Sicurezza nelle reti IEEE 802.11i

Tesina per il corso di Sicurezza su Reti 2

prof. Alfredo De Santis

di

Ivan Di Giacomo (digiacomoivan@gmail.com)

Daniele Mastrangelo (danielemastrangelo@tiscali.it)

1. Introduzione

1.1. Le reti wireless

La comunicazione, sin dall'antichità, è intesa come processo di trasmissione di informazioni che nel corso degli anni è stata nel mondo una delle principali protagoniste della ricerca e dell'evoluzione dell'infrastrutture di rete.

Nel 1985 viene pubblicato lo standard ***IEEE 802.3*** per le reti LAN (Local Area Network) in cui la comunicazione avviene tramite un infrastruttura di rete cablata. Con il passare degli anni si è cercata una soluzione che potesse eliminare il cablaggio e quindi nel 1997 viene presentata la prima versione dello standard ***IEEE 802.11*** chiamata ***802.1y*** la quale specificava velocità di trasferimento comprese tra 1 e 2 Mb/s e utilizzava i raggi infrarossi o le onde radio nella frequenza di 2,4 Ghz per la trasmissione del segnale.

Il problema principale, tuttavia, indipendentemente dalla tecnologia di rete utilizzata, è sempre stato quello di fornire un protocollo che rendesse tale comunicazione sicura.

Per quanto riguarda le reti LAN (reti cablate) è necessario rendere protetto il mezzo fisico di comunicazione, ovvero i cavi, in modo da evitare spiacevoli intrusioni.

Le reti Wireless, invece, presentano un canale di comunicazione ben diverso dai cavi: l'aria. Quest'ultimo risulta molto più difficile da proteggere in quanto "pubblico"; infatti, chiunque possiede una strumentazione adeguata può intercettare le onde radio trasmesse e quindi accedere alla rete.

Nei paragrafi successivi verranno presentati i protocolli di sicurezza che vengono utilizzati per rendere tale canale difficilmente attaccabile.

1.2. Classificazione dei protocolli di sicurezza

I protocolli di protezione principali che interessano le reti wireless e che saranno trattati sono i seguenti:

- **WEP (Wired Equivalent Privacy):** è il primo protocollo definito per lo standard IEEE 802.11. WEP usa lo stream cipher RC4 per la sicurezza e utilizza il CRC-32 per verificare l'integrità dei dati.
- **WPA (Wi-Fi Protected Access):** A causa di errori scoperti nell'algoritmo crittografico del protocollo WEP si è sviluppato il protocollo WPA. WPA è progettato per utilizzare lo standard IEEE 802.1x sia per gestire l'autenticazione dei client e dei server sia per la distribuzione di differenti chiavi per ogni utente. I dati sono cifrati con lo stream cipher RC4 con chiave a 128 bit.
- **WPA2:** WPA2 è il protocollo che succede WPA; realizzato nel settembre del 2004 implementa tutte le funzionalità definite dallo standard 802.11i, a differenza di WPA che è basato solo alcune funzionalità dello standard. La differenza principale con WPA è il nuovo algoritmo di cifratura basato su AES (**Advanced Encryption Standard**) che prende il nome di CCMP (**Counter-Mode/CBC-Mac Protocol**).

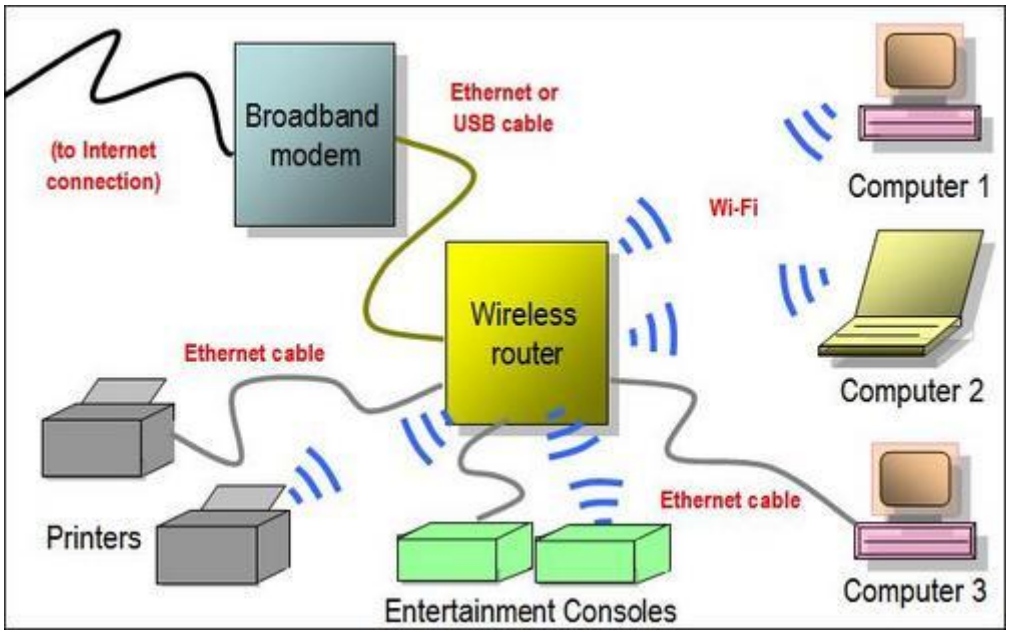
Nei prossimi capitoli analizzeremo in dettaglio questi protocolli focalizzandoci soprattutto sul protocollo WPA per cui verrà anche mostrato un possibile attacco.

Nel prossimo paragrafo, invece, verrà analizzato in dettaglio lo standard IEEE 802.11 e le principali versioni rilasciate negli anni.

1.3. Lo standard IEEE 802.11

IEEE 802.11 o **Wi-Fi** definisce uno standard per le reti WLAN sviluppato dal gruppo 11 dell'IEEE 802. Questa famiglia di protocolli include tre protocolli dedicati alla trasmissione delle informazioni (802.11a, 802.11b, 802.11g), la sicurezza è stata inclusa in uno standard a parte, 802.11i. Gli altri standard della famiglia (c, d, e, f, h,etc.) riguardano estensioni dei servizi base e miglioramenti di servizi già disponibili. Tra i protocolli precedentemente citati il primo largamente diffuso è stato 802.11b; in seguito si sono diffusi il protocollo 802.11a e soprattutto il protocollo 802.11g.

Nella figura sottostante possiamo vedere una configurazione di una rete in cui sono presenti dispositivi collegati tramite lo standard Wi-Fi (IEEE 802.11) oppure tramite cavo ethernet (IEEE 803.2).



1.3.1. Il protocollo 802.11b

Il protocollo *802.11b* permette la trasmissione di al massimo 11Mb/s ed utilizza il CSMA/CA (Carrier Sense Multiple Access con Collision Avoidance) come metodo di trasmissione delle informazioni. Quest'ultimo indica una tecnica di trasmissione dati che si basa sull'accesso multiplo tramite rilevamento di un segnale elettrico chiamato *portante* (*Carrier Sense*). CSMA/CA è un protocollo MAC (*Medium Access Control*) utilizzato nelle reti a bus per

condividere tra più host la capacità della rete evitando, quindi, che due dispositivi trasmettano contemporaneamente.

1.3.2. Il protocollo 802.11a

Il protocollo *802.11a* approvato nel 1999 utilizza frequenze nell'intorno dei 5 Ghz e opera con una velocità massima di 54 Mb/s. Lo standard definisce 12 canali non sovrapposti, 8 dedicati alle comunicazioni interne e 4 per le comunicazioni punto a punto.

Questo standard non ha avuto notevole successo dato che l'802.11b si era già molto diffuso in diversi paesi. In Europa lo standard 802.11a non è stato autorizzato all'utilizzo dato che quelle frequenze erano riservate all'hiperlan (particolare standard WLAN); solo a metà del 2002 tali frequenze vennero liberalizzate e quindi si poté utilizzare l'802.11a.

1.3.3. Il protocollo 802.11g

Il protocollo 802.11g viene rilasciato nel giugno del 2003 ed utilizza le stesse frequenze dello standard 802.11b cioè la banda di 2,4 Ghz e fornisce una banda massima di 54 Mb/s.

È totalmente compatibile con lo standard 802.11b ma quando si trova ad operare con periferiche di tale standard deve ovviamente ridurre la sua velocità.

1.3.4. Il protocollo 802.11i

IEEE 802.11i è uno standard sviluppato dalla IEEE specificamente per fornire uno strumento di sicurezza alle comunicazioni basate sullo standard IEEE 802.11. Tale protocollo è stato rilasciato il 24 giugno 2004 .

1.4. Protocolli di sicurezza per le reti Wi-Fi

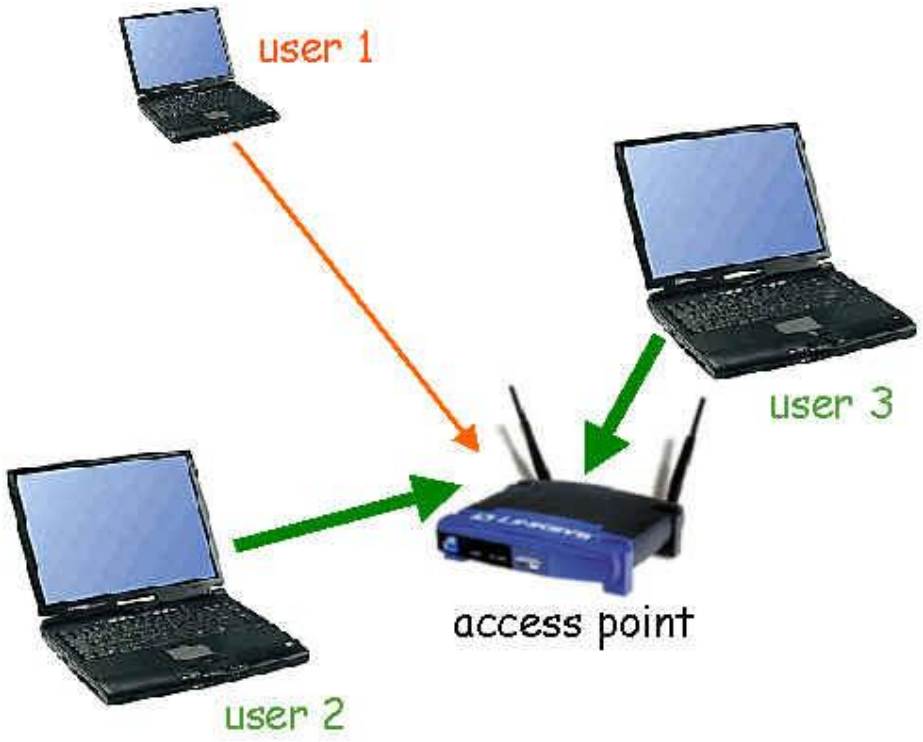
1.4.1. Validità di un protocollo di sicurezza

Nei paragrafi precedenti abbiamo visto che uno dei problemi che occorre affrontare quando si progetta un'infrastruttura di rete è garantire un protocollo di sicurezza valido. La domanda allora sorge spontanea: Quali sono gli aspetti che un protocollo di sicurezza deve avere affinché possa essere definito valido per la sicurezza di una rete?

Gli aspetti che potrebbero essere presi in considerazione sono diversi ma possiamo riassumerli nei seguenti:

- *Autenticazione alla rete;*
- *Segretezza della comunicazione;*
- *Integrità dei dati.*

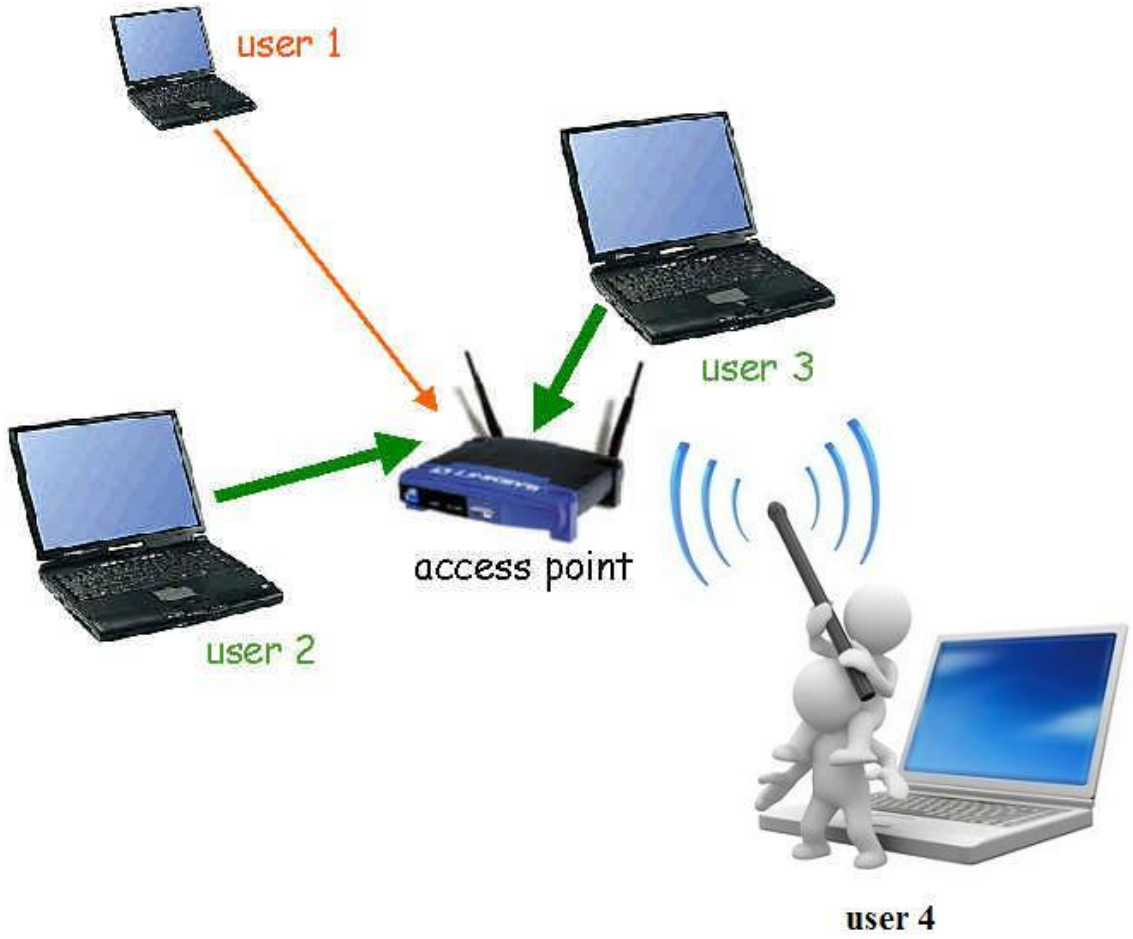
Consideriamo la seguente infrastruttura di rete



Supponiamo lo scenario seguente: l'utente *user 1* vuole accedere alla rete Wi-Fi. Per prima cosa, come accennato in precedenza, il protocollo di sicurezza avvia la fase di *autenticazione* per consentire a *user 1* di poter accedere ai servizi offerti dalla rete stessa.

Una volta che *user 1* ha effettuato la fase di autenticazione, decide di comunicare con *user2*.

In questo caso, il protocollo di sicurezza deve garantire una comunicazione sicura in modo da non permettere ad un attaccante di intercettare il contenuto della comunicazione (*Segretezza della comunicazione*).



Nello scenario di esempio *user 4* (attaccante del sistema) non deve poter intercettare la comunicazione tra *user 1* e *user 2*.

Infine, il protocollo di sicurezza deve garantire l' *Integrità dei dati* e quindi non deve permettere ad *user 4* di poter modificare un pacchetto inviato da *user 1* a *user 2*.

2. WEP

2.1. Introduzione

Come accennato nel capitolo precedente, il **WEP** (**W**ired **E**quivalent **P**rivacy) è stato il protocollo di protezione definito nella prima versione dello standard 802.11 per le reti wireless.

Nei primi anni in cui fu definito il WEP risultò essere un protocollo di protezione molto resistente agli attacchi in quanto utilizzava una chiave di 40 bit, tuttavia come vedremo in seguito, con il passare degli anni ci sono stati attacchi che hanno portato alla rottura dell'algoritmo stesso.

Il WEP è basato su di uno schema a chiave simmetrica, la quale è utilizzata sia per la fase di cifratura che di decifratura dei dati. Gli obiettivi principali forniti dal WEP sono:

- *Access Control* : prevenire gli accessi non autorizzati al sistema da parte di utenti che non presentano una chiave WEP corretta;
- *Privacy:* proteggere i dati della rete wireless tramite la loro codifica, mostrando la decodifica soltanto agli utenti che posseggono la corretta chiave WEP.

Lo standard 802.11 fornisce due schemi di definizione della chiave WEP. Il primo schema fornisce un insieme di chiavi condivise da tutte le stazioni della rete Wi-Fi (utenti, access point, etc.). Quando il cliente ottiene la chiave di default potrà comunicare con tutte le stazioni appartenenti alla rete. Il problema con la chiave di default è che quando essa è inviata a molte stazioni potrebbe essere compromessa da un attaccante che intercetterebbe così la comunicazione.

Nel secondo schema, invece, ogni utente stabilisce una " *key mapping relationship* " con un'altra stazione: questa è un'operazione più sicura perché meno stazioni conoscono la chiave. Tuttavia si presenta il problema di distribuzione della chiave quando il numero di stazioni cresce notevolmente.

Nel prossimo paragrafo andremo a descrivere in dettaglio quello che è il funzionamento del protocollo WEP.

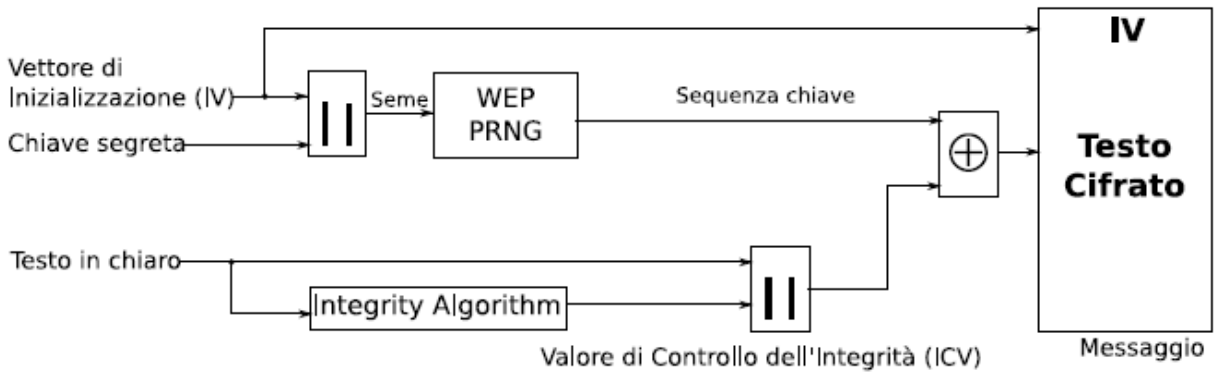
2.2. Struttura del protocollo

Il protocollo di protezione WEP usa lo stream cipher RC4 per la sicurezza e utilizza il CRC-32 per verificare l'integrità dei dati.

Come succede in quasi tutti gli stream cipher, anche in RC4 il testo cifrato è ottenuto effettuando uno XOR dei bit del testo in chiaro con una sequenza pseudo-random di bit ottenuta dalla chiave segreta.

Il testo cifrato è ottenuto quindi concatenando una chiave condivisa dalle due stazioni della rete (di 40 bit) con un vettore di inizializzazione IV (di 24 bit) che poi viene concatenato al pacchetto cifrato.

Nella figura sottostante possiamo vedere il funzionamento descritto dell'algoritmo utilizzato dal protocollo WEP



Come si evince dalla figura il cuore dell'algoritmo è il generatore di sequenze numeriche pseudo-random WEP-PRNG il quale sfrutta, come dicevamo in precedenza, per la fase di codifica l'algoritmo RC4 di RSA Data Security. Il WEP-PRNG è indispensabile in quanto trasforma una chiave relativamente corta in una sequenza pseudo-random arbitrariamente lunga.

Il vettore di inizializzazione, invece, è utilizzato per estendere la durata della chiave e fornisce il meccanismo di auto sincronizzazione. Solitamente è concatenato al messaggio in chiaro perché non fornisce nessuna informazione sulla chiave segreta. Come si vede dallo schema ad ogni vettore di inizializzazione corrisponde un nuovo seme e quindi una nuova sequenza chiave. Solitamente è buona norma cambiare tale vettore ad ogni MPDU(MAC Protocol Data Unit).

Infine per garantire l'integrità del messaggio, al testo da cifrare viene concatenato un ICV (Integrity Check Value) calcolato, come accennato già in precedenza, tramite la funzione CRC32. Tale valore è molto importante perché nella fase di decodifica viene ricalcolato e confrontato con quello ricevuto per vedere se vi è corrispondenza o meno.

2.3. Livello di sicurezza fornita dal protocollo WEP

Nonostante i progettisti del WEP nel 1999 consideravano tale protocollo sicuro, con il passar del tempo si sono dovuti ricredere per le tante vulnerabilità che nel corso degli anni sono state trovate e che quindi hanno abbassato notevolmente quello che è il livello di sicurezza fornito dal protocollo stesso.

Andremo in seguito a descrivere i 3 fattori principali che hanno caratterizzato molti dei problemi di sicurezza legati all'utilizzo del protocollo WEP:

a) *Lunghezza della chiave:* La lunghezza della chiave, che secondo i progettisti era il punto di forza del WEP visti i 40 bit, si è rilevata inadeguata. Infatti basti pensare che per un attacco di forza bruta un attaccante dovrebbe provare 2^{40} chiavi, che, visto soprattutto quelle che sono le risorse degli attuali computer, non è per niente proibitivo.
b) *Integrità del messaggio ottenuto tramite CRC32:* La funzione CRC32 si è rilevata insufficiente per garantire l'integrità del messaggio. Infatti ci sono degli attacchi che permettono, sfruttando alcune proprietà di questa funzione, di generare nuovi ICV validi senza dover necessariamente decifrare il messaggio originale.
c) *Riutilizzo del vettore di inizializzazione:* La specifica dello standard IEEE 802.11 non obbliga, pur consigliandolo, a cambiare il vettore di inizializzazione ad ogni messaggio inviato. Per le implementazioni che lo fanno tuttavia, ce ne sono comunque alcune che utilizzano un semplice contatore che incrementa il IV ad ogni messaggio e che viene resettato ad ogni riavvio della scheda. Questo può causare la ripetizione della key stream nei messaggi che ovviamente andrebbe evitata dato che può esporre a rischi di attacchi.

2.4. Alcune debolezze del WEP

Nel corso degli anni sono stati proposti molti attacchi al protocollo WEP sviluppati proprio a partire dalle lacune precedentemente descritte, tuttavia noi ne analizzeremo brevemente soltanto due nei sottoparagrafi successivi.

2.4.1. Riutilizzo della stessa Key stream

Abbiamo visto in precedenza che una delle vulnerabilità del WEP consiste nel riutilizzo del vettore di inizializzazione che può comportare la ripetizione della keystream tra diversi pacchetti. Infatti consideriamo il seguente scenario

$$C1 = P1 \text{ xor } RC4 (IV; k)$$

$$C2 = P2 \text{ xor } RC4 (IV; k)$$

allora

$$C1 \text{ xor } C2 = (P1 \text{ xor } RC4 (IV; k)) \text{ xor } (P2 \text{ xor } RC4 (IV; k)) = P1 \text{ xor } P2$$

Questo infatti ci dimostra che se si effettua lo XOR di due testi cifrati C1 e C2 utilizzando la stessa keystream (si noti che il vettore di inizializzazione IV e la chiave k sono le stesse sia nel calcolo di C1 che di C2) questa si elimina e otteniamo lo XOR dei due testi in chiaro P1 e P2.

2.4.2. Utilizzo del checksum di CRC32

Come detto in precedenza si possono sfruttare delle proprietà dell'algoritmo CRC32 per effettuare degli attacchi al protocollo WEP. Una di questa proprietà è il "checksum". Quest'ultima è una funzione del messaggio che non usa chiavi. Questo quindi può permettere ad un attaccante che non conosce la chiave, ma che conosce i testi in chiaro, di poter calcolare il checksum e quindi la keystream. Lo scenario è dimostrato di seguito

$$P \text{ xor } C = P \text{ xor } (P \text{ xor } RC4 (IV; k)) = RC4 (IV; k)$$

La conoscenza della keystream permette ad un attaccante di poter inviare pacchetti sulla rete pur senza conoscere la chiave segreta. Infatti lo standard IEEE 802.11 non vieta il riuso di una stessa keystream in messaggi sequenziali.

2.5. Possibili attacchi

Nei prossimi paragrafi saranno analizzati brevemente alcuni degli attacchi al protocollo WEP che sfruttano alcune delle debolezze accennate in precedenza.

2.5.1. FMS

Nel 2001 Fluhrer, Mantin, Shamir pubblicano il primo attacco al WEP.

Come abbiamo visto in precedenza il WEP è basato sullo stream cipher RC4; quest'ultimo è composto a sua volta da due algoritmi:

- *RC4-KSA*: trasforma una chiave di lunghezza variabile da 1 a 256 byte in una permutazione iniziale S di numeri da 0 a 255. Di seguito ne è mostrato il codice:

```
for i = 0 to 255
  S[i] = i                                    /*"S" indica l'array del cifrario
Next                                             ed è il seme*/
j = 0                                         /*in funzione di S gli indici i e j
for i = 0 to 255                                vengono azzerati*/
  j = (j + S[i] + key[i mod keylength]) mod 256
  swap (S[i], S[j])                           /*mod indica la dimensione dell'
next                                            array appunto 256 byte*/
```

- *RC4-PRGA*: genera un singolo byte della keystream per ogni permutazione S restituendo, quindi, il nuovo valore aggiornato di S. La figura sottostante ne mostra un'implementazione

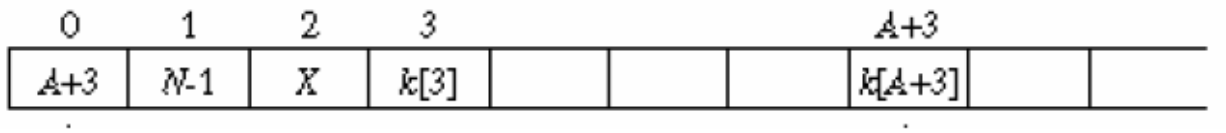
```
i = 0
j = 0
for l = 0 to len(input)                    /*il valore di input contiene il testo in
    i = (i + 1) mod 256                      chiaro mentre quello di output il
    j = (j + S[i]) mod 256                   risultato ovvero il testo criptato*/
    swap (S[i], S[j])
    output[l] = S[(S[i] + S[j]) mod 256] XOR input[l]
next
```

L'idea dell'attacco si basa sul fatto che, raccogliendo un numero sufficiente di pacchetti, è possibile individuare la chiave nel caso in cui il primo byte della keystream sia noto.

Prima di vedere in dettaglio l'attacco andiamo a considerare le seguenti informazioni:

- Nel protocollo 802.11b, ovvero quello utilizzato dalla rete wireless, il primo byte di qualsiasi pacchetto è fortunatamente costituito dall'intestazione SNAP (SubNetwork Access Protocol) che ha il valore di 0xAA. Applicando di conseguenza l'operatore XOR si arriva ad ottenere il primo byte del keystream.

- Gli IV deboli, che dobbiamo raccogliere, si trovano nella forma (A+3, N-1, X) dove A indica la posizione del byte da attaccare, N indica il modulo (nel nostro caso l'RC4 funziona in modulo 256), e X è un valore arbitrario casuale compreso tra 0 e 255. E' fondamentale ricordare che per attaccare un byte bisogna andare in ordine, ovvero bisogna conoscere quello prima; di conseguenza per partire bisogna scoprire per primo il byte 0.



Qui sopra è per l'appunto rappresentata la chiave d'inizializzazione K. Più specificatamente l'array K, formato dalla chiave e dall'IV spedito in chiaro alla fine del processo di cifratura, è organizzato nel seguente modo:

- L'IV che è formato da K[0], K[1] e K[2]
- La chiave WEP formata da K[3],…,K[Lunghezza della chiave] (40 o 104)

Supponiamo dunque che un eventuale attaccante conosca i primi A bytes della chiave K; egli potrebbe simulare nuovamente il processo KSA per recuperare i dati mancanti. Dato che la chiave è sconosciuta, l'array K viene caricato solo con i dati noti all'attaccante e l'array S viene riempito con valori sequenziali tra 0 e 255. A questo punto il KSA può essere avviato. Inizialmente vengono eseguiti A+3 passaggi del ciclo KSA con A che è all'inizio uguale a 0, dunque utilizzando solamente i primi tre bytes dell'IV. Il KSA con j che viene inizializzata a 0 viene fatto girare per i primi tre passaggi. A questo punto se S[0] o S[1] sono stati "disturbati" (ovvero se il valore di j in questo punto è inferiore di 2) il tentativo è andato a vuoto. Altrimenti j e S[A+3] vengono sottratti al primo byte del keystream, in mod 256. Le statistiche dateci dai tre autori affermano che questo potrebbe essere il byte corretto della chiave per il 5% delle possibilità, e per il restante 95% un byte casuale. A questo punto per riuscire ad alzare le probabilità al 50% se non oltre bisogna effettuare questo processo su circa 60 IV deboli (IV che lasciano trapelare informazioni sulla chiave). Fatto ciò e individuato uno dei bytes della chiave bisogna ripetere la procedura ottenendo così il byte successivo, ed è possibile fare ciò fino a

recuperare l'intera chiave. Per meglio comprendere questo difficile procedimento riporterò qui sotto una simulazione dell'inizializzazione del ciclo KSA nel quale però il mod sarà ridimensionato da 256 (com'è nell'RC4 originale con array a 256 byte) a 16 (quindi con array a 4 bit) e verrà riportata la notazione decimale per le cifre al posto di quella binaria. Tale scelta è effettuata per rendere facilmente comprensibile e molto più veloce il processo che deve servire solo a scopo esplicativo.

```
1  Output = 9
2  A = 0
3  IV = 3, 15, 2
4  Chiave = 1, 2, 3, 4, 5
5  Seme = IV e Chiave
6
7  K[] = 3 15 2 X X X X X X X X X X X X
8  S[] = 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

In questo primo riquadro ho riportato la situazione generale della chiave, dei byte e dell'IV che andiamo ad attaccare. In particolare notiamo in basso K[] che appunto indica l'array K dove possiamo vedere chiaramente l'IV (3 15 2) e S[] che è l'array S in cui sono inseriti valori sequenziali da 0 a 15 (perché ricordiamoci che questo processo è semplificato, con una chiave normale sarebbero da 0 a 255). A questo punto, come già spiegato prima, ciò che viene fatto è caricare l'array K con i soli valori che sono conosciuti (3 15 2) e l'array S con valori compresi nella fascia del mod.

Di seguito saranno mostrati i 3 passaggi di KSA

```
1  Primo Passaggio KSA
2
3  i = 0
4  j = j+S[i]+K[i] = 0+0+3 = 3
5  Swap S[i] e S[j]
6
7  K[] = 3 15 2 X X X X X X X X X X X X
8  S[] = (3) 1 2 (0) 4 5 6 7 8 9 10 11 12 13 14 15
```

```
Secondo passaggio KSA

i = 1
j = j+S[i]+K[i] = 3+1+15 = 3
Swap S[i] e S[j]

K[] = 3 15 2 X X X X X X X X X X X X X
S[] = 3 0 2 1 4 5 6 7 8 9 10 11 12 13 14 15
```

```
Terzo Passaggio KSA

i = 2
j = j+S[i]+K[i] = 3+2+2 = 7
Swap S[i] e S[j]

K[] = 3 15 2 X X X X X X X X X X X X X
S[] = 3 0 7 1 4 5 6 2 8 9 10 11 12 13 14 15
```

E' in questo punto che viene fatto appunto il controllo su j. Difatti se j fosse minore a 2 bisognerebbe rinunciare all'attacco ma in questo caso, come vedete (j = j+S[i]+K[i] = 3+2+2 = 7), j è maggiore di 2 visto che il suo valore è 7. A questo punto si procede con il calcolo spiegato in precedenza ovvero j e S[A+3] vengono sottratti dal primo byte di output del keystream dell'RC4. Perciò sempre seguendo l'esempio avremo:

```
S[A+3]  = 1
j       = 7
Output  = 9

(Output) - (j) - (S[A+3]) = 9-7-1 = 1 = corretto
```

Abbiamo dunque ottenuto il primo byte, il byte zero, che come possiamo verificare è corretto visto che la chiave era 1, 2, 3, 4, 5. Avendo ottenuto il byte zero possiamo ora procedere e recuperare il byte immediatamente seguente applicando lo stesso procedimento.

Nell'attacco FMS è infatti fondamentale ricordare che per attaccare un byte bisogna andare in ordine, ovvero bisogna conoscere quello precedente; di conseguenza per partire bisogna scoprire per primo il byte 0 e quindi andare a ricavare i byte successivi.

Tale attacco è statistico per sua natura, ogni pacchetto ci dà una probabilità del 5% associata all' ipotesi di chiave corretta ed una probabilità di 95% di ipotesi di

chiave errata. L'osservazione di un numero sufficiente di pacchetti, tuttavia, porta sicuramente alla rivelazione della shared key utilizzata da WEP.

L’attacco ha successo quasi al 50% quando si vanno ad analizzare dai 4.000.000 ai 6.000.000 di pacchetti.

2.5.2. Korek (ChopChop)

Nel 2004 un giovane hacker di nome KoreK ha teorizzato un attacco particolarmente efficace nei confronti del WEP, sfruttando la vulnerabilità dell'ICV. Tale attacco non recupera la chiave WEP, ma il keystream necessario per creare un pacchetto da iniettare nella rete per creare il traffico necessario al cracking della chiave WEP.

L’idea dell’attacco è la seguente:

- Troncando il byte finale a un messaggio cifrato C generico (intercettato) si ottiene un messaggio non valido C1;
- L'attacco Chopchop considera il valore troncato pari a 0, corregge C1 e lo inoltra all'Access Point. Possono ora verificarsi due situazioni:
    - il pacchetto viene accettato e "broadcastato" (injection attack);
    - il frame viene rifiutato e l'attacco continua (per al più 256 tentativi ovvero i possibili valori del byte) fino a che non viene ritenuto valido.

La procedura si ripete per risalire agli altri byte del messaggio finché non lo si ottiene integralmente.

L’attacco ha successo quasi al 50% quando si vanno ad analizzare all’in circa 700.000 pacchetti.

2.5.3. Analisi di Klein

Nel 2005 Andrea Klein presenta una dettagliata analisi di RC4 mostrando molte correlazioni tra la Keystream generata da RC4 e la chiave utilizzata dall’algoritmo stesso.

2.5.4. PTW

Nel 2007 Tews, Weinmann & Pyshkin usano l'analisi effettuata da Klein per creare "air crack-ptw", un tool freeware (scaricabile dal sito http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/) che è in grado di risalire a 104 bit dei 128 della chiave WEP in meno di un minuto.

L'attacco ha bisogno di 35000 - 40000 pacchetti per ottenere il 50 % di successo.

3. IEEE 802.11i

3.1. Introduzione

Per rispondere alle giustificate preoccupazioni delle aziende in merito alla sicurezza wireless offerta dal protocollo WEP, l'IEEE il 24 Giugno del 2004 ha ratificato il nuovo standard 802.11i.

Lo standard IEEE 802.11i definisce un'architettura di sicurezza scalabile che comprende politiche per l'autenticazione, la gestione delle chiavi e la segretezza ed integrità dei dati.

Quest'architettura di rete wireless è utilizzabile sia in grandi reti aziendali che in reti domestiche ed è chiamata Robust Security Network (RSN).

Una RSN è un'architettura molto complessa e permette solo la creazione di RSNAs (Robust Security Network Association) imponendo dei vincoli precisi ai dispositivi che si vogliono collegare alla rete. Una RSNA è una relazione di sicurezza basata sull'IEEE 802.11i 4-Way Handshake che garantisce un livello di protezione dei data frames superiore al WEP.

Anche se una RSN dovrebbe accettare esclusivamente dispositivi RSN, è stata prevista nello standard 802.11i un'architettura Transitional Security Network (TSN) dove possono accedere sia utenti RSN che utenti WEP che non hanno ancora dispositivi compatibili con RSN.

In questo capitolo mostreremo una ad una le fasi necessarie per stabilire una comunicazione RSNA:

1. **Accordo sulla politica di sicurezza:** in questa fase il client wireless identifica l'access point con cui vuole avviare la comunicazione ed insieme stabiliscono la politica di sicurezza da adottare. L'accordo sulla politica di sicurezza permette di definire alcune capacità di sicurezza principali come i protocolli da utilizzare per garantire la confidenzialità e l'integrità del traffico, un metodo di autenticazione ed un approccio per la generazione e la distribuzione delle chiavi.
2. **Autenticazione 802.1X o Pre-Shared Key:** durante questa fase se si utilizza l'autenticazione 802.1X, il client wireless ed il server di autenticazione (tipicamente un server RADIUS) provano la propria identità l'un l'altro. L'access point blocca il traffico di non autenticazione tra il client wireless ed il server di autenticazione finché l'autenticazione non và a buon fine. Se l'autenticazione và a buon fine il client wireless ed il server di

autenticazione avranno generato una Master Key (MK) comune. Nel caso di autenticazione Pre-Shared Key non viene utilizzato un server di autenticazione ma semplicemente una passphrase pre-condivisa tra il client wireless e l'access point. In questo caso non avviene una vera e propria autenticazione del client poiché la stessa passphrase è utilizzata da tutti i client associati allo stesso access point.

3. **Derivazione e distribuzione delle chiavi:** durante questa fase l'access point, il client wireless ed eventualmente un server di autenticazione RADIUS (che comunica la MK all'access point), eseguono diverse operazioni che permettono di generare ed installare chiavi crittografiche che verranno utilizzate nei protocolli che garantiscono la segretezza e l'integrità dei dati.
4. **Segretezza ed integrità dei dati:** in questa fase il client wireless e l'access point possono comunicare in modo sicuro, usando la politica di sicurezza e le chiavi crittografiche stabilite durate le prime tre fasi. Siccome la comunicazione sicura avviene solo tra il client wireless e l'access point, non viene assicurata sicurezza end-to-end (ad esempio nel sistema di distribuzione a cui l'access point è connesso).
5. **Chiusura della connessione:** durante questa fase il client wireless e l'access point chiudono la loro connessione sicura e cancellano la loro associazione terminando così la loro connessione wireless.

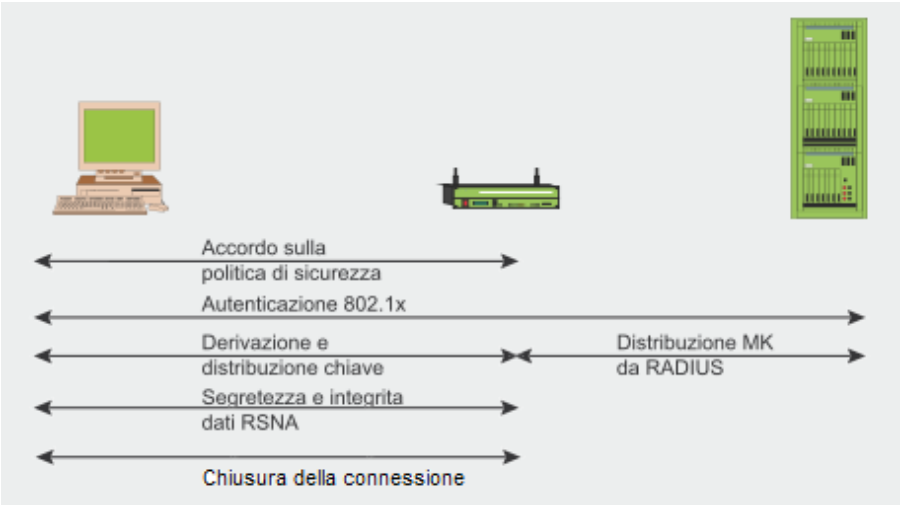


Figura 1: Fasi necessarie per stabilire una comunicazione in IEEE 802.11i

3.2. Fase 1: Accordo sulla politica di sicurezza

La prima fase per stabilire una comunicazione in IEEE 802.11i consiste nell'accordo sulla politica di sicurezza da adottare per le future comunicazioni tra l'access point (AP) ed il client wireless (STA).

Ci sono due modalità con cui l'STA può conoscere le politiche di sicurezza supportate dall'AP:

- l'AP le pubblicizza attraverso periodici messaggi Beacon
- l'AP le comunica attraverso un messaggio Probe Response dopo aver ricevuto un Probe Request dal client.

L'AP comunica le politiche di sicurezza supportate attraverso il campo RSN IE (Information Element) del frame Probe Response o del Beacon.

L'RSN IE contiene informazioni riguardo:

- metodi di autenticazione supportati (802.1X, Pre-Shared Key (PSK)),
- protocolli di sicurezza per traffico unicast (pairwise cipher suite: TKIP, CCMP),
- protocolli di sicurezza per il traffico multicast (group cipher suite: TKIP, CCMP),
- supporto per la pre-autenticazione per permettere agli utenti di pre-autenticarsi prima di passare ad un nuovo AP della stessa rete senza perdere la connessione.

Quando l'STA riceve le politiche di sicurezza supportate dall'AP, avvia una *autenticazione a sistema aperto* (Open System Authentication) che consiste semplicemente nello scambio delle reciproche identità (indirizzo MAC dell'STA e Service Set IDentifier dell'AP) tra le due parti e non offre alcun vantaggio in termini di sicurezza (sia l'indirizzo MAC che il SSID dell'AP possono essere clonati). Un'STA per avviare un tipo di autenticazione a sistema aperto, invia all'AP un frame di controllo MAC, chiamato frame di autenticazione (authentication request). L'AP risponde con il proprio frame di autenticazione (authentication response) e la procedura è completa.

Lo scopo di questa sequenza di frame (che non fornisce sicurezza) è semplicemente quello di mantenere retro compatibilità con lo standard IEEE 802.11.

A seguito dello scambio di questi frame di autenticazione, l'STA invia un frame di Association Request all'AP in cui specifica un insieme di politiche di sicurezza da lui supportate che sono state pubblicizzate dall'AP.

Nel caso in cui nessuna delle politiche di sicurezza pubblicizzate dall'AP sia compatibile con quelle disponibili sull'STA, l'AP rifiuta l'Association Request; altrimenti l'AP associa l'STA rispondendo con un frame Association Response in cui conferma la politica di sicurezza da adottare per le prossime comunicazioni.

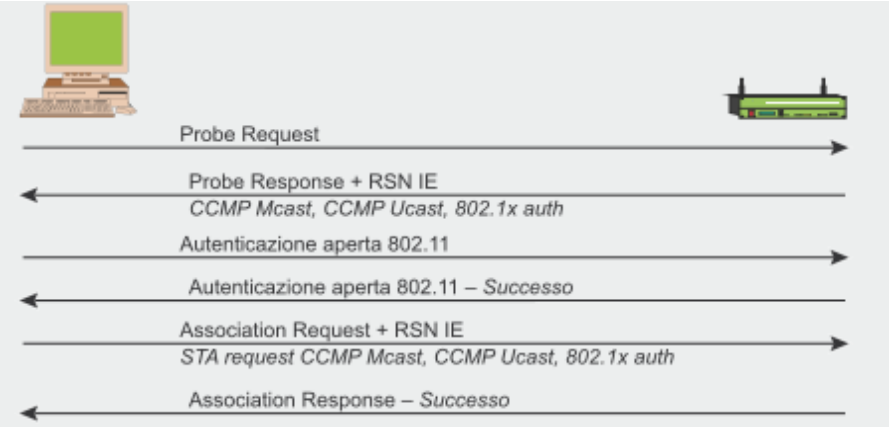


Figura 2: Accordo sulla politica di sicurezza

3.3. Fase 2: Autenticazione 802.1X o Pre-Shared Key

3.3.1. Autenticazione 802.1X

Dopo che l'STA ha concordato le politiche di sicurezza da adottare con l'AP, ha inizio l'autenticazione che è la seconda fase necessaria per stabilire una comunicazione RSNA in IEEE 802.11i.

L'autenticazione è una fase importante per prevenire accessi non autorizzati alle risorse della rete.

Lo standard IEEE 802.11i utilizza lo standard IEEE 802.1X che è un "Port-based access control mechanism", ovvero un sistema in grado di autenticare un utente collegato ad una determinata porta ethernet o ad un AP ed applicare di conseguenza il livello di sicurezza necessario.

L'architettura dello standard IEEE 802.1X ha tre componenti principali:

- il supplicant (o client) che entra nella rete
- l'autenticatore che fornisce il controllo sugli accessi
- il server di autenticazione che esegue le autorizzazioni

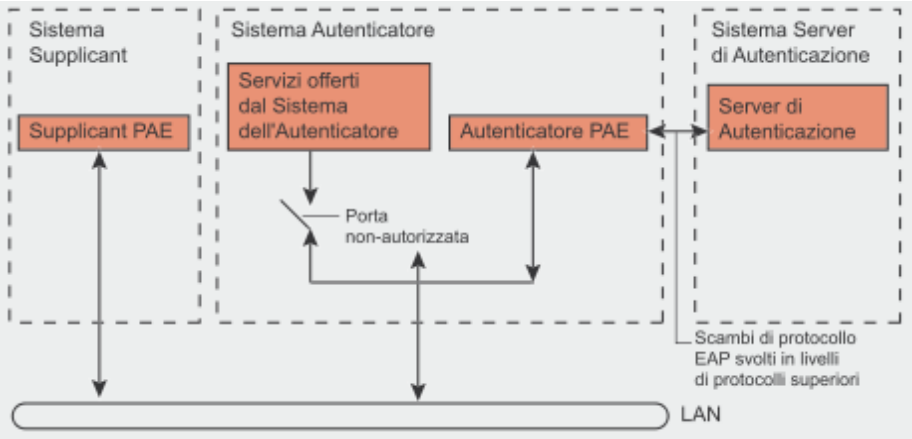


Figura 3: Modello IEEE 802.1X

Il sistema supplicant nelle reti wireless è rappresentato dall'STA, il sistema autenticatore è l'AP ed il sistema server di autenticazione in genere è un server RADIUS o un processo che gira su un AP nel caso di reti domestiche.

IEEE 802.1X controlla il flusso di dati tra l'AP (o il sistema di distribuzione) e l'STA usando un modello di porte controllate e non controllate.

Ogni porta fisica (porta virtuale nelle reti wireless) si divide in due porte logiche che compongono il PAE (Port Access Entity). La porta dell'autenticatore del PAE è sempre aperta (non controllata) e

permette di far passare i frame di autenticazione, mentre i servizi offerti dall'autenticatore sono accessibili al supplicant solo in seguito ad un'autenticazione andata a buon fine (porte controllate).

Il sistema autenticatore in questa architettura si limita a smistare le richieste di autenticazione del supplicant al server di autenticazione che permette l'accesso alla rete nel caso in cui l'utente sia autenticato ed autorizzato.

Il supplicant e l'autenticatore comunicano usando un protocollo Extensive Authentication Protocol (EAP). EAP è una framework per il trasporto di diversi metodi di autenticazione, che prevede solo un numero limitato di messaggi (Request, Response, Success, Failure), mentre gli altri messaggi intermediari dipendono dal metodo di autenticazione scelto.

Tra i possibili metodi EAP di autenticazione vi sono:

- **EAP-MD5** - Si tratta di un'autenticazione basata su MD5 dove un algoritmo di hash *one-way* viene usato in combinazione ad uno *shared secret* ed una *challenge*. L'algoritmo hash prende in input la challenge inviata dall'autenticatore e lo shared secret, e genera in output il valore hash che permette all'utente di autenticarsi. Il suo uso è sconsigliabile in ambiente wireless perché, come ogni metodo che utilizza richieste random e un algoritmo hash, è vulnerabile agli attacchi basati su dizionario. Se un potenziale intruso riesce ad ottenere la *challenge* e l'hash fornito come risposta, questo può provare a ricavare la password off-line. Inoltre, EAP-MD5 fornisce solo un'autenticazione del client non verificando la rete a cui ci si sta autenticando. In questo caso è possibile che un potenziale intruso, attraverso l'uso di un falso AP, possa ridirigere l'utente in una falsa rete e prendere informazioni preziose.
- **EAP-TLS** - Il Transport Layer Security (TLS) offre un'autenticazione sicura, che sostituisce le password con una autenticazione basata sui certificati digitali X.509. Al contrario di EAP-MD5, EAP-TLS supporta la "mutual authentication", ovvero sia il client che il server vengono verificati, evitando frodi relative all'inserimento di falsi AP. EAP-TLS è un'ottima scelta per la sicurezza dell'autenticazione in 802.1x quando una Public Key Infrastructure (PKI) è già stata adottata. Il grosso svantaggio di EAP-TLS è il costo elevato generato dalla manutenzione di una PKI: essa infatti richiede licenze software, personale

qualificato e corsi di formazione. Tra i vari meccanismi EAP, il TLS è lo standard più diffuso per l'autenticazione basata su 802.1x.

- **EAP-TTLS -** Tunneled Transport Layer Security (TTLS) è un estensione di EAP-TLS che è stata creata per evitare la necessità di certificati per i client. Come per altri sistemi di autenticazione "tunneling", TTLS è basato su un'autenticazione a due fasi. Nella prima fase un algoritmo asimmetrico basato sulla chiave del server è usato per verificare le credenziali del server e la creazione di un tunnel sicuro. Nella seconda fase, il client viene riconosciuto usando un secondo metodo di autenticazione che verrà fatto passare attraverso il tunnel sicuro creato precedentemente. Può essere usato un qualsiasi schema di autenticazione per la seconda fase.
- **EAP-PEAP -** Il Protected EAP (PEAP) è un protocollo di autenticazione progettato per Internet da Cisco, Microsoft e RSA. PEAP è simile al TTLS, in quanto sono gli unici due protocolli EAP di tipo "tunneling". Come per TTLS, viene creato un tunnel sicuro tra il server e il client in cui viene incapsulata l'autenticazione del client. Al contrario di TTLS, PEAP supporta il tunneling soltanto di protocolli di tipo EAP.
- **EAP-LEAP -** Light EAP (LEAP), chiamato anche Cisco EAP, è una implementazione proprietaria di Cisco che permette la "mutual authentication" e permette di usare username e password come meccanismo di autenticazione. Anche se una buona politica delle password può fare di LEAP un protocollo sicuro, esso è soggetto ad attacchi basati su dizionario così come EAP-MD5. Nonostante LEAP sia un protocollo proprietario di Cisco Systems, la casa di San Francisco si sta orientando verso i protocolli EAP-TLS e EAP-PEAP.

Il flusso dei messaggi di autenticazione tra il supplicant e l'autenticatore tipicamente utilizza il protocollo EAP over LAN (EAPOL) che permette di trasportare, mediante incapsulamento, EAP nei frame di protocolli di livello di collegamento di IEEE 802.

Per trasportare i messaggi EAP tra l'autenticatore ed il server di autenticazione in genere viene utilizzato il protocollo RADIUS (Remote Authentication Dial-In User Service).

RADIUS è utilizzato come meccanismo per la gestione dell'AAA (Autenticazione, Autorizzazione, Accounting). L'autenticazione è il processo di verifica dell'identità dichiarata da un utente; l'autorizzazione coinvolge un insieme di regole per decidere cosa può fare un utente autenticato all'interno di un sistema, ed infine l'accounting definisce e stima le risorse di cui un utente può trarre vantaggio durante l'accesso. La motivazione che ha portato alla diffusione di RADIUS è stata la necessità di avere un server centrale di autenticazione per tutti gli utenti che volessero accedere alla rete. E' possibile quindi usare un server RADIUS per fornire la centralizzazione delle decisioni di autenticazione.

Le fasi necessarie prima che 802.1X permetta l'accesso di un supplicant alla rete sono:

1. Il supplicant (STA) richiede l'accesso alla WLAN. Un autenticatore (AP) chiede l'identità al supplicant. Nessun altro tipo di traffico è permesso a questo punto, la "porta" è chiusa.
2. Il supplicant risponde all'autenticatore con i dati dell'identità che stabiliscono le sue credenziali. In genere non viene inviata la vera identità prima che sia stabilita una sessione cifrata.
3. Dopo che l'identità è stata inviata ha inizio il processo di autenticazione. L'autenticatore re-incapsula i messaggi EAPOL nel formato RADIUS e li passa al server di autenticazione. Durante il processo di autenticazione, l'autenticatore smista semplicemente i pacchetti tra il supplicant ed il server di autenticazione.
4. Ogni processo di autenticazione è leggermente diverso, a seconda del tipo di autenticazione EAP utilizzato, tuttavia supplicant e server di autenticazione si scambiano i messaggi adatti per generare una comune master key (MK).

5. Alla fine della procedura, se il server di autenticazione invia un messaggio di successo, l'autenticatore “apre la porta” per il supplicant e l'accesso alla rete è concesso. Altrimenti vene inviato un messaggio di errore, la porta non viene aperta ed il supplicant è libero a questo punto di tentare di nuovo l’autenticazione.

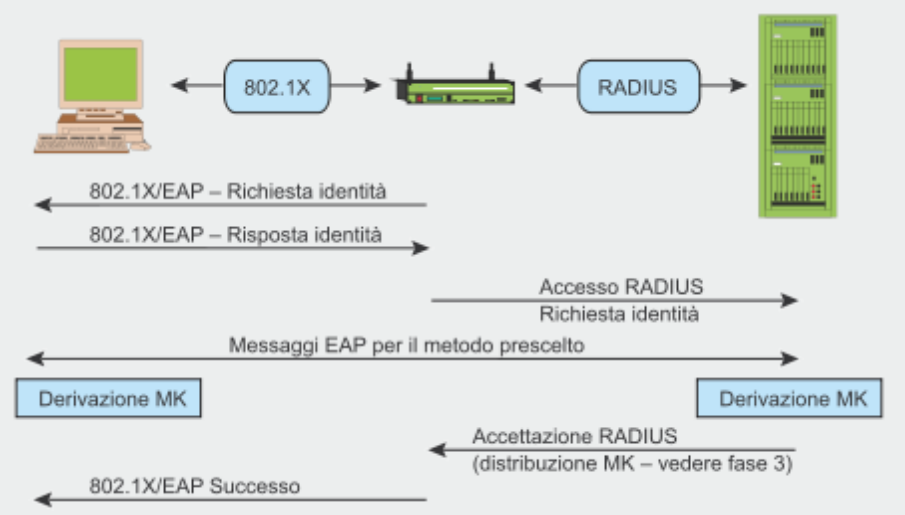


Figura 4: Autenticazione 802.1X

3.3.2. Autenticazione Pre-Shared Key (PSK)

Nelle reti in cui non è presente un server di autenticazione, un'alternativa all'autenticazione 802.1X è quella attraverso Pre-Shared Key (PSK).

Con l'autenticazione attraverso PSK non avviene nessuna transazione esplicita di autenticazione.

Se la PSK è unica per ogni STA, l'STA e l'AP si autenticano reciprocamente possedendo un'identica Pre-Shared Key, senza la quale la riservatezza e l'integrità dei dati non potrebbero essere garantiti.

In pratica, molti AP utilizzano una singola PSK per tutte le STA. Ciò significa che, piuttosto che autenticare il client, l'AP verifica che il client sia un membro di un gruppo autorizzato (il gruppo che condivide la chiave). L'effettiva identità del client non viene stabilita, per cui questa non è un'autenticazione del client nel senso normale del termine. Tuttavia, l'STA autentica l'AP. Tipicamente, la fase di autenticazione in un'RSNA, prevede l'autenticazione reciproca tra un'STA ed un server di autenticazione, e la consegna di una comune master key (MK) di sessione all'AP e, talvolta, all'STA. Tuttavia, in un'RSNA che ha negoziato PSK durante la fase di accordo sulle politiche di sicurezza, la fase di autenticazione non è necessaria perché la chiave PSK è già stata distribuita ed installata in modo da rendere implicita la condizione di autenticazione.

3.4. Fase 3: Distribuzione e gerarchia di chiavi

La sicurezza nelle connessioni dipende molto dalle chiavi segrete utilizzate dagli algoritmi di cifratura. Nella RSN, ogni chiave ha una vita limitata e la sicurezza generale è garantita da un insieme di diverse chiavi, organizzate gerarchicamente. Quando viene stabilito un contesto di sicurezza dopo un'autenticazione andata a buon fine, le chiavi temporanee (di sessione) vengono create e aggiornate regolarmente fino a quando il contesto di sicurezza non viene chiuso.

In questo paragrafo analizzeremo la fase a cui sono affidati i compiti di generazione e scambio delle chiavi.

Si hanno due handshake durante le derivazione delle chiavi:

- Handshake a quattro vie per la derivazione della PTK (Pairwise Transient Key) e della GTK (Group Transient Key);
- Group Key Handshake per il rinnovo della GTK.

La derivazione della PMK (Pairwise Master Key) dipende dal metodo di autenticazione usato:

- se viene usata una PSK (Pre-Shared Key), PMK = PSK. La PSK viene generata dalla passphrase (da 8 a 63 caratteri) o da una stringa di 256 bit e fornisce una soluzione per le reti domestiche e di piccole imprese che non hanno un server di autenticazione;
- se viene usato un server di autenticazione, la PMK è derivata dall'autenticazione 802.1X MK.

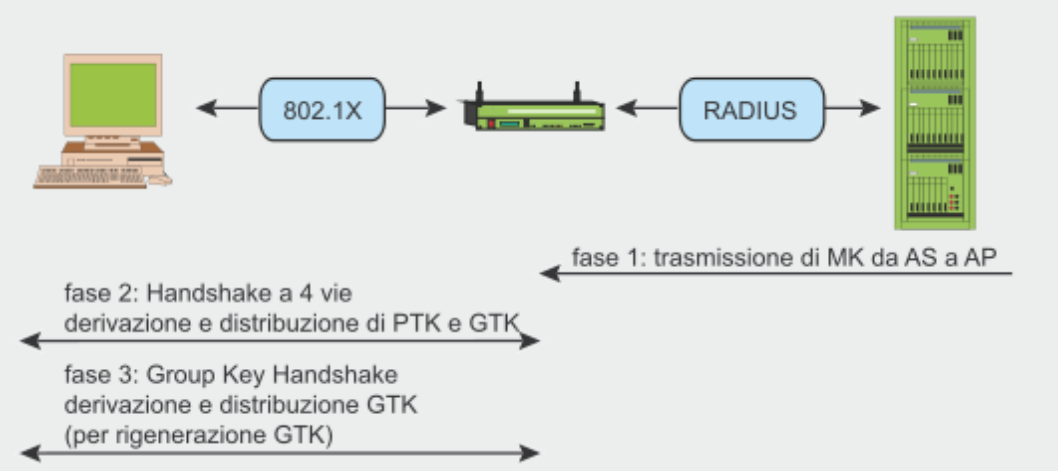


Figura 5: Derivazione e distribuzione di chiavi

La PMK stessa non è mai usata per il controllo di cifratura o integrità. Questa viene utilizzata per generare una chiave di cifratura temporanea per il traffico unicast PTK (Pairwise Transient Key).

La funzione utilizzata per la derivazione della PTK in IEEE 802.11i è la seguente:

802.11i-PRF(*K, A, B, Len*)

R **←** **“”**

for *i* **←** **0 to ((*Len*+159)/160) – 1) do**

R **←** ***R*** **|| HMAC-SHA1(*K, A* || *B* || *i)***

return Truncate-to-len(*R, Len*)

- K = PMK (Pairwise Master Key)
- A = una stringa fissa (“Pairwise key expansion”)
- B = min(AP-Addr, STA-Addr) || max(AP-Addr, STA-Addr) || min(ANonce, SNonce) || max(ANonce, SNonce)
- Len = lunghezza della chiave da generare (TKIP=512; CCMP=384)

La lunghezza della PTK dipende dal protocollo di cifratura: 512 bit per TKIP e 384 bit per CCMP.

La PTK consiste di diverse chiavi temporanee:

- KCK (Key Confirmation Key – 128 bit): Chiave per i messaggi di autenticazione (MIC) durante l’handshake a 4 vie e la Group Key Handshake;
- KEK (Key Encryption Key – 128 bit): Chiave per garantire la segretezza durante l’handshake a 4 vie e la Group Key Handshake;
- TK (Temporary Key – 128 bit): Chiave per la cifratura dei dati (usata per TKIP o CMMP);
- TMK (Temporary MIC Key – 2x64 bit): Chiave per l'autenticazione dei dati (usata solo da Michael con TKIP). Una chiave dedicata è usata per ogni lato delle comunicazione.

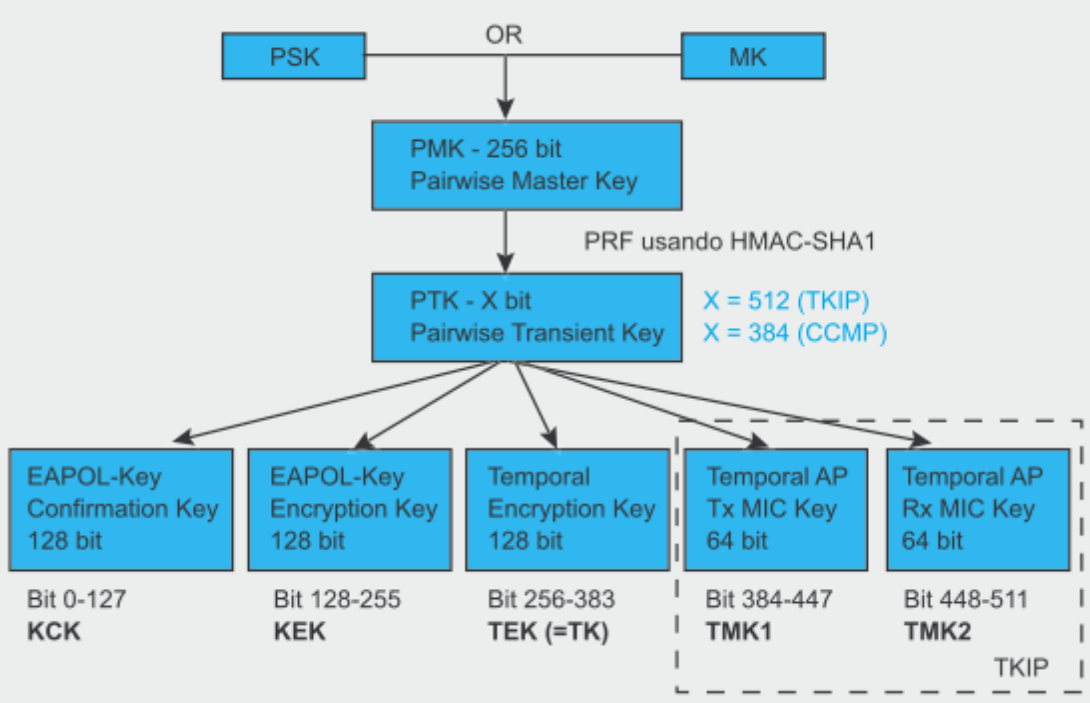


Figura 6: Pairwise Key Hierarchy

Tramite l'handshake a 4 vie, iniziato dal punto di accesso, è possibile:

- confermare la conoscenza del client della PMK,
- derivare una nuova PTK,
- installare chiavi di cifratura e di integrità,
- cifrare il trasporto della GTK,
- confermare la selezione di cifratori.

Durante l'handshake a 4 vie sono scambiati quattro messaggi EAPOL-Key tra il client ed il punto di accesso.

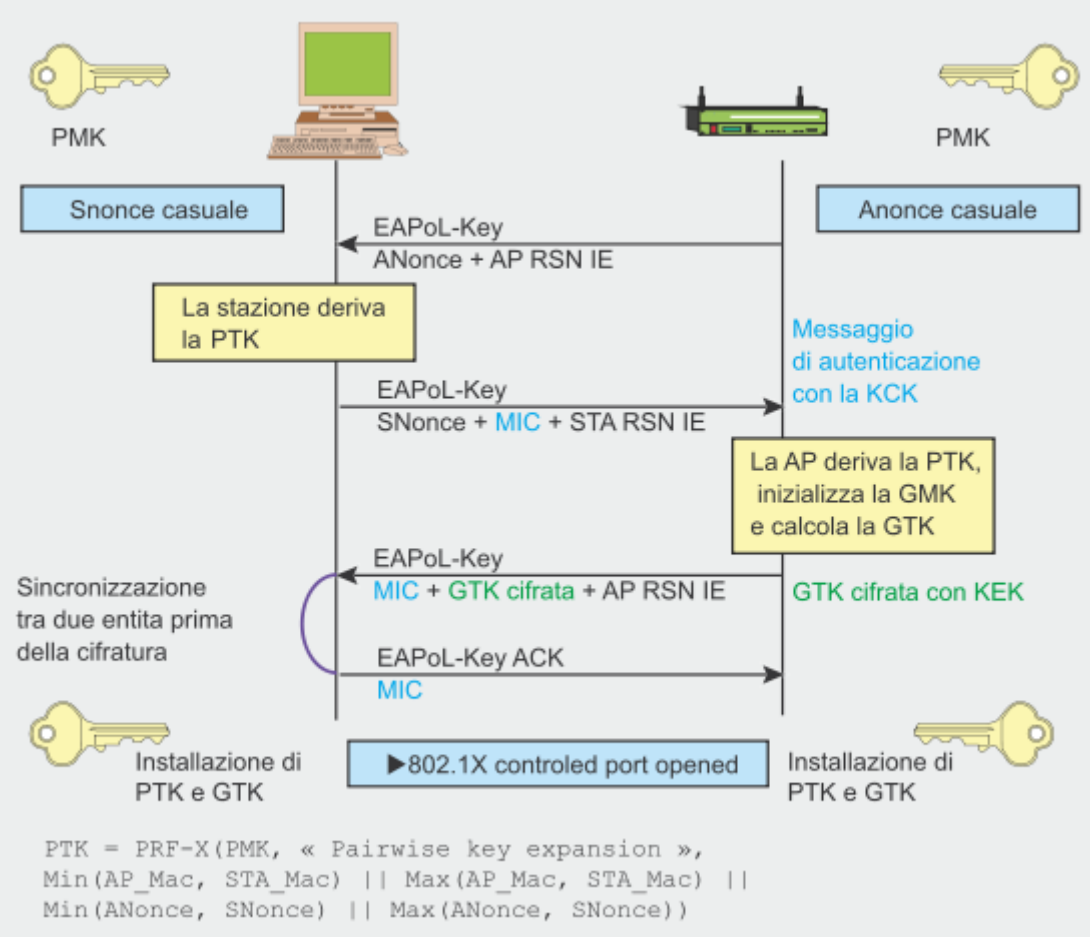


Figura 7: Handshake a 4 vie

L'AP inizializza il primo messaggio selezionando il numero casuale ANonce e lo invia al supplicant, senza cifrare il messaggio.

Il supplicant genera il proprio numero causale SNonce e adesso può calcolare una PTK e le chiavi di derivazione temporanee, quindi invia SNonce e la MIC calcolata dal secondo messaggio usando la chiave KCK.

Quando l'AP riceve il secondo messaggio, può estrarre SNonce (perché il messaggio non è cifrato) e calcolare la PTK e le chiavi di derivazione temporanee. Adesso l'AP può verificare il valore della MIC del secondo messaggio ed essere sicuro che il supplicant conosca la PMK e che abbia calcolato correttamente la PTK e le chiavi di derivazione temporanee.

A questo punto l'AP genera la chiave GTK e, dopo averla cifrata con la chiave KEK, la invia al supplicant attraverso il terzo messaggio insieme alla MIC calcolata dal terzo messaggio usando la chiave KCK.

Quando il supplicant riceve questo messaggio, la MIC viene controllata per essere sicuri che l'AP conosca la PMK e abbia calcolato correttamente la PTK e le chiavi di derivazione temporanee.

L'ultimo messaggio riconosce il completamento dell'intero handshake e indica che il supplicant adesso installerà le chiavi ed inizierà la comunicazione cifrata.

Dopo la ricezione, l'AP installa le proprie chiavi dopo aver verificato il valore MIC. Quindi, il dispositivo mobile e l'AP hanno ottenuto, calcolato e installato le chiavi di cifratura e adesso sono in grado di comunicare su un canale sicuro per traffico unicast e multicast.

Mentre il traffico unicast è protetto dalle chiavi derivate dalla PTK, Il traffico multicast è protetto da un'altra chiave, la GTK (Group Transient Key) generata da una chiave principale detta GMK (Group Master Key), una stringa fissa, l'indirizzo MAC del punto di accesso ed un numero casuale GNonce. La lunghezza GTK dipende dal protocollo di cifratura – 256 bit per la TKIP e 128 bit per la CCMP.

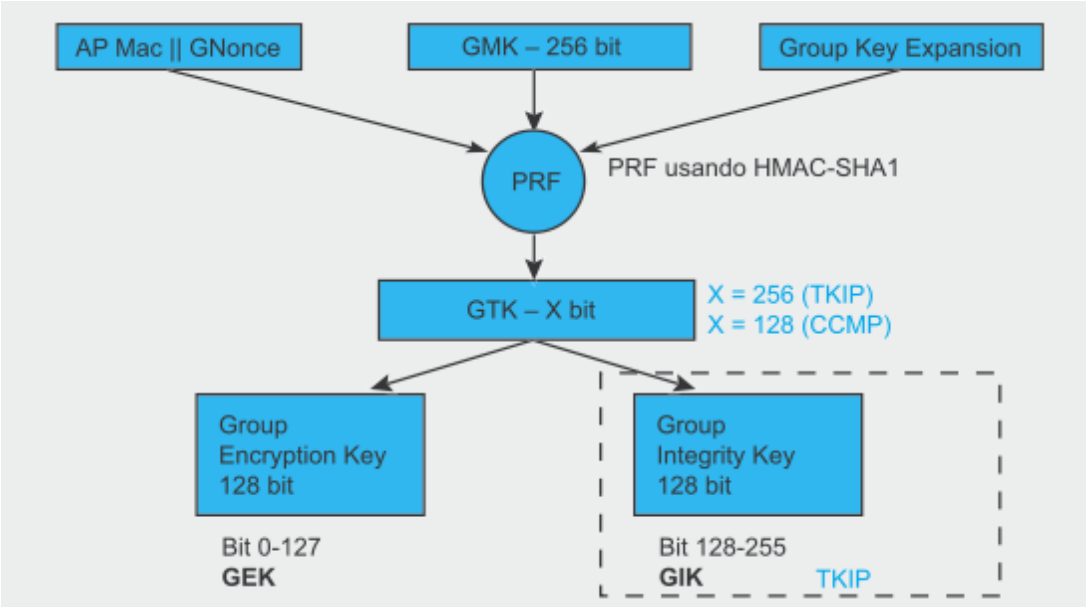


Figura 8: Generazione da parte dell'AP della GTK e della conseguente Group Key Hierarchy

La GTK si divide in diverse chiavi temporanee:

- GEK (Group Encryption Key): Chiave per la cifratura dei dati (usata da CCMP per l'autenticazione e la cifratura e dalla TKIP);
- GIK (Group Integrity Key): Chiave per l'autenticazione dei dati (usata solo da Michael con TKIP).

Durante il Group Key Handshake vengono scambiati due messaggi EAPOL-Key tra il client ed il punto di accesso. Questo handshake fa uso di chiave temporanee generate durante l'handshake a 4 vie (KCK e KEK).

Il Group Key Handshake è richiesto solo per disassociare un host e per rigenerare la GTK su richiesta di un client. L'AP inizializza il primo messaggio scegliendo il numero causale GNonce e calcolando una nuova GTK. Poi invia al supplicant la GTK cifrata (usando KEK), il numero di sequenza GTK e la MIC calcolata da questo messaggio usando KCK. Quando il supplicant riceve il messaggio, la MIC viene verificata e la GTK può essere decifrata. Il secondo messaggio riconosce il completamento della Group Key Handshake inviando un numero di sequenza e la MIC calcolata su questo secondo messaggio. Dopo la ricezione, l'AP verifica il valore MIC ed installa la nuova GTK.

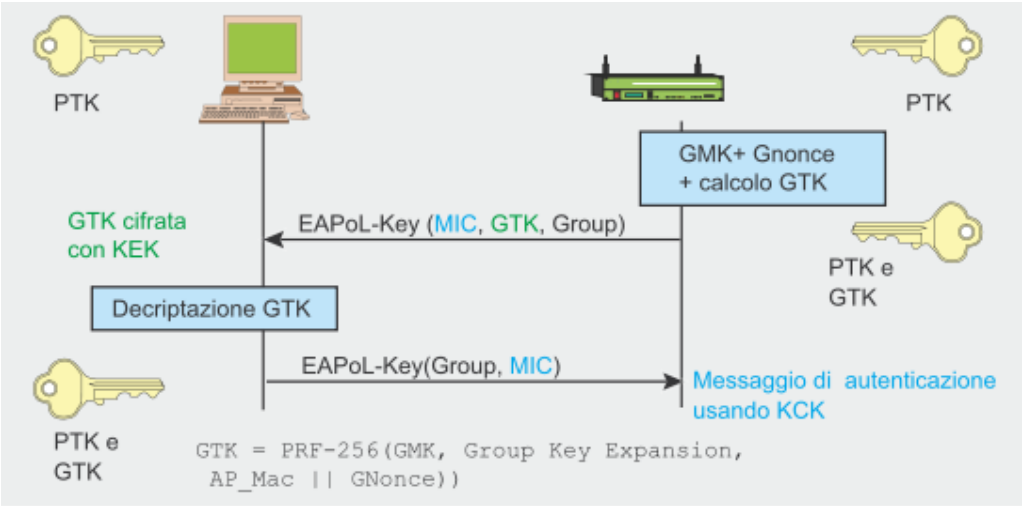


Figura 9: Group Key Handshake

Esiste anche una STAkey Handshake che supporta la creazione dal punto di accesso di chiavi segrete transitorie chiamate STAkey per le connessioni ad-hoc.

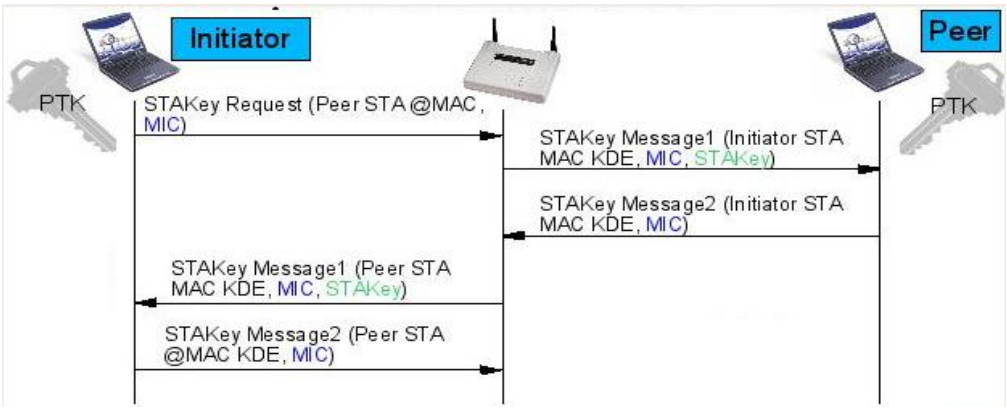


Figura 10: STAkey Handshake (STAKey cifrata con KEK)

3.5. Fase 4: Segretezza ed integrità dei dati

Tutte le chiavi generate in precedenza sono usate nei protocolli che supportano la segretezza e l'integrità dei dati RSNA:

- TKIP (Temporal Key Integrity Protocol)
- CCMP (Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol)
- WRAP (Wireless Robust Authenticated Protocol)

Prima di analizzare in dettaglio questi protocolli dobbiamo capire un concetto importante: la differenza che passa tra un MSDU (MAC Service Data Unit) ed un MPDU (MAC Protocol Data Unit). Entrambi si riferiscono ad un singolo pacchetto di dati, ma il MSDU rappresenta i dati prima della frammentazione, mentre gli MPDU sono unità di dati multipli dopo la frammentazione. La differenza è importante nella cifratura TKIP e CCMP, dal momento che in TKIP la MIC viene calcolata dal MSDU, mentre nel CCMP viene calcolata dal MPDU.

3.5.1. TKIP (Temporal Key Integrity Protocol)

Proprio come WEP, la TKIP si basa sull'algoritmo di cifratura RC4, ma esiste per una sola ragione: per permettere ai sistemi WEP di essere aggiornati e implementare protocolli più sicuri. La TKIP è richiesta per la certificazione WPA ed è anche inserita nel RSN 802.11i come opzione facoltativa. La TKIP aggiunge anche misure correttive per tutte le vulnerabilità WEP descritte prima:

- integrità del messaggio: una nuova MIC (Message Integrity Check) chiamata Michael che può essere implementata nei software che girano su microprocessori lenti;
- initialization vector (IV): nuove regole di selezione per i valori IV, riutilizzando il vettore IV come contatore replay (TSC, o TKIP Sequence Counter) e aumentando le dimensioni del vettore IV per evitare il riutilizzo;
- funzione Per Packet Key Mixing: per generare chiavi di cifratura apparentemente non legate;
- gestione chiave: nuovo meccanismo per la distribuzione e la modifica delle chiavi.

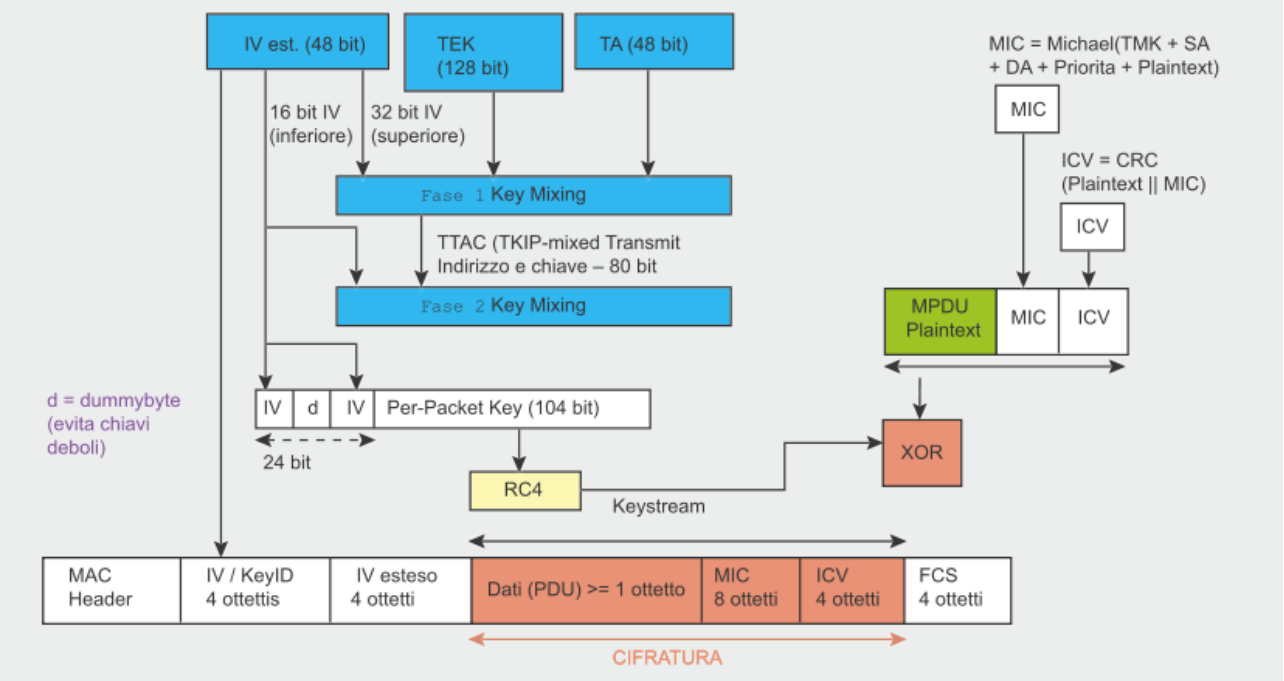


Figura 11: Modello TKIP Key-Mixing e cifratura

Il modello TKIP Key-Mixing si divide in due fasi:

1. La Fase 1 riguarda i dati statici – la chiave di sessione segreta TEK, l'indirizzo trasmettitore MAC TA (per prevenire le collisioni tra vettori IV) e i 32 bit più alti del vettore IV.

   L'output di questa fase è una chiave intermedia che servirà da input per la fase 2.

2. La Fase 2 dipende dall'output della Fase 1 e comprende i 16 bit più bassi del vettore IV, modificando tutti i bit del campo Per Packet Key per ogni nuovo IV. Il valore IV inizia sempre con 0 ed è aumentato di 1 per ogni pacchetto inviato, con il rifiuto di qualsiasi messaggio il cui TSC non è più grande dell'ultimo messaggio.

L'output della Fase 2 e parte del IV esteso (più un dummy byte per evitare chiavi deboli) sono l'input per l'RC4, e generano un keystream con un operatore XOR con un MPDU in testo in chiaro, la MIC calcolata dalla MPDU ed il vecchio ICV di WEP.

La figura 12 mostra come avviene la fase di codifica e decodifica utilizzando TKIP.

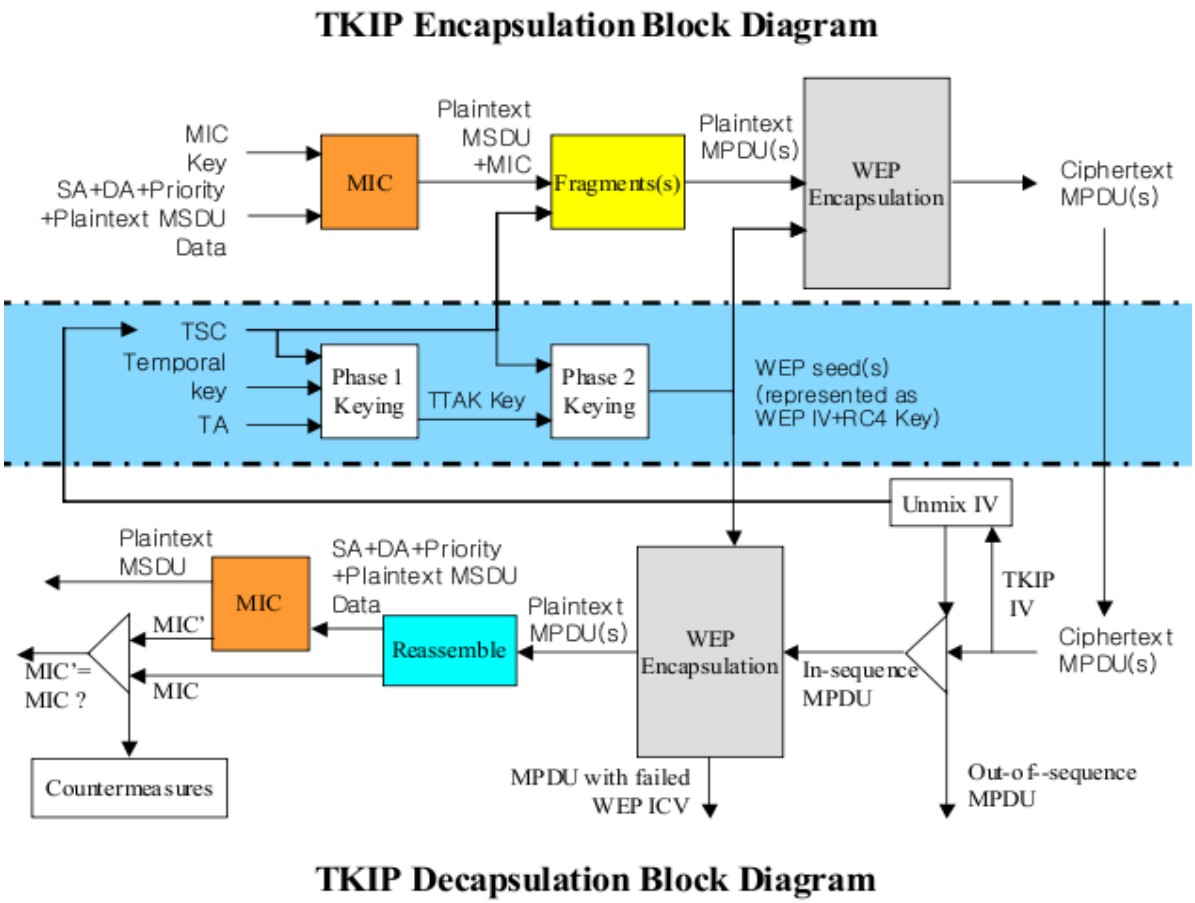


Figura 12: TKIP block diagram

Il calcolo MIC utilizza l'algoritmo Michael di Niels Ferguson. Venne creato per la TKIP ed ha un livello di sicurezza di 20 bit (l'algoritmo non usa la moltiplicazione per ragioni di prestazioni, poiché deve essere supportato da hardware wireless di vecchia generazione che deve essere aggiornato per il WPA). A causa di questi limiti, delle contromisure sono necessaire per evitare alterazioni MIC.

I guasti MIC devono essere ridotti a due al minuto, altrimenti viene applicato un blackout di 60 secondi e le nuove chiavi (GTK e PTK) devono essere ristabilite in un secondo momento. Micheal calcola un valore di controllo di 8 ottetti chiamato MIC e lo aggiunge al MSDU prima della trasmissione.

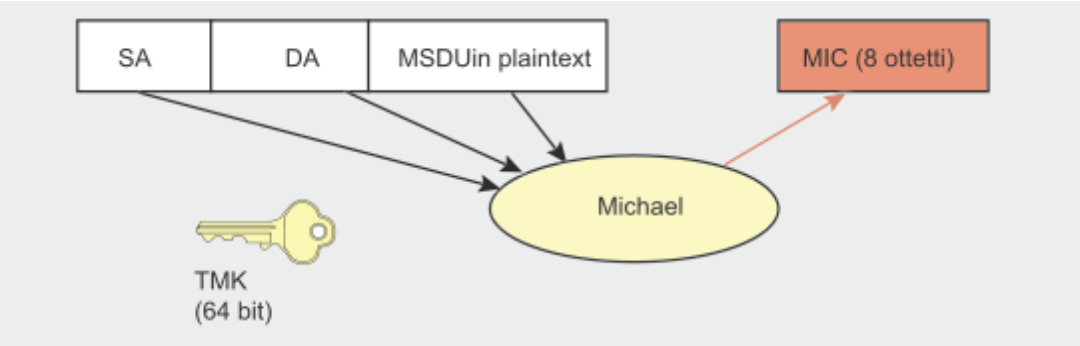


Figura 13: Calcolo MIC con algoritmo Michael

Il MIC viene calcolato dall'indirizzo di origine (SA), indirizzo di destinazione (DA), MSDU in testo in chiaro e la TMK appropriata (a seconda dei casi, viene usata una chiave diversa per la trasmissione e la ricezione).

3.5.2. CCMP (Counter-Mode / CBC MAC Protocol)

Il CCMP si basa sulla suite del cifrario a blocchi AES (Advanced Encryption Standard) in modalità CCM con le chiavi e i blocchi di 128 bit. AES è per CCMP quello che RC4 è per TKIP, ma al contrario di TKIP che era stato creato per accogliere l'hardware WEP esistente, CCMP non è un ibrido bensì un nuovo protocollo. Il CCMP utilizza Counter Mode (CTR) per la confidenzialità combinato con un metodo di autenticazione di messaggio chiamato Cipher Block Chaining (CBC-MAC) che produce un MIC.

Esso aggiunge altre funzionalità interessanti, come l'uso di una singola chiave per la cifratura e l'autenticazione (con diversi vettori di inizializzazione) e l'autenticazione dei dati non cifrati.

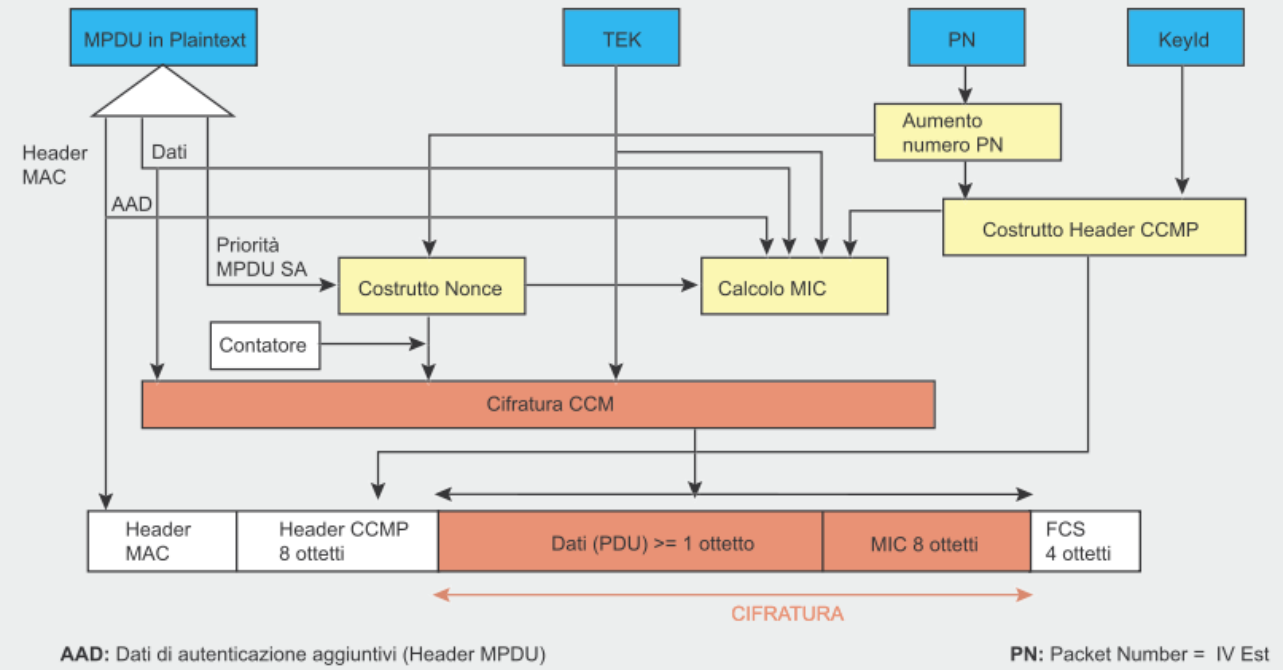


Figura 14: Cifratura CCMP

Il protocollo CCMP aggiunge 16 byte alla MPDU: 8 byte per l'intestazione CCMP e 8 byte per il MIC. L'intestazione CCMP è un campo non cifrato incluso tra l'intestazione MAC ed i dati cifrati, ed include il PN di 48 bit (Packet Number = IV esteso) ed il KeyID (un byte che contiene: Ext IV (bit 5), Key ID (bits 6-7), ed un campo riservato (bits 0-4). Il PN viene aumentato di uno per ogni MPDU successivo. Il calcolo MIC utilizza l'algoritmo CBC-MAC che cifra il blocco nonce di partenza (calcolato dai campi Priority, l'indirizzo di origine dell'MPDU ed il PN aumentato) ed esegue lo XOR con i blocchi successivi per ottenere una MIC finale di 64 bit (la MIC finale è un blocco di 128 bit però i 64 bit più bassi vengono ignorati). Il MIC viene poi aggiunto ai dati in testo in chiaro per la cifratura AES in modalità contatore. Il contatore è costruito da un nonce simile a

quello del MIC, ma con un campo contatore in più inizializzato ad 1 ed incrementato per ogni blocco.

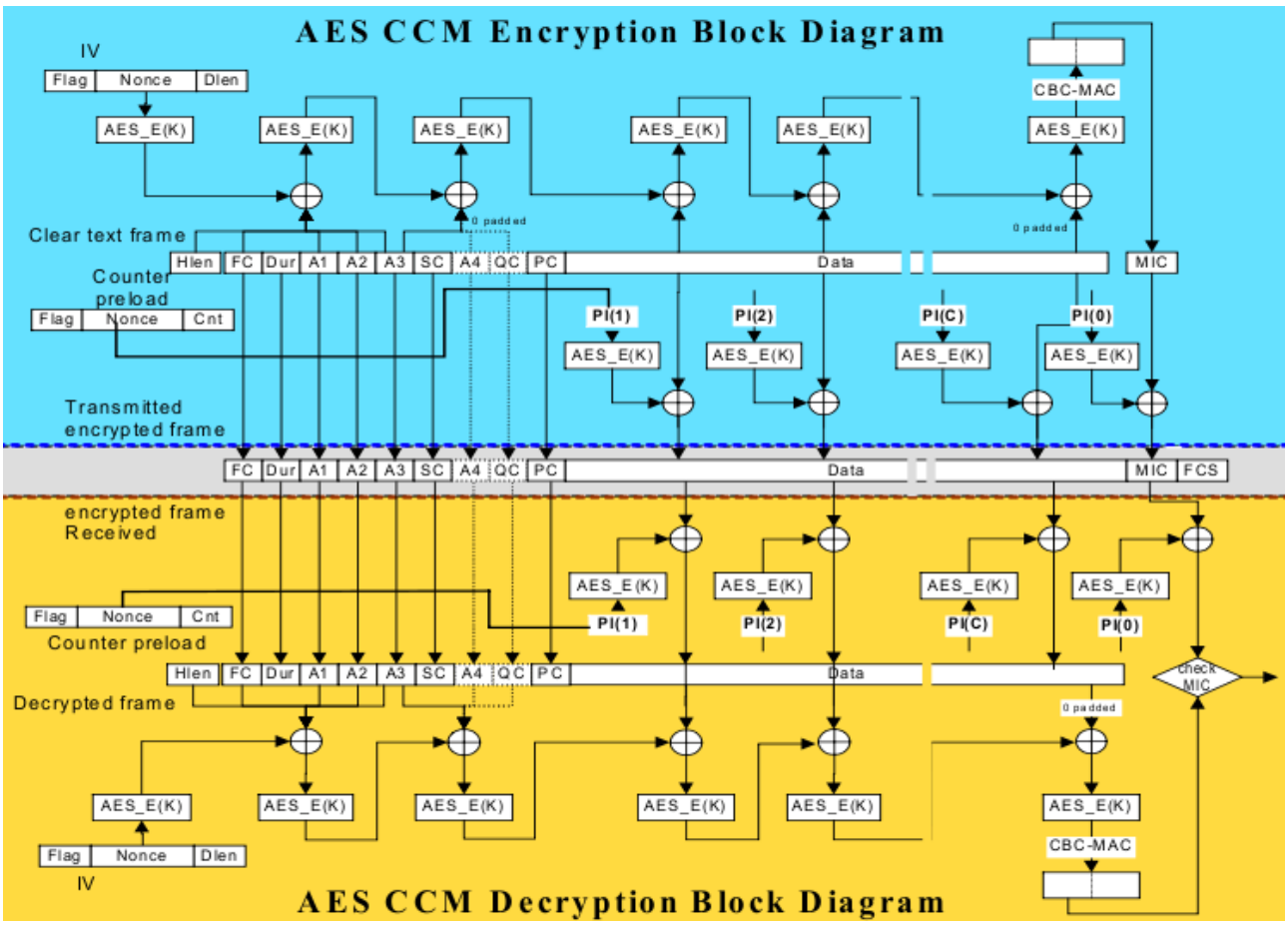


Figura 15: AES CCMP block diagram

L'ultimo protocollo è WRAP, basato anch'esso su AES, ma che utilizza il modello di cifratura autenticato OCB (Offset Codebook Mode, cifratura e autenticazione in un unico calcolo).

Il modello OCB fu il primo scelto dal gruppo di lavoro di IEEE 802.11i, ma venne poi abbandonato a causa di problemi legati alla proprietà intellettuale e le tariffe della licenza. Il CCMP venne allora adottato come metodo obbligatorio.

3.6. Fase 5: Chiusura della connessione

La quinta ed ultima fase di una comunicazione RSNA è la fase di terminazione della connessione. Durante questa fase, l'associazione tra l'STA e l'AP viene cancellata e la connessione wireless viene terminata attraverso i seguenti eventi:

- L'AP deautentica l'STA.
- Le associazioni di sicurezza, usate internamente dall'AP per tener traccia delle associazioni tra STA ed AP vengono eliminate.
- Le chiavi temporanee usate per cifrare e proteggere l'integrità del traffico dati vengono cancellate.
- Le porte controllate in IEEE 802.1X ritornano in uno stato bloccato in modo che il traffico dell'utente non possa più passare.

La fase di chiusura della connessione può essere iniziata in diversi modi, inclusi i seguenti:

- Si perde la comunicazione radio tra l'STA e l'AP (e.g. l'STA si muove fuori dalla portata dell'AP).
- Si ha un timeout durante l'esecuzione dell'handshake a 4 vie o del Group Key Handshake.
- Non c'è accordo sulla politica di sicurezza da adottare.
- L'utente spegne l'STA o disattiva l'interfaccia di rete wireless.
- La politica di sicurezza implica una terminazione della connessione.

Questa fase riporta l'AP e l'STA nello stato iniziale, in questo modo sarà possibile stabilire nuove connessioni ricominciando dalla prima fase.

4. Wireless Protected Access (WPA)

4.1. Funzionalità di WPA

Prima che lo standard 802.11i venisse completamente definito, il gruppo Wi-Fi Alliance (consorzio di fornitori Wi-Fi), fornì un protocollo di sicurezza chiamato Wireless Protected Access (WPA) basato solo su alcune delle funzionalità presenti nello standard 802.11i.

Questo protocollo aveva il compito di risolvere le vulnerabilità riscontrate in WEP che all'epoca era l'unica protezione di sicurezza disponibile per IEEE 802.11.

Per risolvere queste vulnerabilità WPA sfrutta le seguenti principali caratteristiche di sicurezza di IEEE 802.11i:

- Il cambiamento di chiave è una caratteristica integrata nel WPA, nonostante si possa scegliere una chiave condivisa a priori, come nel WEP, chiamata PSK (Pre-Shared Key), è preferibile utilizzare l'autenticazione IEEE802.1X che prevede un server per la scelta e la distribuzione delle chiavi ai client.
- Generazione e distribuzione delle chiavi basati sul 4-Way Handshake di IEEE 802.11i.
- Cifratura TKIP che include:
  - La lunghezza del vettore IV è stata raddoppiata (da 24 bit a 48) portando le combinazioni da 16,7 mln a circa 281.475 Miliardi. Un riutilizzo dell'IV può avvenire, in condizioni di traffico elevato, dopo circa 100 anni.
  - L'IV in WPA è usato come un contatore, chiamato TSC (TKIP Sequence Counter), previene la ripetizione del keystream; quest'ultima è un'importante debolezza del WEP.
  - La chiave viene calcolata ad ogni pacchetto (per packet) usando il vettore IV.
  - La chiave "Master" PMK (Pairwise Master Key) non viene MAI usata direttamente. Viene ricavata sempre una nuova chiave PTK (Pairwise Transient Key) usando la PMK.
  - Il problema del CRC, è stato risolto con un algoritmo apposito chiamato "Michael" che funge da MIC (Message Integrity Check) garantendo l'integrità del messaggio.

4.2. Funzionalità di WPA2

Realizzato nel Settembre del 2004, WPA2 (a differenza di WPA) implementa tutte le funzionalità definite dallo standard IEEE 802.11i.

Come il WPA, anche WPA2 assicura un alto livello di protezione dei dati ed un accesso alla rete ristretto agli utenti autorizzati. Così come il suo predecessore, WPA2 utilizza 802.1x ed EAP per l'autenticazione (oltre all'alternativa PSK). La differenza sostanziale con WPA è che WPA2 fornisce un più forte meccanismo di cifratura attraverso l'AES (Advanced Encryption Standard) piuttosto che il TKIP. AES è un block cipher, nel senso che la cifratura viene fatta su blocchi di dati invece che bit a bit (come in RC4). Questo richiede capacità computazionali più elevate da parte dell'hardware, per cui non tutti i dispositivi che supportano WPA possono essere aggiornati via software per essere compatibili con WPA2, mentre invece è garantita l'interoperabilità di WPA2 con WPA. WPA2 crea delle nuove chiavi ad ogni associazione proprio come WPA. I vantaggi sono che le chiavi di cifratura usate per ogni utente sulla rete sono uniche e specifiche dell'utente stesso. Ogni pacchetto che viaggia in aria è cifrato con un'unica chiave. L'abilità di evitare il riuso della chiave e fornire delle chiavi di cifratura uniche e nuove è il principio base di una buona pratica di sicurezza ed è il motivo per cui WPA e WPA2 offrono un buon livello di sicurezza.

4.3. Modalità operative di WPA / WPA2

Entrambi WPA e WPA2 hanno due modalità operative: Personal ed Enterprise.

La modalità Personal implica l'utilizzo di una chiave pre-condivisa per l'autenticazione, mentre la modalità Enterprise utilizza lo standard IEEE 802.1X ed EAP.

I prodotti possono essere certificati per entrambe le modalità, o soltanto per la modalità Personal. Pertanto, le organizzazioni che intendono utilizzare un server di autenticazione, piuttosto che chiavi pre-condivise dovrebbero cercare esclusivamente prodotti con certificazione Enterprise. L'uso di un server di autenticazione, piuttosto che di chiavi pre-condivise, è raccomandato per la maggior parte delle situazioni in cui è impraticabile la generazione, la distribuzione e la periodica sostituzione delle chiavi pre-condivise.

La mancanza di autenticazione del singolo utente, nella maggior parte dei punti di accesso che utilizzano PSK è un altro motivo per evitare l'uso di chiavi pre-condivise.

4.4. Attacchi a WPA / WPA2

Attaccare una rete WPA e navigare sfruttando reti wireless altrui non è legale. In ogni caso studiare le modalità con cui è possibile attaccare una rete WPA ci consente di studiare eventuali falle nella protezione della rete stessa, con l'obiettivo di correggere questi bug.

Anche se sono stati scoperti un numero di limiti minori in WPA/WPA2, nessuna di queste debolezze è considerata troppo pericolosa a condizione che si rispettino delle raccomandazioni di sicurezza.

La vulnerabilità più pratica è l'attacco contro la chiave PSK di WPA/WPA2. Come abbiamo già detto, la PSK fornisce un alternativa alla generazione PMK di 802.1X attraverso un server di autenticazione. Si tratta di una stringa di 256 bit o passphrase da 8 a 63 caratteri usata per generare tale stringa con un algoritmo noto: PSK = PMK = PBKDF2 (password, SSID, lunghezza SSID, 4096, 256), dove PBKDF2 è un metodo definito in PKCS#5[9], 4096 è il numero delle hash da calcolare (# d'iterazioni) e 256 è la lunghezza dell'output. La PTK è derivata dalla PMK usando l'handshake a 4 vie e tutte le informazioni usate per calcolare il suo valore sono trasmesse in testo in chiaro.

La forza di PTK quindi risiede solo nel valore PMK che per la PSK significa la passphrase. Il secondo messaggio dell'handshake a 4 vie potrebbe essere soggetto sia ad attacchi a dizionario, sia ad attacchi a forza bruta offline. Il cracking tool Cowpatty[16] fu creato per sfruttare questo difetto, ed il suo codice sorgente era stato usato e migliorato da Christophe Devine[14] in Aircrack per consentire gli attacchi a dizionario e di forza bruta sulla PSK di WPA. La struttura del protocollo (4096 hash da calcolare per ogni tentativo di password) implica un'eccessiva lentezza in un attacco a forza bruta (solo alcune centinaia di password per secondo possono essere calcolate con i più recenti processori dual-core). La PMK non può essere precalcolata dal momento che la passphrase viene mischiata ulteriormente in base al SSID. Per proteggersi efficacemente da questo difetto è bene scegliere una buona passphrase con parole inesistenti (con almeno 20 caratteri). Per eseguire questo attacco, l'aggressore dove catturare i messaggi dell'handshake a 4 vie monitorando passivamente la rete wireless o usando l'attacco di deautenticazione per velocizzare il processo.

Infatti, i primi due messaggi sono necessari per iniziare la previsione dei valori PSK. Ricordate che PTK = PRF-X (PMK, Pairwise key expansion, Min(AP_Mac, STA_Mac) || Max(AP_Mac, STA_Mac) || Min(ANonce, SNonce) || Max(ANonce, Snonce)), dove la PMK è uguale alla PSK nel nostro caso. Dopo il secondo messaggio, l'aggressore conosce ANonce (dal primo messaggio) e SNonce (dal secondo messaggio) e può iniziare a indovinare il valore PSK per calcolare la PTK e le chiavi temporanee derivate. Se la PSK calcolata è corretta, il MIC del secondo messaggio può essere ottenuto con la KCK corrispondente – altrimenti una nuova previsione deve essere fatta.

4.5. Esempio pratico di un attacco a WPA / WPA2

Prima di descrivere un esempio pratico di attacco, è importante ricordare che come disposto dell'art. 615-ter c.p. è reato l'accesso abusivo in un sistema informatico o telematico protetto da misure di sicurezza.

Detto ciò mostreremo per puri scopi educativi uno scenario di attacco ad una rete WPA creata appositamente per questo esempio.

4.5.1. Ricerca dell'AP "bersaglio"

La prima operazione da eseguire è quella di localizzare la rete WPA / WPA2 (in modalità PSK) da attaccare.

Per far ciò utilizziamo un'applicazione chiamata Kismet[15] che è un wireless network detector (rilevatore di reti wireless) con funzioni di "packet sniffer". Questo significa che oltre ad essere in grado di rilevare la presenza di reti Wi-Fi 802.11 è anche in grado di registrare il traffico che intercetta da reti 802.11a, 802.11b e 802.11g, i tre maggiori standard attualmente utilizzati per la realizzazione di reti senza fili. Per raccogliere i dati, Kismet modifica le impostazioni della scheda di rete in modo da utilizzare la cosiddetta "monitor mode" o anche "rfmon" (acronimo che sta per Radio Frequency Monitoring). A differenza della modalità promiscua che consente l'intercettazione dei dati solo dopo aver associato la scheda ad una qualche rete (quindi circoscrivendo i pacchetti raccolti a quelli della rete stessa) la monitor mode consente di intercettare tutti i pacchetti wireless in viaggio su un particolare canale, completi di header 802.11 e compresi i pacchetti di gestione della rete. Tutta quest'attività viene svolta in modo completamente passivo ovvero senza inviare

alcun pacchetto e quindi senza produrre alcun tipo di rumore nell'ambiente che stiamo ispezionando.

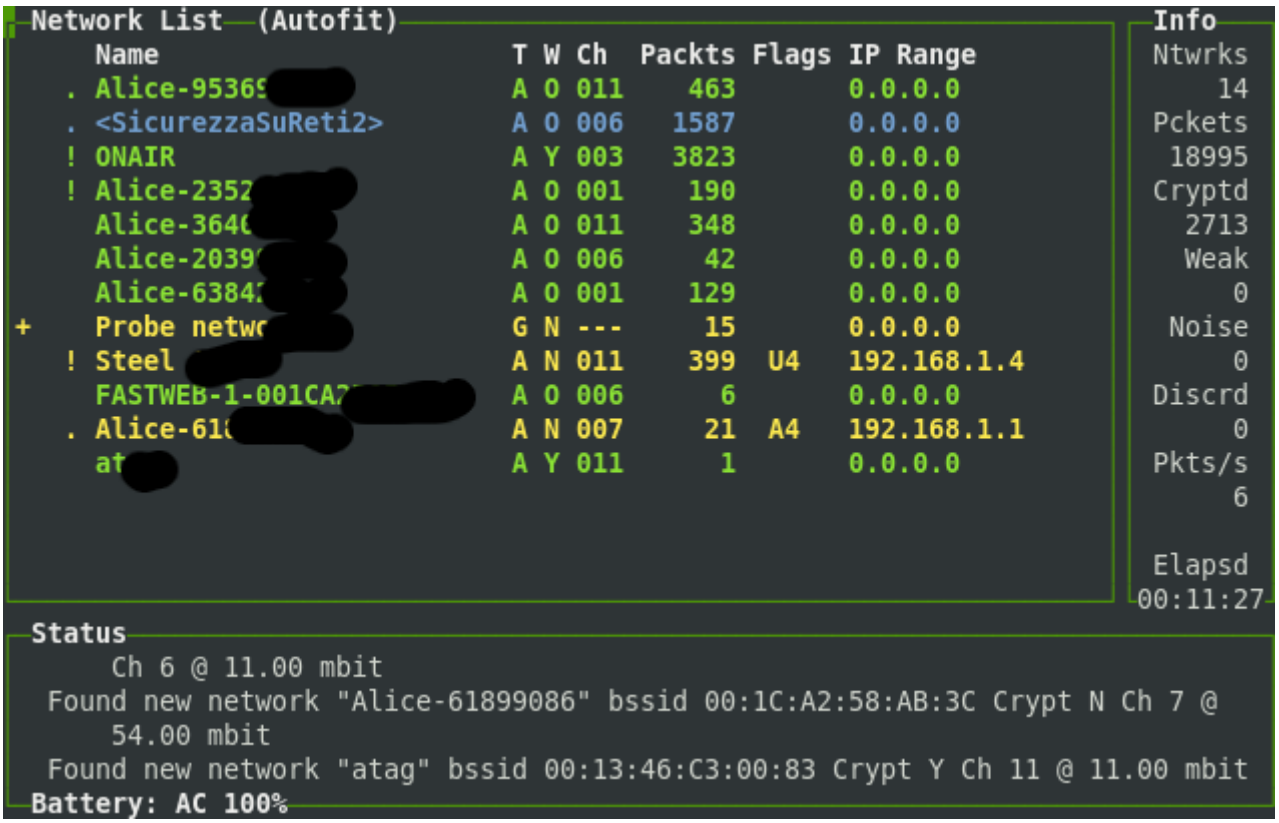


Figura 16: Kismet permette di rilevare i SSID di reti “nascoste”

Analizzando il traffico dati, Kismet è in grado di scovare reti nascoste che non producono i cosiddetti pacchetti "beacon" che altro non fanno che segnalare la presenza della rete ai possibili client in ascolto. In particolare per conoscere il SSID di una rete nascosta è possibile forzare la disassociazione di almeno un client legittimo di questa rete in modo da permettere a Kismet di scoprire il SSID della rete dalla richiesta di riassociazione del client quando tenta di riconnettersi alla rete.

Come abbiamo detto prima però la modalità rfmon funziona su di un solo canale alla volta; per questo Kismet implementa una tecnica denominata "channel hopping" (letteralmente salto di canale) attraverso la quale il programma modifica ad intervalli regolari il canale utilizzato dalla scheda wireless in modo non sequenziale. Affinché sia possibile catturare gli handshake è necessario che la nostra scheda wireless comunichi alla stessa velocità e nella stessa modalità dell’AP. Quindi per esempio se la nostra scheda è in “B” mode e l’AP è in “G” mode e non utilizzano la stessa velocità (rate) non sarà possibile catturare gli handshake. Per scoprire quale siano la modalità e la velocità corrette si può provare a cambiarle finché gli handshake non vengono

catturarti oppure utilizzare Kismet che, per ogni rete rilevata, fornisce alcune informazioni tra cui anche la modalità e la velocità con cui l'AP comunica.

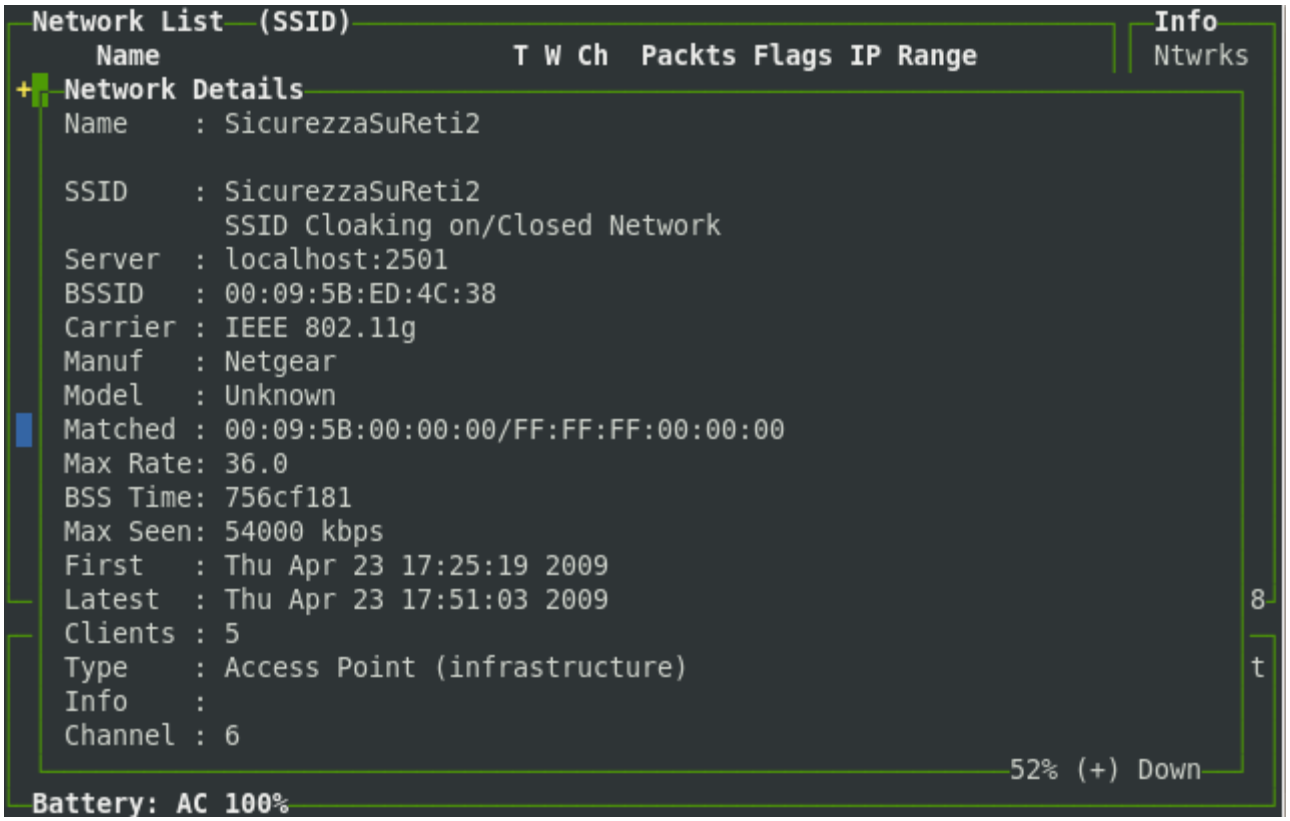


Figura 17: Kismet fornisce i dettagli sulle reti 802.11 raggiungibili

Per cambiare il rate della nostra scheda di rete useremo il seguente comando:

iwconfig wlan0 rate [auto,11,54 etc]

Per cambiare la modalità di trasmissione eseguiremo il comando:

iwpriv wlan0 mode 2

Dove il numero indica uno fra le seguenti modalità: Mode 0 Automatic (a/b/g), Mode 1 solo 802.11a, Mode 2 solo 802.11b e Mode 3 solo 802.11g.

Se nonostante il rate di trasmissione della nostra scheda di rete sia uguale a quello dell'AP non riceviamo i pacchetti dell'handshake, allora bisogna riprovare impostando il rate ad 1 M. In molti casi il rate ad 1 M risolve ogni problema.

4.5.2. Sniffing dei pacchetti dell'handshake a 4 vie

In questo scenario supponiamo di essere interessati ad attaccare l'AP scoperto nella fase precedente che aveva SSID "SicurezzaSuReti2" e BSSID "00:09:5B:ED:4C:38". Grazie all'utilizzo di Kismet sappiamo che l'AP in questione utilizza come cifratura WPA sul canale 6 in modalità "g" a 54Mbps. Ora per poterci ricavare la PSK non ci resta che catturare i pacchetti scambiati durante l'handshake a 4 vie tra l'AP ed un client legittimo della rete. Per evitare l'attesa che un client si connetta o riconnetta alla rete, è possibile forzare la disassociazione di un client legittimo (che ha già eseguito l'handshake a 4 vie) attraverso l'applicazione Aireplay (questa operazione veniva fatta anche quando si voleva conoscere il SSID di una rete nascosta). Anche se Aireplay consente di inviare pacchetti di disassociazione broadcast per far dissociare tutti i clients legittimi di una rete questo risulta meno efficace che creare un pacchetto di disassociazione per un client specifico. Per far ciò utilizziamo Kismet per conoscere l'indirizzo MAC di un qualsiasi client da disassociare, ciò è mostrato in figura 18.

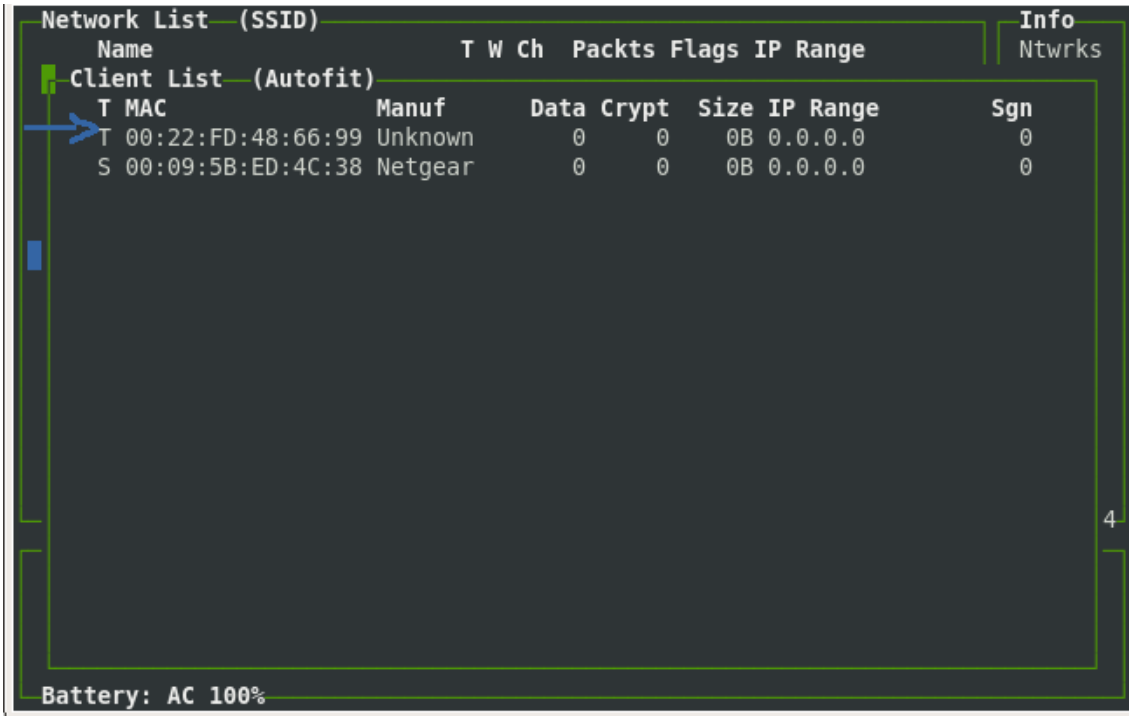


Figura 18: Kismet ci permette di conoscere i clients connessi ad una rete

In questo scenario il nostro client da dissociare ha indirizzo MAC “00:22:FD:48:66:99”. A questo punto usiamo Aireplay per disassociare il client selezionato inviando una richiesta di disassociazione fasulla utilizzando il BSSID dell’AP:

 # aireplay-ng -0 10 -a <BSSID> -c <client_MAC> wlan0

```
root@linux86-laptop:~# aireplay-ng -0 10 -a 00:09:5B:ED:4C:38 -c 00:22:FD:48:66:99 wlan0
19:10:22  Waiting for beacon frame (BSSID: 00:09:5B:ED:4C:38) on channel 6
19:10:22  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 0| 0 ACKs]
19:10:23  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 0| 0 ACKs]
19:10:24  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 0| 0 ACKs]
19:10:24  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 0| 0 ACKs]
19:10:25  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 0| 0 ACKs]
19:10:26  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 1| 4 ACKs]
19:10:27  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 1| 8 ACKs]
19:10:27  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 0| 1 ACKs]
19:10:28  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 0| 0 ACKs]
19:10:28  Sending 64 directed DeAuth. STMAC: [00:22:FD:48:66:99] [ 0| 0 ACKs]
```

Figura 19: Aireplay ci permette di far dissociare un client dalla rete

Il client legittimo dovrebbe quindi essere disassociato, obbligandolo ad iniziare una nuova associazione e permettendoci di catturare i messaggi dell’handshake a 4 vie attraverso l'applicazione Airodump:

airodump-ng -c 6 --bssid 00:09:5B:ED:4C:38 -w catturaHandshake wlan0

Dove:

-c 6 è il canale su cui l’AP comunica

-bssid 00:14:6C:7E:40:80 è l'indirizzo MAC dell’AP

-w catturaHandshake è il nome del file in cui verranno salvati i pacchetti scambiati durante l’handshake

```
root@linux86-laptop:~# sudo airodump-ng -c 6 --bssid 00:09:5B:ED:4C:38 -w catturaHandshake wlan0
 CH  6 ][ Elapsed: 48 s ][ 2009-04-23 20:43 ][ WPA handshake: 00:09:5B:ED:4C:38

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

 00:09:5B:ED:4C:38  230   2      471       55    0   6  54. WPA  TKIP   PSK  SicurezzaSuReti2

 BSSID              STATION            PWR   Rate  Lost  Packets  Probes

 00:09:5B:ED:4C:38  00:22:FD:48:66:99  228  54- 2     0       77
```

Figura 20: Airodump ci permette di catturare i pacchetti dell'handshake a 4 vie.

4.5.3. Attacco a dizionario usando Aircrack

Adesso che abbiamo catturato i pacchetti dell'handshake a 4 vie possiamo provare a ricavarci la PSK attraverso un attacco a dizionario (un attacco a forza bruta come vedremo tra un pò è improponibile!).

Per effettuare questo passo è necessario avere un file dizionario di password che contenga il più grosso numero possibili di password.

Figura 21: Parte del file dizionario che è stato usato per l'attacco nel nostro scenario

Una volta selezionato il file dizionario avviamo la ricerca della chiave PSK attraverso il seguente comando:

aircrack-ng -w password.lst -b 00:09:5B:ED:4C:38 catturaHandshake*.cap

Dove:

-w password.lst è il nome del file dizionario

*.cap è l'elenco dei file di capture che abbiamo collezzionato

```
root@linux86-laptop:~# sudo aircrack-ng -w password.lst -b 00:09:5B:ED:4C:38 catturaHandshake*.cap

Opening catturaHandshake-01.cap
Opening catturaHandshake-02.cap
Opening catturaHandshake-03.cap
Opening catturaHandshake-04.cap
Opening catturaHandshake-05.cap
Opening catturaHandshake-06.cap
Reading packets, please wait...

                           Aircrack-ng 1.0 rc1


              [00:00:00] 74 keys tested (355.37 k/s)


                     KEY FOUND! [ Frase Segreta ]


  Master Key     : 5E 57 73 85 1A 31 A3 A7 10 48 53 E3 82 8D 3E 9B
                   03 D2 8D DC D5 57 FA 59 B7 1F 93 60 13 9D FA D1

  Transcient Key : 8E 42 E5 B5 F0 AF E9 93 24 BE AD DC 2F E0 57 73
                   DB 9A EA 3B 1E 36 3D 79 55 56 20 85 17 91 02 F6
                   0A 39 A3 B1 C1 21 35 C6 90 36 C1 42 A6 3F F9 31
                   B7 30 9C E6 BF 63 88 5D 50 B8 E1 55 77 3F 3F 72

  EAPOL HMAC     : 9A D4 33 74 55 13 09 87 09 AE 4D FF 60 D3 60 10
```

Figura 22: Aircrack ha trovato la PSK poiché questa era presente nel file dizionario password.lst

Come si può notare in figura 22, nel nostro scenario la passphrase utilizzata nella rete WPA "bersaglio" è "Frase Segreta" ed è stata scoperta poiché questa era presente nel nostro file dizionario.

Come già abbiamo anticipato, un attacco a forza bruta anche solo per scoprire una passphrase da 8 caratteri (8 è la lunghezza minima mentre 63 caratteri è quella massima) è improponibile. Infatti se considerassimo soltanto le possibili password alfanumeriche di 8 caratteri, allora si avrebbero 62 possibili scelte per ogni carattere: [A-Z][a-z][0-9].

Utilizzando una potente GPU come quella della GeForce 280GTX che prova circa 11000 chiavi al secondo (una cpu dual-core come l'Intel Core Duo T9400 prova circa 400 chiavi al secondo) ci vorrebbero circa 630 anni per calcolare tutte le possibili passphrase alfanumeriche di 8 caratteri:

62^8 = 218 340 105 584 896 possibili chiavi

218340105584896/11000k/s = 19 849 100 508 sec

19849100508 sec = 5 513 639 ore

5513639 ore = 229 735 giorni

229735 giorni = 630 anni

Dato che in realtà si possono utilizzare tutti i 95 caratteri stampabili della tabella ASCII le possibili chiavi per una passphrase da 8 caratteri sono 95^8 che sono molte di più delle 62^8 chiavi già resistenti ad un attacco a forza bruta.

Per questo motivo si può ottenere un ottimo livello di sicurezza scegliendo una passphrase con le seguenti caratteristiche:

- con almeno 20 caratteri;
- con caratteri speciali (come “$”,”@”,”_”, ecc.);
- con sequenze casuali di caratteri (non di senso compiuto per evitare attacchi a dizionario).

4.6. Altre vulnerabilità di WPA/WPA2

L'altra grande debolezza di WPA è la possibilità di un Denial of Service (DoS) durante l'handshake a 4 vie. Changhua He e John C. Mitchell[7] hanno notato che il primo messaggio della handshake a 4 vie non è autenticato ed ogni client deve memorizzare ogni primo messaggio fino a quando non riceve un terzo messaggio valido (firmato), lasciando il client vulnerabile all'esaurimento della memoria. Falsando il primo messaggio inviato dall'AP, un aggressore può eseguire un attacco DoS sul client. Il Michael Message Integrity Code è noto anche a causa della sua debolezza dovuta alla sua struttura semplice (forzata dal task group di 802.11i). La sicurezza di Michael si basa su una comunicazione cifrata. Anche se le MIC crittografiche sono di solito pianificate per resistere ad attacchi di testo in chiaro noti (dove l'aggressore ha un messaggio in chiaro ed il proprio MIC), Micheal è vulnerabile a tali attacchi perché è invertibile. Dato un unico messaggio noto ed il suo valore MIC, è possibile scoprire la chiave segreta MIC, quindi mantenere il valore MIC segreto è cruciale. L'ultima debolezza nota è un attacco teoretico contro la Temporal Key Hash di WPA, che comprende una complessità ridotta dell'attacco (da $\partial 128$ a $\partial 105$) in alcune circostanze (conoscenza di diverse chiavi RC4).

WPA e WPA2 sono anche soggetti a vulnerabilità che colpiscono altri meccanismi 802.11i come gli attacchi con lo spoofing dei messaggi 802.1X (EAPoL Logoff, EAPoL Start, EAP Failure ecc.), descritti per la prima volta da William A. Arbaugh e Arunesh Mishra[17] e dovuti alla mancanza di autenticazione.

Infine, è importante notare che usare il protocollo WPA/WPA2 non fornisce nessuna protezione contro le tecnologie sottostanti, come la radio frequency jamming, DoS attraverso violazioni 802.11, deautenticazione e disassociazione.

4.7. Controlli sulla sicurezza

Se disponete di una rete senza fili, procedete come segue per salvaguardare le risorse condivise:

1. Cambiare i SSID di default

Il Service Set IDentifier (SSID) identifica univocamente ogni punto di accesso all'interno della rete. Tramite una configurazione opportuna, soltanto i dispositivi che utilizzano il corretto SSID possono comunicare con i punti di accesso. Molti dei dispositivi hanno già preconfigurato un SSID di default: un intruso può usare questi nomi per cercare di accedere ad AP che hanno ancora la configurazione di fabbrica.

2. Utilizzare SSID non descrittivi

Usare SSID descrittivi facilita il compito di un eventuale intruso nell'individuare luoghi o aziende e nel ricavare maggiori informazioni su come entrare, ragion per cui è consigliabile utilizzare nomi anonimi o altamente scoraggianti.

3. Disabilitare il Broadcast SSID

Gli AP mandano ad intervalli regolari Beacon Frames per la sincronizzazione con i client, i quali contengono il SSID. Questi frames servono ai client per configurarsi automaticamente la rete di accesso, ma servono anche a potenziali aggressori durante la ricerca delle reti wireless. È auspicabile disabilitare il Broadcast SSID qualora l'AP supporti questa opzione. Il client dovrà essere configurato manualmente con il SSID corretto per poter accedere alla rete.

4. Cambiare le password

Come per i SSID, è importante cambiare le password di default degli AP. È buona norma che la password sia lunga almeno otto caratteri e che includa caratteri speciali e numeri.

5. Aggiornare il firmware

Nella scelta di un AP, è preferibile orientarsi verso un apparato che abbia la possibilità di aggiornare il suo firmware. È bene pertanto assicurarsi che l'AP abbia l'ultimo firmware consigliato dal produttore.

6. Chiavi WEP

Anche se è stato dimostrato che il WEP non è adeguato a proteggere una rete wireless, rappresenta comunque un deterrente per gli intrusi occasionali. Serve catturare dai 100 Mb a 1 Gb di traffico per provare a ricavare la chiave WEP, pertanto l'aggressore deve essere ben motivato per tentare l'intrusione. Cambiare spesso le chiavi WEP di crittografia sugli AP fa in modo che una rete compromessa non lo sia a tempo indeterminato: un intruso, infatti, dovrebbe provare nuovamente a ricavare la chiave WEP, e questo dovrebbe farlo desistere da un secondo tentativo. Cambiare le chiavi WEP è abbastanza oneroso: alcuni AP supportano la dynamic WEP-key exchange per cambiare la chiave WEP per ogni adattatore. È consigliato controllare dal produttore degli AP la disponibilità di questa feature. Alcuni AP, ad esempio, non dispongono di questa feature, ma è possibile specificare fino a quattro differenti chiavi per facilitare il cambio periodico della chiave.

7. Chiave WPA/WPA2 PSK

Se si utilizza la codifica WPA / WPA2 in modalità Personal (PSK) è importante scegliere una passphrase che rispetti i criteri discussi nel paragrafo 3 del capitolo corrente.

8. Autenticazione 802.1X e WPA2

Se possibile utilizzare WPA / WPA2 in modalità Enterprise (con server di autenticazione RADIUS). Inoltre, quando possibile, è preferibile utilizzare WPA2 a WPA poiché offre un miglior algoritmo di cifratura rispetto a WPA.

9. Abilitare il MAC filtering

Molti produttori includono nei loro AP la possibilità di abilitare soltanto alcune schede di rete, usando come metodo discriminatorio il loro indirizzo MAC. Alcuni AP permettono di fornire l'elenco degli indirizzi MAC abilitati attraverso una GUI, linea di comando o RADIUS. Si suggerisce di usare la GUI o la linea di comando nel caso di implementazione con pochi AP, RADIUS in un contesto più ampio. È necessario però comprendere che l’indirizzo MAC di una scheda può essere facilmente cambiato, pertanto il MAC filtering non può essere usato come solo metodo di protezione.

10. Spegnere l’AP quando non serve

Gli intrusi agiscono solitamente durante la notte e il fine settimana, ovvero quando la rete ed i sistemi non sono controllati. È consigliato, quando possibile, collegare gli AP ad un timer, in modo da spegnerli quando non vengono utilizzati.

11. Minimizzare l'intensità del segnale

Gli intrusi sfruttano il fatto che le onde radio non si possono limitare a dei luoghi ben definiti, esempio l'ufficio vendite, ma riescono ad espandersi fuori dalle mura perimetrali dall'ufficio. Da qui la definizione del nome “parking lot attack”, o più semplicemente attacchi provenienti dal parcheggio. È pertanto importante scegliere un'adeguata collocazione dell’AP all'interno dell'edificio, in modo che il segnale sia sufficiente a garantire il collegamento solo ed esclusivamente alla zona interessata. Attraverso appositi strumenti radio, è possibile verificare che il segnale non sia visibile all'esterno del palazzo o della zona identificata. Per minimizzare l'intensità del segnale, è sufficiente non posizionare l’AP vicino alle finestre e usare antenne direzionali con basso guadagno in decibel. Alcuni AP inoltre hanno la possibilità di definire l'intensità del segnale via software.

12. Cambiare le community di default di SNMP

Su molti AP risulta installato un agente SNMP (Simple Network Management Protocol). Se la community password non risulta correttamente configurata, un aggressore può leggere e scrivere dati di configurazione sull’AP, in maniera analoga ad altri sistemi che supportano SNMP.

13. Limitare il traffico di broadcast

Alcuni protocolli, in particolare il NetBIOS su TCP/IP usato da Windows, usano assiduamente i messaggi di broadcast. Questi messaggi di broadcast minimizzano per un intruso i tempi di raccolta dei dati per ricavare la chiave WEP. È consigliabile limitare il traffico di broadcast quando possibile, ad esempio disattivando il protocollo NetBIOS su TCP/IP dal binding con la scheda di rete Wireless.

14. Protezione dei client

Alcuni attacchi sono mirati ai client wireless in quanto vengono usati come ponte per entrare nella rete interna e per ricavare preziose informazioni. Ad esempio, alcuni client wireless scrivono in chiaro, nel registro di Windows o in un file di testo, le chiavi WEP di crittografia. È preferibile usare un personal firewall sui client in modo da ridurre i rischi di attacchi.

15. Non utilizzare il DHCP

È consigliabile non utilizzare il DHCP per l'assegnazione dinamica degli indirizzi, ma considerare l'utilizzo di IP statici. Anche se è un ulteriore impegno per l'amministratore, è assai utile per evitare che la rete wireless attribuisca indirizzi IP validi a chiunque voglia associarsi con l'AP. Anche se un attaccante, utilizzando uno sniffer wireless, può facilmente ricavare gli IP, il fatto di non distribuirli via DHCP rappresenta un'ulteriore barriera. Inoltre, è consigliabile evitare di usare indirizzamenti di default facilmente intuibili come 192.168.1.0 o 192.168.0.0.

16. Uso di una VLAN separata

È consigliabile utilizzare una Virtual Lan separata per il traffico wireless, separandola dalla rete intranet. Esistono varie metodologie, per unire in maniera sicura le due LAN, tra le più semplici ricordiamo l'uso di un router/switch con capacità di filtro IP o un proxy. In alcune piccole aziende e in ambienti SOHO (Small Office, Home Office) dove la protezione della rete non rappresenta un problema, queste semplici regole sono sufficienti a proteggere l'accesso wireless. In ambienti più critici, dove è necessario mantenere la confidenzialità dei dati, è necessario applicare delle regole più rigorose.

17. Disabilitare amministrazione remota dell'AP

Considerate di disabilitare l’amministrazione remota del punto di accesso. Se dovete modificare queste impostazioni, potete farlo direttamente, utilizzando la connessione ethernet o il cavo fornito in dotazione.

18. Verificare la sicurezza della rete

Attraverso gli strumenti più utilizzati dagli hacker, sottoporre a scansione la rete senza fili per determinare se la rete è vulnerabile a possibili attacchi.

5. Uno scenario reale: Convergenze s.p.a.

5.1. Introduzione

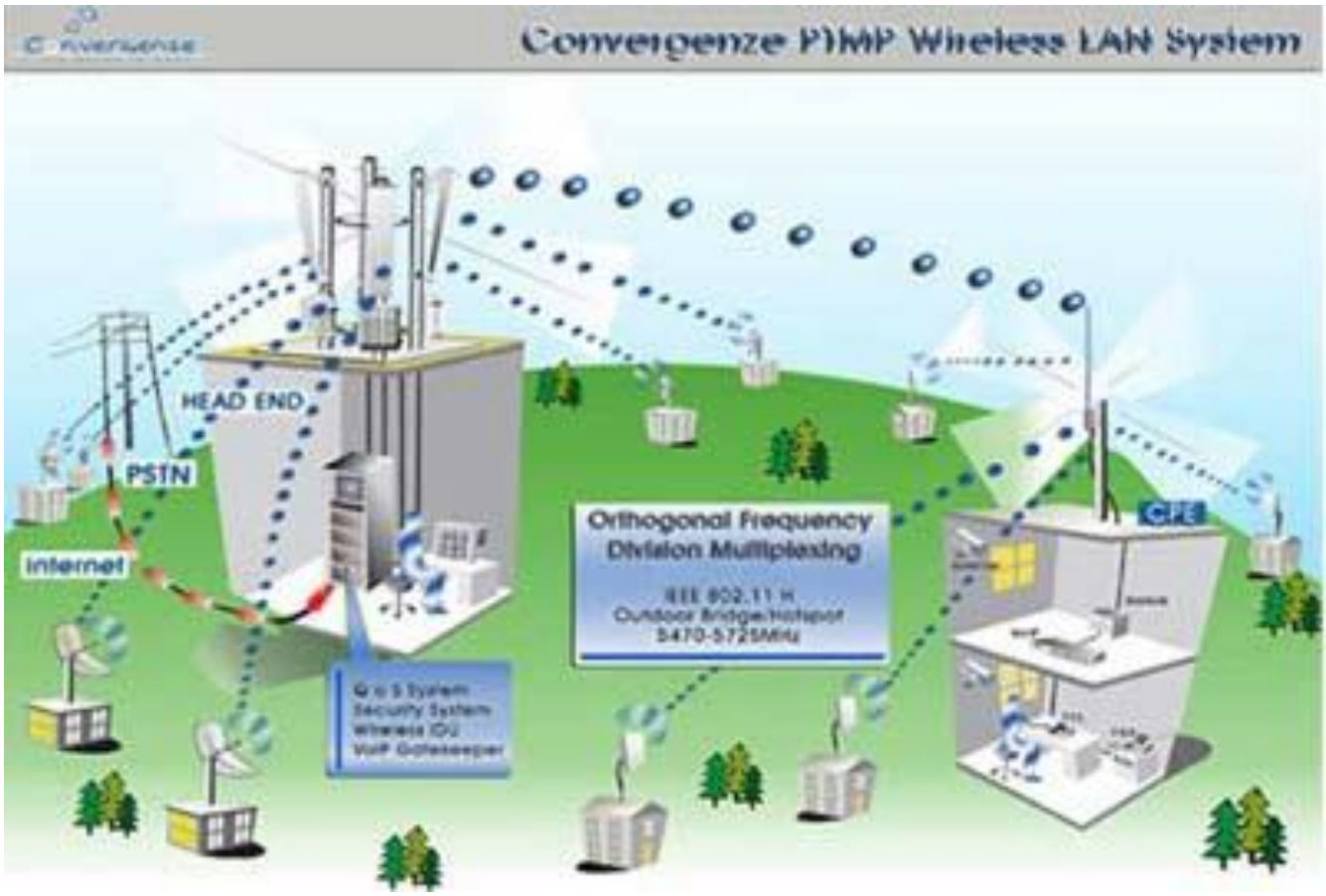
In questo capitolo descriveremo lo scenario di utilizzo del servizio Wi-Fi fornito dall'azienda Convergenze s.p.a., analizzando quelli che sono i protocolli di protezione utilizzati per rendere la rete sicura ed affidabile. Lo standard internazionale adottato per le reti wireless "Convergenze" è noto tecnicamente come *IEEE 802.11h* o *Hiperlan/2* con frequenze nel range tra 5.4-5.7 Ghz e velocità di trasmissione dati che può arrivare sino a 54 Mbps. La disponibilità dell'accesso a banda larga ai servizi Internet in Italia è stata per lungo tempo legata allo sviluppo della rete ADSL terrestre. I primi a poter beneficiare di questa nuova possibilità di accesso al servizio di rete sono stati gli abitanti delle città maggiori. In tempi relativamente rapidi sono stati creati dei collegamenti tra queste metropoli (le dorsali) e pian piano il servizio ADSL è stato reso disponibile anche ai centri minori. Questo processo si è molto rallentato, se non interrotto del tutto, al momento di collegare alla rete gli agglomerati urbani più piccoli o più difficilmente raggiungibili e le abitazioni più isolate (si pensi ai piccoli centri di montagna, alle isole minori, ai comuni più distanti dal capoluogo, ecc.). Il motivo di ciò è, sostanzialmente, l'elevato costo dell'infrastruttura (scavi, posa dei cavi, ecc.) a fronte dei possibili guadagni da parte degli operatori. Questa situazione di stallo ha preso il nome di "*digital divide*", intendendo con questo il fenomeno proprio la mancanza di servizio di accedere alla rete e ai servizi che sempre più si vanno trasferendo su Internet ai cittadini. La soluzione a questo problema è stata individuata nell'utilizzo di diverse tecnologie tra cui:

- Hiperlan
- WiMax
- *WLL (Wireless Local Loop)*

Il principio di funzionamento dell'Hiperlan è simile a quello delle comunicazioni cellulari: viene costruita una dorsale di stazioni che si trasmettono i segnali radio l'una con l'altra fino a raggiungere un sito dove è facile interconnettersi alla rete fissa. A partire dalla dorsale, una serie di

stazioni trasmettono il segnale radio fino a raggiungere l'utente, dove è installata un'antenna diretta verso la stazione più vicina.

La figura sottostante mostra lo scenario di utilizzo di una rete Convergenze



Infatti come si può vedere dalla figura soprastante il servizio fornito all'utente finale è del tutto analogo a quello di un comune collegamento Adsl, con l'unica differenza che l'accesso al servizio wireless avviene grazie ad un apposito router di piccole dimensioni che si collega alla Rete Internet tramite una antenna outdoor, che viene solitamente posizionata sul tetto dell'abitazione o dell'azienda. Tale antenna è di dimensioni piuttosto ridotte, ed è alimentata dalla normale rete elettrica dell'edificio, senza necessità di ulteriori dispositivi. L'antenna del cliente e' in collegamento permanente con il punto di accesso Wireless più vicino, a sua volta connesso alla rete internet attraverso collegamenti wireless.

5.2. Hiperlan

Hiperlan (**HI**gh **PE**rformance **R**adio **LAN**) è il nome di uno standard WLAN (standard ETS 300 652 ed ETS 300 893) che identifica l'alternativa europea agli standard IEEE 802.11. Gli apparati compatibili con questo standard hanno emissioni elettromagnetiche limitate, a norma di legge, a 1 watt e quindi inferiori a quelle di un'antenna per cellulari. Lo standard può assicurare un throughput di 24 Mb/s su frequenze dei 2,4 gigahertz. L'evoluzione di questo standard, implementabile anche nei vecchi apparati con protocollo Hiperlan/1, è l'Hiperlan/2 che raggiunge una velocità di 54 Mb/s su frequenze in Banda ISM dei 5 Ghz, con un raggio di copertura del segnale che può arrivare fino a 30–40 km. L'ufficio Europeo della Radiocomunicazione (ERO) che emana le decisioni della CEPT (Conferenza Europea delle Poste e Telecomunicazioni) in materia di telecomunicazioni ha definito lo standard Hiperlan in una direttiva del 29 novembre 1999 riguardante l'armonizzazione della banda di frequenze da designare all'uso delle Hiperlan ERC/DEC(99)23 e una integrazione del 12 novembre 2004 ECC/DEC(04)08. Nell'integrazione non sono state apportate modifiche di rilievo, eccetto alcune precisazioni sulla densità spettrale di potenza del segnale emesso: in particolare i trasmettitori degli apparati Hiperlan outdoor (operanti nel range di frequenze 5,470 - 5,725 Ghz), il cui limite EIRP è 1 watt (pari a 30 dBm), devono trasmettere con una densità spettrale massima di 50 mW/MHz, il che significa che tipicamente dovranno avere canali larghi 20 MHz (50 mW/MHz × 20 MHz = 1 W). Altre ampiezze di canale sono ammesse, purché non vengano superati i limiti di densità imposti. Secondo la normativa standard Europea ETSI EN 301 893, la massima larghezza di canale ammessa con una densità di potenza massima è di 20 MHz. Larghezze inferiori sono ovviamente permesse. L'ERO ha poi emanato una decisione, operativa dal 12 novembre del 2004 che ha, di fatto, liberalizzato in tutta l'UE l'uso delle frequenze intorno ai 5 gigahertz, e la tecnologia

Hiperlan. Possibile soluzione al problema del digital divide, dopo una sperimentazione di due anni, con il decreto Stanca (8 giugno 2005) ne è liberalizzato l'uso in Italia. Vari provider hanno costruito reti Hiperlan per fornire connettività, con buoni successi. La limitazione principale alla copertura con questo tipo di tecnologia è il fatto che i collegamenti debbano essere a vista, ovvero le antenne delle due stazioni devono vedersi senza che vi siano ostacoli di mezzo.

5.2.1. Hiperlan/1

La sua architettura prevede la presenza di una o più stazioni forwarder (lo scopo è quello di inoltrare ai suoi vicini i frame con destinazioni diverse dal suo indirizzo), una o più stazioni non-forwarder (che si limitano a ricevere i messaggi) e stazioni di bridge (per connettere più reti Hiperlan/1).

Ogni stazione forwarder e non-forwarder deve aggiornare una serie di basi di dati per effettuare il routing. Lo standard Hiperlan tipo 1 ridefinisce lo strato fisico e parte dello strato datalink: specifica i livelli MAC, di accesso al canale (CAC) e fisico (PHY). Questa tecnologia implementa, inoltre, un sistema di QoS a livello MAC ed un sistema di priorità di accesso al canale a livello CAC. Il controllo di accesso al canale è regolato mediante il protocollo EY-NPMA (Elimination Yeld - Non-preemptive Priority Multiple Access), che permette vi sia un numero relativamente basso di collisioni. Questo protocollo è utilizzato per la gestione dell'accesso al canale dallo strato CAC (sotto strato del datalink). Il funzionamento di questo protocollo si snoda attraverso tre fasi fondamentali: prioritizzazione, contesa e trasmissione. Durante la prima fase, tutte le stazioni rimangono in ascolto per N-1 slot (dove N è la priorità di trasmissione di ogni nodo). Se durante questi slot la stazione ascolta una PA (*priority assertion*), rinuncia al canale ed aspetta il prossimo ciclo, altrimenti trasmette la sua PA.

Le stazioni sopravvissute alla prima fase si contendono l'accesso al canale. Durante questa fase avviene l'*eliminazione*, secondo la quale tutte le stazioni inviano raffiche (*burst*) di lunghezza casuale e, se dopo la raffica, per un tempo ESV (*elimination survival verification*) il canale risulta libero, si continua verso una ulteriore contesa, detta *yeld*. In questo tipo di contesa tutte le stazioni

rimaste attendono in ascolto per un periodo di tempo casuale e, se il canale risulta occupato durante l'ascolto, si ritirano. Nella terza fase il nodo superstite trasmette. Non è garantito che non vi siano collisioni, tuttavia la probabilità che queste accadano è molto bassa.

5.2.2. Hiperlan/2

Lo standard Hiperlan/2 è stato sviluppato dall'ETSI (European Telecommunications
Standards Institute) come estensione dello standard Hiperlan/1. Tale standard è quello utilizzato dall'azienda Convergenze ed è essenzialmente suddiviso in tre livelli:

- Physical layer (PHY)
- Data Link Control layer (DLC)
- Convergence layer (CL)

Il livello fisico si dintingue per l'utilizzo di una tecnica di modulazione per la trasmissione del segnale analogico detta OFDM (Orthogonal Frequency Digital Multiplexing), adottata anche dai cellulari di ultima generazione.

Il livello DLC comprende a sua volta altri sottolivelli tra cui il MAC, l'Error Control (EC) e il Radio Link Control (RLC). RLC include a sua volta altri moduli che si occupano della gestione delle associazioni da parte dei terminali mobili.

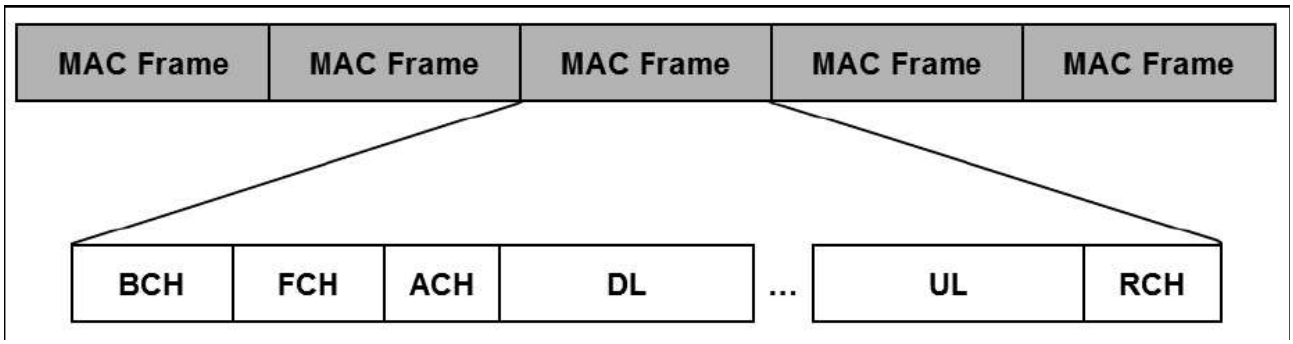
Il livello CL ha il compito di adattare le richieste provenienti dai livelli più alti in funzione dei servizi che il DLC può offrire. In aggiunta si occupa anche della frammentazione dei pacchetti secondo i limiti specificati dal DLC in modo da permetterne la trasmissione affidabile.

Il controllo del canale è di tipo centralizzato ed è affidato all'AP. Gli host che hanno necessità di trasmettere inviano una richiesta all'AP. Quest'ultimo, una volta collezionate tutte le richieste, provvederà in un secondo momento a fornire informazioni sulle risorse allocate a ciascun host. Ciò è possibile grazie ad una suddivisione logica del tempo sul canale in slot. Il termine slot indica un intervallo temporale la cui lunghezza viene stabilita dalle specifiche implementative del protocollo in questione. Il funzionamento dell'interfaccia wireless è basato sul TDMA (Time Division

Multiple Access), una tecnica di accesso al mezzo che risolve il problema della contesa del canale assegnando ad ogni host slot diversi.

Da notare che il TDMA richiede un ambiente altamente sincronizzato, difficile da mantenere in contesti prettamente ad hoc. Nel caso di Hiperlan/2 si può parlare di un'organizzazione dell'accesso al mezzo secondo una strutturazione ben definita che prende il nome di MAC frame. Questo tipo di struttura è ciclica nel tempo e si adatta dinamicamente alle dimensioni del traffico. In Hiperlan/2 un MAC frame ha la lunghezza di 2 ms ed è composto da diverse fasi dette transport channels.

Nella figura sottostante è illustrata la composizione di un MAC frame di Hiperlan/2.



Le fasi che compongono un MAC frame di Hiperlan/2 sono: broadcast(BCH), frame control (FCH), access feedback (ACH), down link (DL), uplink (UL) e random access (RCH).

La fase di broadcast è di tipo downlink ossia prevede un flusso di informazioni solo dall'AP verso gli host e non viceversa. Nel BCH vengono trasmessi parametri fondamentali

per la sincronizzazione dell'intero MAC frame come istante d'inizio e lunghezza dell'FCH e dell'RCH.

L'FCH, anch'esso di tipo downlink, contiene un'esatta descrizione dell'allocazione delle fasi UL e DL del MAC frame corrente. In questo modo ogni host viene a conoscenza delle presenza o meno di slot allocati per le proprie trasmissioni. Nella fase di access feedback l'AP informa gli host sull'esito degli accessi nel RCH immediatamente precedente. Nell'RCH l'accesso al mezzo avviene in maniera totalmente distribuita, senza un minimo di coordinazione,

quindi si possono verificare delle collisioni. In questo caso si dice che l'accesso è "in contesa". Se invece esiste un qualche meccanismo che prevede una regolamentazione degli accessi al mezzo si parla di accesso non in contesa.

Durante la fase RCH gli host inviano le proprie richieste di banda in funzione della quantità e della tipologia del traffico che hanno da trasmettere.

La suddivisione del canale in fasi logiche proposta da Hiperlan/2 fornisce uno strumento efficiente per la gestione del canale. Con questo sistema si riducono considerevolmente le collisioni in quanto l'accesso al canale è quasi totalmente organizzato, eccezion fatta per la fase RCH.

Inoltre con il meccanismo di allocazione delle risorse su richiesta, si ha la possibilità di attuare diverse politiche di scheduling, anche orientate al QoS. Le frequenze utilizzate dall'Hiperlan/2 sono le stesse usate dai radar, per questo motivo questo standard europeo implementa TPC (Transmit Power Control) e il DFS (dynamic frequency selection) che evitano interferenze possibilmente dannose con questi apparati.

Il TPC o Controllo della potenza di trasmissione identifica apparati che impiegano la sola potenza necessaria per il buon esito delle comunicazioni.

Questo garantisce:

- minore interferenza con altri sistemi radio
- minore inquinamento elettromagnetico
- minore consumo energetico

IL DFS o Selezione dinamica del canale identifica un meccanismo per l'allocazione delle comunicazioni all'interno dei canali disponibili.

Gli apparati effettuano il CONTROLLO DEL CANALE:

- per evitare trasmissioni cocanale
- per rilevare segnali da parte di altri sistemi (Radio Interference Detection)

In caso di rilevamento, il canale deve essere variato. Inoltre ogni canale può essere scelto in maniera equiprobabile; per questo motivo si parla di utilizzo uniforme della banda (Uniform Spreading).

5.3. I tre livelli di protezione

Il livello di sicurezza adottato dall'azienda si basa sostanzialmente sullo standard WPA-2, che abbiamo già descritto nei capitoli precedenti, sull'utilizzo del protocollo PPPoE, per quanto riguarda la fase di autenticazione del cliente e sul MAC dell'antenna che permette all'azienda di controllare gli accessi all'infrastruttura impedendo accessi non autorizzati (MAC di antenne non presenti nel Database o non associate a nessun cliente) .

La tabella sottostante ci mostra come tali livelli di protezione forniscano sicurezza ai due diversi attori dell'infrastruttura di rete: l'azienda e il cliente.

PROTOCOLLO	DESCRIZIONE
WPA-2	Il protocollo di sicurezza WPA-2 descritto nel capitolo precedente fornisce, sia per l'azienda che per l'utente, un livello di sicurezza elevato grazie alle politiche per l'autenticazione, la gestione delle chiavi e la segretezza ed integrità dei dati.
PPPoE	L'azienda tramite la coppia (*username*,*password*), comunicata dall'antenna al momento dell'autenticazione,controlla l'accesso alla rete. Tale accesso sarà consentito soltanto ai clienti la cui combinazione(*username*,*password*) è presente nel DB.
MAC	Non è possibile che antenne, il cui MAC non sia presente nel DB centrale dell'azienda, possano accedere alla rete. Inoltre eventuali antenne "aziendali" non attivate (non associate quindi a nessun cliente) non possono in ogni caso accedere alla rete.

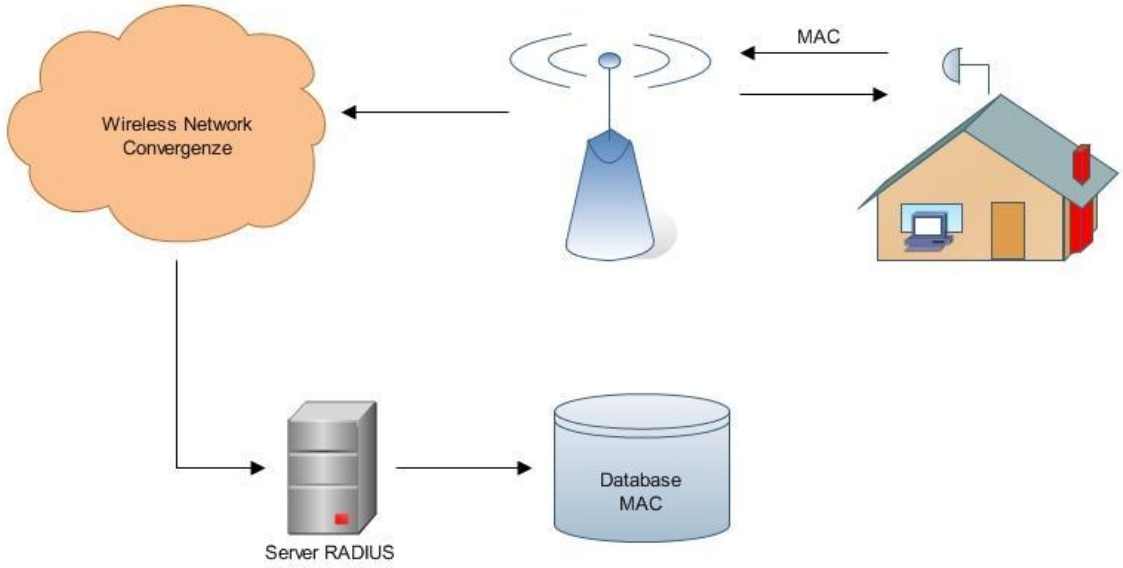
La tabella su descritta permette di capire come i diversi livelli di protezione adottati dall'azienda permettano di fornire un grado di sicurezza elevato.

Nei prossimi paragrafi andremo a descrivere in dettaglio l'importanza del protocollo PPPoE e del MAC dell'antenna e di come essi giocano un ruolo importante nella sicurezza della trasmissione Wi-Fi fornita da "Convergenze".

5.3.1. Il MAC dell'antenna

Come dicevamo in precedenza ogni antenna è associata ad un utente ed è collegata all'access point dell'azienda più vicino.

Lo scenario di autenticazione dell'antenna è descritta dalla seguente figura



L'antenna comunica il proprio MAC all'access point dell'azienda più vicino il quale tramite la rete wireless lo comunica al server RADIUS dell'azienda. Quest'ultimo interfacciandosi con il DB verifica la presenza o meno del MAC. In caso positivo autentica l'antenna e quindi la collega alla rete, altrimenti non consente l'accesso.

5.3.2. Lo standard PPPoE

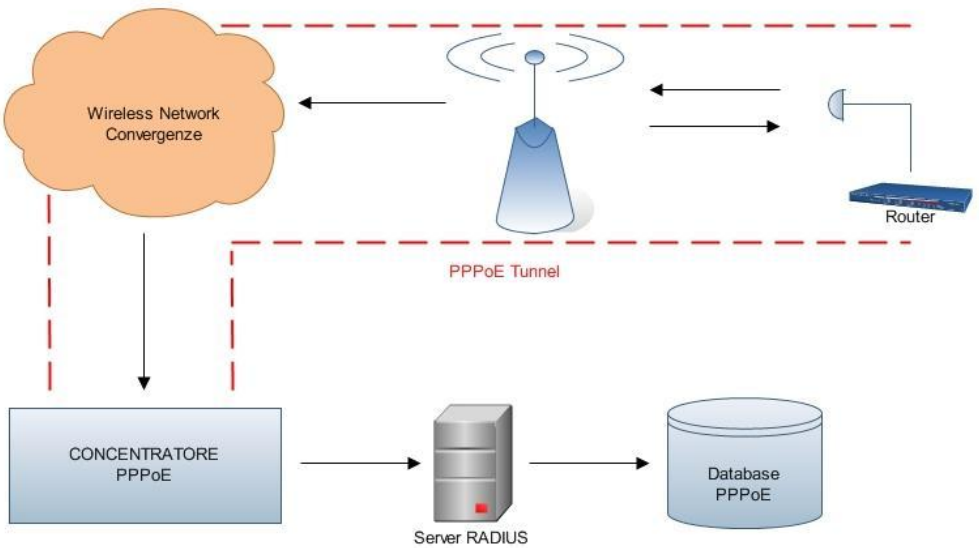
PPPoE significa "Point-to-Point Protocol over Ethernet" ed è un protocollo di rete che permette di incapsulare frame PPP in frame Ethernet. Tale protocollo è usato soprattutto per i servizi DSL.

PPP compone spesso il livello datalink (il livello di collegamento dati) del modello OSI nelle connessioni su circuiti punto-punto sincronizzati e non sincronizzati, soprattutto in ambito WAN.

Nella seguente tabella possiamo visualizzare la struttura del frame PPP

Nome	Numero di bytes	Descrizione
Flag	1	indica l'inizio o la fine del frame
Address	1	indirizzo broadcast
Control	1	byte di controllo
Protocol	2	indica il protocollo del campo data
Data	variabile (0 o più)	campo di dati
Checksum	2 (o 4)	somma di correzione

Lo standard PPPoE fornisce le caratteristiche standard di un protocollo PPP come l'autenticazione, la cifratura e la compressione . In particolare l'autenticazione di ogni cliente Convergenze viene effettuata tramite il controllo della coppia (username , password) fornita dall'azienda come ci mostra la figura sottostante



Come ci mostra la figura dal router del cliente al *concentratore PPPoE* dell'azienda si forma, in maniera del tutto trasparente, un tunnel di comunicazione.

Il concentratore ha un ruolo molto importante nella fase di autenticazione poiché va a controllare tramite un server RADIUS la presenza della coppia (username,password) nel DB dell'azienda. In caso positivo effettua l'autenticazione e quindi fornisce il servizio all'utente, altrimenti nega l'accesso.

Lo schema, inoltre, ci mostra come, indipendentemente dalla locazione del router (infrastruttura di rete a cui si è collegato), il concentratore controlla la fase di autenticazione. Ovviamente se il numero di utenti, come nel caso di Convergenze, è elevato ci saranno più concentratori ad occuparsi della fase di autenticazione (l'idea è quella di assegnare i concentratori in base alle zone di copertura).

6. Bibliografia

[1] Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i", National Institute of Standards and Technology, Special Publication 800-97, 2007, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[2] Guillaume Lehembre, "Sicurezza Wi-Fi – WEP, WPA e WPA2", articolo pubblicato nel numero 2/2006 della rivista hakin9, Febbraio 2006

[3] Wikipedia, "IEEE 802.11i", http://it.wikipedia.org/wiki/IEEE_802.11i

[4] Wikipedia, "IEEE 802.1X", http://it.wikipedia.org/wiki/IEEE_802.1x

[5] Fronza Danilo, "Wireless Ethernet standard, sicurezza e corretta configurazione della rete", 2005, http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0304/WirelessEthernet/

[6] CISCO White Paper, "EAP-TLS Deployment Guide for Wireless LAN Networks", 2002, http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a008009256b.shtml

[7] Changhua He, John C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i", NDSS Symposium 2005, http://www.isoc.org/isoc/conferences/ndss/05/proceedings/

[8] Duck-Ki Ahn, Su-Yong Kim, and Sung-Joon Cho, "An Analysis of Enhanced Wireless LAN for Robust Security Network", Dept. of Inform. & Telecom. Eng., Graduate School of Hankuk Aviation University, KICS 2003, http://mnet.skku.ac.kr/data/2003data/KICS2003/pdf/15-37.pdf

[9] RSA Laboratories, "PKCS #5 v2.0: Password-Based Cryptography Standard", Marzo 1999

[10] Andreas Klein, "Attacks on the RC4 stream cipher", Designs, Codes and Cryptography, Volume 48, Issue 3, Settembre 2008

[11] Martin Beck, Erik Tews, "Practical attacks against WEP and WPA", Conference On Wireless Network Security, Novembre 2008

[12] WIFI-ITA, articolo dal titolo "WPA crack", http://www.wifi-ita.com/index.php?option=com_content&task=view&id=127&Itemid=52

[13] WIFI-ITA, articolo dal titolo "NORMATIVA ATTUALE SUL WIRELESS", http://www.wifi-ita.com/index.php?option=com_content&task=view&id=23&Itemid=46

[14] Christophe Devine, documentazione "Aircrack-ng ed Aireplay-ng", http://aircrack-ng.org/doku.php

[15] Mike Kershaw, documentazione “Kismet: 802.11 layer2 wireless network detector”, http://www.kismetwireless.net/

[16] Joshua Wright, documentazione “coWPAtty: Brute-force dictionary attack against WPA-PSK”, http://www.willhackforsushi.com/Cowpatty.html

[17] Arunesh Mishra, William A. Arbaugh, “An Initial Security Analysis of the IEEE 802.1x Standard”, CS-TR-4328, UMIACS-TR-2002-10, University of Maryland, College Park, MD, Febbraio 2002, http://kulsoom.net/papers_slides/802_1x.pdf

[18] Yan Zhang, Jun Zheng, Honglin Hu, “Security in Wireless Mesh Networks”, CRC Press 2009

[19] Amitabh Mishra, “Security and Quality of Service in Ad Hoc Wireless Networks”, Cambridge University 2008

[20] Xiao, Shen, Z. Du, “Wireless Network Security”, Springer 2007

[21] Saitek, “How do I crack your WEP: The FMS attack explanation”, Italian Net Raiders, Maggio 2009, http://www.packetstormsecurity.org/papers/wireless/crack-your-wep.pdf