoli uffici e in generale per reti di piccole dimensioni, la seconda invece permette di gestire reti più estese.

La successiva implementazione del WPA è il WPA2 che implementa interamente le funzioni definite nello standard 802.11i, prevede entrambi i modi Personal ed Enterprise e la sostanziale differenza con il suo predecessore è che WPA2 fornisce un migliore meccanismo di criptaggio attraverso l' AES.

1.1 I miglioramenti rispetto al WEP.

Rispetto al WEP, il WPA introduce una migliore crittografia dei dati poiché per cifrare i dati utilizza RC4 con una chiave a 128 bit e un vettore di inizializzazione a 48 bit, insieme al Temporary Key Integrity Protocol (TKIP) che permette di cambiare dopo un certo numero di messaggi scambiati le chiavi di crittografia utilizzate. In WPA è stato anche migliorato il Cyclic Redundacy Check che nel WEP era insicuro, infatti era possibile alterare il messaggio e aggiornare il CRC pur non conoscendo la chiave. Al posto del CRC è stato introdotto un più sicuro codice di autenticazione dei messaggi il Message Integrity Code (MIC, la cui implementazione in WPA prende il nome di Michael) che include anche un contatore di frame con l'obbiettivo di prevenire i replay attack. Infine è stato aggiunto un meccanismo di mutua autenticazione, funzione quest'ultima assente nel WEP.

1.2 L'autenticazione.

Un elemento critico della sicurezza di una rete Wi-Fi è non permettere l'accesso agli utenti non autorizzati. Grazie all'autenticazione è possibile conoscere l'identità di un utente o di una macchina che tenta di accedere alla rete, e non appena questa viene verificata può essere presa la decisione di permettere o meno l'accesso. E' chiaro quindi che senza un attento controllo delle identità, dei possibili attaccanti potrebbero avere accesso alle risorse di rete protette. Inoltre è necessario che anche la rete si autentichi all'utente per evitare che un utente wireless entri accidentalmente in una rete non sicura nella quale le sue credenziali possano essere rubate da un utente malintenzionato.
L'autenticazione in WPA è basata su EAP (Extensible Autentication Protocol) un protocollo generico di autenticazione tra client e server che supporta numerosi metodi con password, certificati digitali o altri tipi di credenziali. I metodi utilizzati da WPA sono:

- EAP-TLS.
- EAP-TTLS.
- PEAPv0.
- PEAPv1.
- EAP-SIM.

1.2.1 EAP-TLS.

EAP-Transport Layer Security è considerato uno degli standard EAP più sicuri ed è universalmente supportato da tutti i produttori di hardware wireless, e anche di software. Sono infatti disponibili le implementazioni sia lato server che client di Microsoft, Cisco, Apple e Linux. EAP-TLS richiede l'uso di una PKI per rendere sicura la comunicazione con il server di autenticazione RADIUS, o con qualsiasi altro server di autenticazione e necessita anche di certificati lato client.

Anche se la richiesta dei certificati lato client potrebbe risultare poco comoda, è ciò che permette una forte autenticazione e rappresenta un compromesso tra sicurezza e convenienza. Infatti una password compromessa non basta per rompere un sitema abilitato EAP-TLS, perché l'attaccante ha ancora bisogno di avere il certificato lato client. Quando questo certificato è memorizzato in una smartcard otteniamo un livello di sicurezza ancora maggiore, poiché non c'è modo di rubare la chiave privata del certificato nella smartcard, senza rubare la smartcard stessa.

1.2.2 EAP-TTLS.

EAP-Tunneled Transport Layer Security è un estensione di TLS. E' largamente supportato, e offre un livello di sicurezza molto buono. Il client non ha bisogno di autenticarsi al server attraverso un certificato firmato da una CA, ma solamente il server al client, e questo semplifica notevolmente la procedura. Dopo che il server si è autenticato al client con il certificato, può usare la connessione sicura appena stabilita per autenticare il client usando ("tunneling") uno dei metodi di autenticazione esistenti ampiamente utilizzati, utilizzando anche meccanismi con password o database di autenticazione la comunicazione è protetta anche da attacchi man in the middle e ascolto della comunicazione. Inoltre il nome dell'utente non è mai inviato in chiaro o non criptato, e ciò migliora la privacy del sistema.

1.2.3 PEAP.

PEAP è una proposta di standard aperto da parte di Cisco Systems, Microsoft e RSA Security. E' già largamente disponibile e fornisce un livello di sicurezza molto buono. Lo schema è molto simile a EAP-TTLS, richiede solo un certificato PKI per il server, in modo da creare un tunnel TLS sicuro per proteggere l'autenticazione dell' utente. Esistono due sottotipi di PEAP approvati per l'utilizzo in WPA e WPA2. Questi sono:

- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC

PEAPv0/EAP-MSCHAPv2 è il termine a cui molte persone si riferiscono quando utilizzano il termine PEAP non sapendo che esistono altre varianti di PEAP. Dopo EAP-TLS, questo è il secondo standard EAP più supportato nel mondo.
PEAPv1/EAP-GTC è stato creato da Cisco come alternativa a PEAPv0. Permette l'uso di un protocollo di autenticazione interno diverso da MSCHAPv2 di Microsoft. EAP-GTC (Generic Token Card) manda un testo di sfida, e attende la risposta che viene generata utilizzando un token di sicurezza come, ad esempio una smartcard. E' importante notare che EAP-GTC non protegge in alcun modo i dati dell' autenticazione.

1.2.4 EAP-SIM.

EAP-SIM è utilizzato per l'autenticazione e la distribuzione delle chiavi agli utenti mobili che utilizzano la rete GSM (Global System for Mobile Communication).

1.3 L'accesso.

WPA com già detto, supporta due metodi di accesso: Personal ed Enterprise. Il modo personal chiamato anche preshared key mode è appropriato per piccoli uffici o case che non hanno già infrastrutture di autenticazione esistenti. Una password settata manualmente viene inserita nell' access point e condivisa da tutti i client. La password può essere lunga da 8 a 63 caratteri, in generale 256 bit, poiché si ha a che fare con una password, è bene osservare alcune regole per ridurre il rischio di rottura della password ad esempio scegliere parole pronunciabili ma che non abbiano senso per rendere inutili gli attacchi a dizionario, scegliere password abbastanza lunghe, almeno 14 caratteri etc.. Se in vece si ha necessità di gestire una rete più estesa conviene optare per il WPA Enterprise che usa un server RADIUS (Remote Authentication Dial-In User Service) per l'autenticazione e un protocollo EAP per gestire lo scambio di dati di autenticazione tra il server e il client. Quando si utilizza un server per l'autenticazione, il punto di accesso senza fili impedisce l'inoltro del traffico dei dati a una rete cablata o ad un client senza fili che non dispone di una chiave valida. Per ottenerne una, il client deve seguire questo procedimento:

- Quando un client senza fili entra nel raggio di azione di un punto di accesso senza fili, il punto di accesso senza fili richiede la verifica del client
- Il client wireless si identifica e dall' access point le informazioni vengono inviate al server RADIUS
- Il server RADIUS verifica le credenziali del client. Se le credenziali sono valide, il server invia una chiave di autenticazione crittografata all' access point.

- L'access point utilizza la chiave per trasmettere in modo protetto le chiavi di crittografia unicast e muticast.

1.4 Il four-way handshake.

Il processo “four-way handshake” che tradotto diventa stretta di mano a quattro vie è un elemento importante del processo di autenticazione.Questo parte da due considerazioni: l'access point (AP) deve autenticarsi e la chiave di sessione utilizzata per cifrare i messaggi deve ancora essere calcolata. In primo luogo viene stabilita, tra la stazione wireless (STA) e l'AP, una chiave chiamata Pairwise Master Key (PMK). Questa chiave è generata tipicamente durante il procedimento di autenticazione dell’utente verso un server RADIUS (o di altro tipo) sfruttando l’EAP. Sia il client che il server RADIUS ottengono chiavi identiche, e il secondo restituisce la chiave all’AP. A questo punto STA e AP si scambiano una sequenza di quattro messaggi, nell’ambito dello schema “four-way handshake”. Per prima cosa EAP trasmette all'access point una chiave temporanea PTK (Pairwise Transient Key). LA PTK è generata concatenando PMK, una nonce dell'AP, una nonce di STA ed infine l'indirizzo MAC di STA e dell'AP. Il prodotto di questa concatenzione viene inviato ad una funzione crittografica di hash. La PTK è a sua volta suddivisa in più chiavi: una per firmare i messaggi "four-way handshake"; una per rendere sicuri i pacchetti dati trasmessi tra STA e AP; una per cifrare presso la stazione, e durante la fase di four-way handshake, la "group key". Quest’ultima consente all’AP di trasmettere un pacchetto multicast a tutte le stazioni, piuttosto che inviare un pacchetto separato e cifrato a ciascuna di esse. Nel corso della fase di four-way handshake, la stazione e l’access point negoziano, inoltre, il tipo di cifratura che deve essere impiegato per la connessione dati. Vengono quindi negoziati due algoritmi di cifratura: quello "pairwise" è utilizzato per la trasmissione unicast dei dati tra la stazione e l’access point mentre quello "group" è per la trasmissione broadcast/multicast del traffico dall’access point a più stazioni.

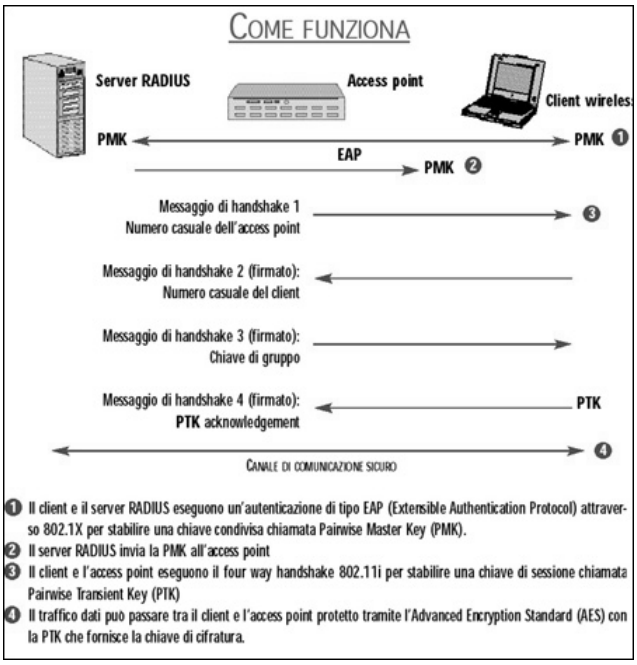

Immagine 1: Evoluzione temporale del Four-way Handshake.

1.5 Debolezze.

Quando WPA lavora in modalità personal una chiave unica, la Pre-Shared Key(PSK) viene utilizzata da tutti i client. Si può però avere che ogni stazione abbia la propria chiave generata a partire dalla PSK e legata all' indirizzo MAC della stazione stessa, oppure la chiave è la PSK stessa. La PSK è una chiave a 256 bit o una password da 8 a 63 caratteri. Accade che se la PSK utilizzata è a 256 bit, questa vine utilizzata direttamente come PMK, altrimenti se è di lunghezza minore la PMK viene derivata attraverso una funzione hash che prende in input la password, il nome della rete wireless, la lunghezza dello stesso e restituisce un hash di 256 bit. La PTK invece è generata a partire dalla PMK utilizzando i due indirizzi MAC e le due nonces che vengono scambiate nei primi due pacchetti durante il processo di four-way handshake e serve inoltre sia per firmare i messaggi durante questo processo, che per generare le chiavi successive del TKIP. Quindi conoscendo la PSK è possibile ricavare la PTK e tutta la gerarchia delle chiavi. Un utente che già conosce la PSK xkè magari è autorizzato ad accedere alla rete, può calcolare la chiave utilizzata da tutte le altre stazioni wireless presenti semplicemente “sniffando” i pacchetti del four-way handshake che contengono le nonces. Quindi anche se le chiavi sono diverse per ogni stazione, all'interno della rete non c'è nulla di privato.

Se invece una stazione non conosce la PSK, può romperla mediante un attacco offline. La PTK è usata per prudurre l'hash dei messaggi durante il four-way handshake ed esiste una lunga lista di

attacchi offline a dizionario contro gli hash. E' quindi possibile modificare uno di questi programmi per prendere in input i dati ottenuti catturati durante il processo di autenticazione per realizzare l'attacco. Questo attacco probabilmente andrà a buon fine se la PSK è una password quindi facile da ricordare e probabilmente di breve lunghezza, una stringa di questo tipo cioè all'incirca di 8 caratteri è sicuramente contenuta nel dizionario. Una stringa di circa 20 caratteri è quanto basta a prevenire un attacco di questo tipo, ma è molto più lunga di quelle che utilizzano normalmente la maggior parte delle persone.

Conclusione.

Ad oggi non esiste ancora un'unica soluzione Standard che puo essere ritenuta affidabile, anche se sono stati introdotti nuovi standard per la sicurezza, non c'è la garanzia totale che le comunicazioni siano realmente sicure. Quindi c'è bisogno di studiare soluzioni alternative, o integrare quelle già conosciute con altre strutture di sicurezza, senza però aumentare o scambio di messaggi e quindi l'overhead di dati con un conseguente calo delle prestazioni. Tuttavia questi due requisiti sono spesso in conflitto e non resta quindi che la ricerca del miglior compromesso possibile.

Riferimenti.

- http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
- http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
- http://blogs.techrepublic.com.com/Ou/?p=67
- http://www.periodiklabs.com/papers/wpaoverview.pdf
- http://wiki.freeradius.org/Extensible_Authentication_Protocol
- http://www.dice.ucl.ac.be/crypto/files/publications/pdf193.pdf
- http://wifinetnews.com/archives/002452.html