Oggi concluderemo il discorso sul protocollo WIFI (802.11).

Abbiamo visto una serie di peculiarità di questo protocollo, come il fatto che è simile all’802.3 (Ethernet) come impostazione, ma è via radio e usa come protocollo di accesso al mezzo il CSMA/CA anziché il CSMA/CD. Da questo consegue che il canale di comunicazione verso l’access point è unico è condiviso tra tutti gli host. Ci sono diverse versioni del protocollo che differiscono per la frequenza utilizzata: abbiamo la versione 11°, 11b e 11c. La 11° lavora su una frequenza di 5GHz come canali radio (e che non era possibile usare in Europa per via della frequenza troppo alta che violava il regolamento sulle reti radio). La 11b lavora sulla frequenza 2.5GHz, ed è quella che si è diffusa di più una rete. La 11g, sviluppata successivamente, lavora sempre su 2.5 GHz ma usa un metodo di accesso ai canali radio uguale a quello della versione a, offrendo una banda di comunicazione più elevata (di 54 Mbit/s). La quantità di informazioni che si riesce a scambiare effettivamente tra due host è di circa 22 Mbit/s, + o – la metà. Questa riduzione deriva dal fatto che due host comunicano attraverso l’access point, facendo lo store and forward per almeno un hop e dall’impatto del protocollo CSMA/CA, che ritarda un minimo la comunicazione per evitare le collisioni. C’è infine da considerare il ritardo dovuto ai messaggi RTS CTS, che generano un overhead che impatta sulla velocità media della trasmissione.

La dimensione massima dei frame 802.11 dovrebbe essere di 2000 bytes (un po’ di più degli ethernet che erano limitati a 1500 bytes), quindi per questi messaggi (che occupano tutti o quasi questi byte) conviene occupare il canale con il RTS e CTS.

Lo standard appena descritto risale al 2003. Successivamente è stata introdotta la versione m (802.11m), che aumenta la banda di comunicazione usando contemporaneamente la connessione a e quella g (5 GHz + 2.5 GHz, però non è utilizzabile in Europa). L’ultimo tipo di protocollo è l’802.11-2020, risalente al 2020 che usa una frequenza a 6 GHz e permette di ottenere una banda di almeno 600 Mbit/s, chiamata anche “versione ax” (802.11ax).

Normalmente l’access point viene collegato anche a una rete fissa, permettendo agli host di comunicare tra di loro ma anche ad altri host di una rete fissa e a quelli presenti sulla rete internet. Dunque l’access point ha sempre almeno una porta di comunicazione su rete fissa, che usa il protocollo di Data Link Ethernet. C’è quindi da considerare la possibilità di comunicazione tra un host appartenente a una rete wireless e un altro collegato via ethernet. Per ottenere ciò bisogna prendere un frame 802.11 e trasformarlo nell’equivalente in 802.3, e viceversa (da 802.3 a 802.11).  
Il canale fisico di trasmissione ha una velocità nettamente maggiore rispetto a quello wireless. Quindi uno potrebbe aspettarsi una banda di comunicazione superiore quando si comunica con un dispositivo connesso via Ethernet, ma questa speranza non è ragionevole per via del tempo richiesto per la trasformazione dei frame. (dunque sia in caso di comunicazione wireless che mista ci si può aspettare una banda di 22 Mbit/s).

Grazie al fatto che si usano gli indirizzi MAC in entrambi i protocolli, la traduzione da un frame Data link di tipo Ethernet a uno di tipo Wi-fi e viceversa non è difficile. Una cosa che si ha in più nell’802.11 è la possibilità di specificare 3 (o a volte 4) indirizzi MAC per permettere la comunicazione via radio. Ma ciò non è un problema perché da rete fissa non si vede l’indirizzo MAC dell’access point (mentre da rete radio sì).

Passiamo ad affrontare il problema relativo alla SICUREZZA del wi-fi. La sicurezza del Wi-fi è un mezzo disastro, perché bisogna tenere conto di quello che è successo alcuni anni fa. Con l’introduzione delle versioni a e b dell’802.11 si era pensato di risolvere il problema introducendo il modello di sicurezza WEP (Wired-equivalent-privacy / protection), cercando di costruire il sistema via radio in modo che fosse simile a quello di una rete fissa/con fili a livello di sicurezza.

Ma se noi mettiamo a confronto una rete 802.3 in modalità Switch (con hosts connessi mediante doppini telefonici) con un’altra di tipo 802.11 con access point e hosts wireless, notiamo che sulla rete fissa l’attaccante deve potersi collegare con un filo allo switch, operazione impossibile se teniamo lo switch in un posto sicuro. Quindi l’unica possibilità per un attaccante nel caso di un rete fissa e avere un virus installato su una macchina già collegata alla rete, ma nel caso di una rete wireless via radio la situazione è diversa: nessuno può impedire a un attaccante di agganciarsi all’access point dalla strada davanti casa nostra (non è quindi necessario che installi un virus su un nostro dispositivo).

L’idea del tipo di sicurezza WEP, dunque, era stato quello di cifrare le comunicazione, rendendo i messaggi trasmessi incomprensibili a un attaccante che non avesse avuto la chiave di cifratura (e si assumeva che ciò desse lo stesso livello di sicurezza di una rete fissa, visto il nome WEP).

L’idea dietro l’algoritmo di cifratura era che fosse da applicare solo ai frame di tipo dati. Questo lasciava non cifrati i frame di tipo Management, Control e Extension (anche perché sennò gli host non potrebbero proprio connettersi). Per effettuare la cifratura si definiva sulla rete locale una password comune, utilizzata da tutti gli host legittimi. La password veniva usata come chiave per l’algoritmo di cifratura RC4 (scelto perché è un algoritmo che permette di cifrare e decifrare molto velocemente), che usa una tecnica di “codice a flusso”: si ha un generatore di numeri pseudocasuali che produce una sequenza di bit che sembra imprevedibile, ma in realtà conoscendo il seme di partenza del generatore è possibile prevedere la sequenza prodotta dall’algoritmo. Per mandare il messaggio bastava dunque fare uno XOR tra questo e la sequenza che si prevede genererà l’algoritmo RC4, Dall’altra parte (a destinazione) facendo sempre lo XOR bit a bit con la sequenza effettivamente generata dall’RC4 era quindi possibile riottenere il messaggio di partenza.

Di base la tecnica era parecchio efficacie, perché prevedere la sequenza avendo il seme era piuttosto veloce come operazione, e il costo temporale dello XOR era trascurabile.

Si è scelto questo algoritmo anzichè “One-Time-Pad, perché questo prevede che sia generato un numero casuale della stessa lunghezza del messaggio che vogliamo inviare e di usare quella per fare lo XOR del messaggio, e di inviarlo. Il problema è che in questo caso le chiavi sarebbero grandissime (lunghe quanto il messaggio) e che dovrebbero essere note a priori, perché non si usa un seme di generazione noto a tutti, nonché utilizzabili una volta sola.  
Questo secondo algoritmo è quindi PERFETTAMENTE SICURO (molto più dell’RC4) ma è inutilizzabile nella pratica.

Ma RC4, sebbene “sicuro”, aveva delle vulnerabilità: infatti se applicato brutalmente per la codifica delle informazioni (senza nessuna accortezza), come è stato fatto, cadeva in un punto debole. RC4 infatti non aveva buone caratteristiche di confusione e di diffusione. Questi termini indicano la possibilità che analizzando un testo cifrato si possa o meno dedurre quale fosse la chiave di cifratura. Infatti, si sarebbero dovuti eliminare i primi byte del keystream perché sono in forte correlazione con la chiave usata per cifrare, mentre i successivi no: eliminando i primi byte si sarebbe ottenuto un algoritmo sicuro. Ma nella specifica del protocollo 802.11 gli sviluppatori non lo hanno fatto e nel giro di un anno o due dall’uscita di questo protocollo sono venuti fuori i primi attacchi che sfruttavano questa vulnerabilità.

Infatti basandosi sul fatto che alcune informazioni negli headers sono sempre le stesse (come il time to live), e analizzando i primi bytes del messaggio codificato era diventato facile ricostruire le chiavi di cifratura (e quindi le password di accesso alla rete).

Il passo successivo è stato l’introduzione del protocollo di cifratura WPA. Si è mantenuto la conoscenza di una chiave condivisa su tutta la rete wireless e su questo algoritmo non sono stati sviluppati attacchi, anche perché poi è stato sostituito da WPA-2, che cambia la tecnica di cifratura dallo Stream CIpher a un Block Cipher. La cifratura con Block Cipher è completamente diversa dall’altra, e una delle sue caratteristiche è che il tempo per cifrare e decifrare un messaggio è più lungo. Per introdurre la cifratura WPA-2 in un access point è stato necessario inserire dei coprocessori nell’access point che decifrassero i messaggi prima dell’invio. Si ha ottenuto un aumento del costo dal punto di vista hardware per la realizzazione dei dispositivi, ma il lato positivo è che non sono ancora stati trovati attacchi da poter fare a questo sistema di cifratura. Il block cipher utilizzato è l’AES (Advanced Encryption Standard): è quello attualmente in uso per tutte le applicazioni sensibili.

Questo ha risolto la problematica dal punto di vista dell’accesso wireless alla rete, ma non ha tenuto conto della possibilità di altri tipi di attacchi, come il Denial Of Service. Per rendere inoperativo un sistema radio è super facile, basta mandare dei disturbi abbastanza potenti con sufficiente frequenza.

In WPA-2 abbiamo un livello di protezione superiore perché la password condivisa è in realtà la base per generare altre chiavi di cifratura, che sono di sessione (e non accessibili da host diversi da quello con cui si è concordato l’access point) e che garantiscono sicurezza. Tuttavia la negoziazione delle chiavi di cifratura avviene in chiaro, quindi chiunque dall’esterno potrebbe mandare dei messaggi di cambio chiave che nullifichino le chiavi concordate tra access point e host legittimo, creando un altro tipo di Denial of Service.