

UNIVERSITA' DEGLI STUDI DI BOLOGNA

Facoltà di scienze matematiche fisiche e naturali

CORSO DI LAUREA IN SCIENZE DI INTERNET

Tesina per il corso di Reti Wireless

“IL WEP. FUNZIONAMENTO, PROBLEMI E POSSIBILI SOLUZIONI”

AUTORE

SUSI STEFANO

DOCENTE

LUCIANO BONONI

CAP 0 - Introduzione

CAP 1 - Il Funzionamento del WEP

- Autenticazione
- L' Algoritmo RC4
- Inizialization Vector (IV)
- WEP Keys
 - Default Keys
 - Key Mapping Keys

CAP 2 - I Meccanismi del WEP

- Frammentazione
- Integrity Check Value (ICV)
- Preparazione del frame per la trasmissione
- L'algoritmo RC4

CAP 3 - Perché il WEP non è sicuro ?

- Authentication
- Access control
- Replay Prevention
- Message modification detection

CAP 4 - Debolezze nell'utilizzo di RC4 in WEP

- Riutilizzo IV
- RC4 Weak Keys
- Direct Key Attacks

CAP 5 - Regole di base per una corretta configurazione degli

apparati di rete

- Configurazione dei dispositivi
- 802.1X . Una possibile soluzione

Introduzione

Una delle problematiche principali delle reti 802.11 è quella relativa alla sicurezza. Sebbene i vantaggi di tale tecnologia sono innumerevoli, esistono molte vulnerabilità legate alla natura intrinseca del mezzo trasmissivo. L'etere infatti è di dominio pubblico, quindi potenzialmente chiunque è in grado di captare in qualche modo i pacchetti di informazioni che vi transitano. Per ovviare a questo problema è stato introdotto fin dalla prima versione dello standard un sistema di sicurezza chiamato Wired Equivalent Privacy, detto comunemente WEP. Come vedremo nella nostra rassegna il WEP risulta essere facilmente aggirabile, fornendo perciò un falsa sensazione di sicurezza negli utenti che penseranno di inviare i loro dati nell'etere in totale sicurezza quando in pratica sono facilmente decifrabili. Inoltre i venditori hardware si sono preoccupati solo in parte di questo aspetto, producendo apparati che molto spesso implementano male uno standard già di per se già fragile, tutto questo è stato fatto per ragioni economiche, prima si arriva sul mercato più vantaggioso si ha rispetto ai concorrenti, tralasciando completamente l'aspetto sicurezza.

Ci sono anche problematiche legali da ricordare, se si è sottoposti ad un attacco, è l'amministratore che sarà formalmente responsabile dell'atto di pirateria informatica, fino a quando autorità giudiziali non troveranno prova dell'avvenuta intrusione .

CAP 1 - Il Funzionamento del WEP

Nei suoi primi anni di vita, l'802.11 ha avuto solo un metodo definito per la sicurezza, il WEP appunto. Sebbene è stato crackato un pochissimo tempo, esso provvede a fare da barriera, sebbene piccola, agli attacchi provenienti dall'esterno di utenti non espertissimi che stanno solamente cercando una rete non protetta. Inoltre esso risulta uno strumento molto efficace per utenti domestici che inoltrano nell'etere pochi pacchetti, per poter crackare WEP si richiedono un enorme mole di pacchetti.

Quando fu sviluppato WEP, l'intento dei programmatori non era quello di garantire un livello di sicurezza militare, lo standard, come indicato nella sezione 8.2.2 dell'IEEE 802.11, doveva risultare :

- **Ragionevolmente forte.** Il Wep risulta difficile da abbattere attraverso un attacco di forza bruta. Logicamente il tempo impiegato sarà proporzionale alla lunghezza della chiave e alla cambiamento della chiave stessa.
- **Auto sincronizzato** In WEP ogni messaggio è auto-sincronizzato. Questa proprietà è critica per un algoritmo che lavora a livello data-link, dove si deve cercare di fare il meglio possibile e dove la perdita dei pacchetti è alta.
- **Efficiente** : l'algoritmo WEP risulta infatti molto efficiente e può essere implementato su qualsiasi hardware e software.
- **Esportabile** e doveva poter essere **opzionabile.**

La sua versione a 40 bits risultò fin da subito vulnerabile ad attacchi di forza bruta.

In ogni caso è ancora un mistero il perché si è voluto sviluppare un livello di sicurezza ragionevole. Molti specialisti ritengono infatti che vi siano solo due livelli di sicurezza: forte e

non. Ed il WEP sicuramente non risulta forte, l'unica spiegazione plausibile sta nel pensare che si ritenesse che la sicurezza fosse garantita ad altri livelli (per esempio attraverso un VPN).

In ogni caso ci sono state anche forti politiche commerciali che hanno guidato lo sviluppo rapido di un protocollo di "sicurezza", per poter fare pensare alle persone che le reti wireless fossero sicure. Sulle prime brochure la parola ragionevolmente sicura fu sostituita con sicura, e nel momento che si sviluppò la versione a 104 bits la rete diventò assolutamente sicura.

1.1 - Autenticazione

Ci sono due parti del WEP che sono descritte nello standard. La prima è la fase di autenticazione, la seconda fase di encryption.

L'idea che è alla base è la seguente : quando un nuovo dispositivo mobile vuole unirsi ad un AP , egli deve provvedere alla sua identificazione. Abbiamo quindi la necessità di studiare meglio il concetto di autenticazione, perché la sua implementazione in WEP si è rivelata un'impresa inutile. Lo scopo dell'autenticazione è quello di dimostrare che ogni device sia quello che sostiene essere.

In un ambiente di LAN, ogni dispositivo ha un numero unico (o presunto tale) denominato il MAC ADDRESS. Ogni trasmissione da un dispositivo sulla lan contiene il relativo MAC ADDRESS in modo tale che la sua identità possa essere controllata. Ma come sapete se qualcun'altro non ha forgiato un messaggio con un MAC ADDRESS falso?

Un metodo può essere quello di autenticare un dispositivo nel momento in cui accede alla rete mettendosi d'accordo su una chiave segreta che sarà usata per proteggere qualsiasi pacchetto.

Poiché soltanto il dispositivo ed il punto di accesso conoscono il codice segreto, ogni messaggio può essere convalidato come autentico quando è ricevuto. Ciò è lo scopo dell'autenticazione si prefigge.

In 802.11 WEP c'è una fase di autenticazione in cui i nuovi device dimostrano di essere un membro fidato del gruppo. Andiamo a vedere come lo si fa.

Logicamente se un client può provare di essere fidato, è ragionevole credere che il suo MAC address sia vero.

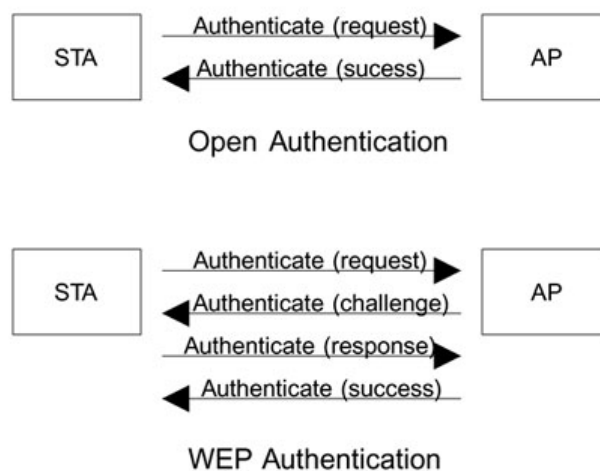
Sfortunatamente in WEP nessun token segreto è scambiato su autenticazione. Quindi non c'è nessun modo per sapere se una sottosequenza di pacchetti proviene da un device fidato o da un "impostore".

Questo tipo di autenticazione infatti è stata ritenuta a posteriori piuttosto imbarazzante oltre che un inutile compito, infatti è stata completamente eliminata nelle successive specifiche Wi-Fi.

Nonostante questi inconvenienti, alcuni sistemi ancora utilizzano la fase di autenticazione dello standard originale IEEE 802.11. Andiamo quindi ad analizzare come i messaggi sono scambiati.

La fase di autenticazione usa management frames, come mostrato in figura

Figure . Authentication Sequences in the Original IEEE 802.11 Standard



Per la Open Authentication , i dispositivi mobili mandano un messaggio di richiesta di autenticazione e l'AP replica sempre con un messaggio di successo.

Per la WEP Authentication vi è uno scambio di quattro messaggi. Prima il client richiede l'autenticazione, successivamente l'AP inoltra un challenge message. Il dispositivo mobile a questo punto risponde dimostrando di sapere la chiave segreta, se quest'ultima è accettata sarà inoltrato un messaggio di successo.

Se l'AP sta operando in open mode, egli accetterà sempre le richieste di autenticazione. In pratica però molti sistemi hanno un metodo di selezione, che contiene una lista indirizzi MAC dei dispositivi a cui è consentito l'accesso. Logicamente questa lista è stipulata dall'amministratore del sistema e può essere aggiornata. Come si vedrà in seguito, il filtraggio dei MAC address non risulta ad ogni modo un metodo per garantire sicurezza.

Quando si opera con la WEP Authentication, si vuole sapere se il client conosce la chiave segreta. Quando il dispositivo mobile richiede l'autenticazione, l'AP manda un numero random chiamato "challenge text". Questo è un numero di 128 bit. Successivamente il client cripta questo numero con la chiave segreta e lo manda indietro all'AP. Visto che l'AP ricorda il numero random che ha precedentemente inoltrato, egli può verificare se la risposta è stata criptata con la chiave corretta. Questo meccanismo paradossalmente risulta un arma a doppio taglio, infatti il challenge contiene il plaintext mentre la risposta il testo cifrato. Proprio per questo la Wi-Fi Alliance, ha deprecato del tutto l'uso di questo meccanismo.

Per completezza andiamo ad analizzare il frame di autenticazione

Figure 11. Authentication Message Format

Algorithm Num	Transaction Seq.	Status Code	Challenge Text
---------------	------------------	-------------	----------------

- Il campo "Algorithm Number" indica il tipo di autenticazione usata :

0 – Open system

1 – Shared key (WEP)

- Il Transaction Sequence ci indica dove ci troviamo nella sequenza di autenticazione . Per il primo messaggio avremo 1, per il secondo 2, per il terzo 3(usato solo in WEP).
- Lo Status Code è mandato nel messaggio finale per indicare il successo o il fallimento della richiesta di autenticazione
- Il Challenge Text è usato solo nell'autenticazione WEP, come precedentemente descritto.

1.2 - L' Algoritmo RC4

In principio nelle specifiche del WEP erano previste due fasi: una fase di autenticazione, una fase di criptazione dei dati. Come abbiamo visto la fase di autenticazione non solo si è dimostrata inutile, ma fornisce un gran numero di informazioni pericolose a coloro che volessero effettuare un attacco. Si tende quindi a saltare completamente la fase di autenticazione, così facendo non si dà nessun particolare vantaggio ad un attaccante, gli si consente solo di associarsi alla rete in maniera incondizionata, ma non gli è permesso ascoltare il traffico della rete senza sapere la chiave WEP per la criptazione .

I sistemi di sicurezza si basano su stream cipher o block cipher. Gli stream cipher prendono una sequenza di dati in chiaro (plaintext) e producono una sequenza di dati criptati (ciphertext), il loro lavoro può essere visto come un processo continuo.

Per quanto riguarda i block cipher utilizza singoli blocchi di dati in un determinato tempo. Solitamente i dati hanno una lunghezza fissa, tipicamente 8,16 o 32 bytes. Ogni blocco è criptato grazie ad un particolare algoritmo che produce un blocco differente della stessa lunghezza.

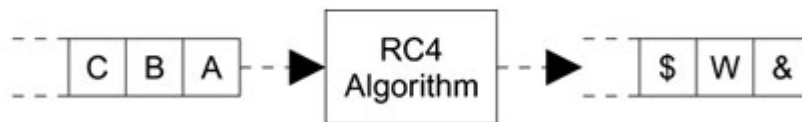
La differenza principale dei due approcci si trova nel fatto che in uno stream cipher il suo stato interno è completamente aggiornato mentre i dati sono processati, al contrario in un block cipher lo stato è resettato nel momento in cui un blocco precedente è stato processato.

Il WEP utilizza un stream cipher chiamato RC4 per criptare i pacchetti di dati.

Ad alto livello, come mostrato in figura, RC4 è una black box che prende un byte da uno stream di dati e produce un byte diverso ma della stessa grandezza in output.

In questo meccanismo la decriptazione avviene attraverso il processo inverso, e fa uso della stessa chiave, proprio per questo è chiamato Symmetric Algorithm.

Figure . Stream Cipher



Uno dei vantaggi dell'RC4 è l'essere abbastanza facile da implementare e non fa uso di complicate o dispendiose (dal punto di vista del tempo) operazioni quali per esempio la moltiplicazione.

In RC4 esistono 2 fasi, nella prima, detta di inizializzazione, alcune tabelle di dati sono costruite basandosi sul valore di chiave fornita, nella seconda fase i dati sono gestiti e criptati.

Nel caso del WEP entrambe le fasi si verificano per ogni pacchetto. Quindi ogni pacchetto è trattato come se fosse un nuovo stream di dati, questo garantisce che se un pacchetto è perso il pacchetto seguente può essere criptato in maniera autonoma. Questa soluzione è da un punto di vista una forza ma, come vedremo successivamente, è anche un punto di debolezza.

1.3 - Initialization Vector (IV)

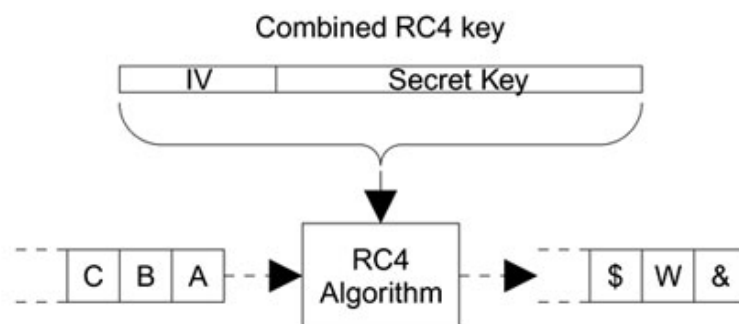
Molti produttori di schede riferiscono che i loro dispositivi hanno un livello di sicurezza a 128 bit invece di 104. In verità 24 bit sono riservati per allocare l'Initialization Vector (IV).

Sebbene le chiavi possono essere cambiate in qualsiasi istante, in pratica i pacchetti sono criptati usando lo stesso valore di chiave. Quindi se la chiave risulta fissa ogni volta che immetto un lo stesso plaintext otterrò un testo cifrato uguale. Come si è già discusso un comportamento del genere potrebbe essere facilmente sfruttato da un attaccante che osserva una ripetizione di testo cifrato. Anche perché l'indirizzo IP è sempre posizionato nella stessa posizione all'interno del pacchetto.

Per risolvere questo problema è stato introdotto l'IV. Invece di usare direttamente la chiave segreta per criptare il pacchetto, si concatena la chiave con l'IV, che è un numero di 24 bit che cambia per ogni pacchetto inviato.

L'IV però viene inviato in chiaro, quindi non sembra corretto parlare di sicurezza a 128, quando in verità è di 104.

Figure . Using the IV



Siccome l'IV è sempre diverso, la chiave usata effettivamente per la criptazione dei dati cambierà sempre per ogni pacchetto inviato, quindi anche se il plaintext fosse lo stesso, il ciphertext sarà sempre differente.

Ma come abbiamo visto l'IV non è segreto, esso è spedito in chiaro, perché in questo modo il ricevente può ricavare il valore usato per la criptazione. In linea teorica la conoscenza dell'IV è inutile per un attaccante senza che egli possiede la chiave segreta, ma in pratica poiché questa soluzione risulti efficace un IV non deve essere mai usato 2 volte con la stessa chiave segreta.

Per sfortuna in WEP l'IV è un numero di soli 24 bits, questo fa sì che vi siano solo 16.777.216 di combinazioni ovvero 2^{24} , questo numero potrebbe sembrare enorme ma in pratica bastano poche ore di ascolto sul canale per trovare una ripetizione dell'IV.

Come se non bastasse la gestione dell'IV da parte del dispositivo è fatta incrementando di uno il contatore, che solitamente si ri-inizializza ogni volta che il dispositivo viene estratto dal PC oppure ogni volta che si verifica una collisione di pacchetti, in questo modo quindi è più facile trovare ripetizioni per numeri bassi.

Ultimamente è stata sviluppata una nuova versione del WEP, chiamata TKIP, anch'essa basata su RC4, ma che evita il riuso degli IV.

1.4 - WEP Keys

Una scomoda terminologia degli standard WEP, ha portato molti produttori a clonare nuovi termini, con l'intento di facilitare la comprensione degli utenti finali. Il risultato però è stato disastroso, attualmente esistono svariati modi per indicare lo stesso concetto.

Nel standard WEP originario sono menzionati solo due tipi di chiavi WEP :

- Default key(s)
- Key mapping key(s)

Di seguito riporto quali sono gli altri termini di uso comune per indicare lo stesso concetto :

Table . Manufacturer Names for WEP keys

Standard Term	Manufacturer's Term
Default key	Shared key
	Group key
	Multicast key
	Broadcast key
Key mapping key	Key
	Individual key
	Per-station key
	Unique key

Le chiavi WEP hanno le seguenti caratteristiche :

- **Lunghezza fissa** : solitamente di 40 o 104 bits.
- **Statiche**: non possono essere cambiate se non riconfigurando il dispositivo.
- **Condivise**: L'AP e i client devono avere la copia della stessa chiave.
- **Simmetriche**. La chiave è usata sia in fase di criptazione che di decrittazione

Lo standard convenientemente "bypassa" i problemi relativi alla sicurezza, affermando semplicemente che :

"The required secret is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11."

Una soluzione a molte problematiche del WEP potrebbe essere quella di cambiare frequentemente la chiave, ma sebbene questa operazione potrebbe essere facilmente svolta in un ambiente domestico con pochi computer, diviene impensabile per una grossa azienda con centinaia di macchine da dover riconfigurare periodicamente.

Molte aziende produttrici di dispositivi wireless stanno presentando differenti approcci, implementati o sui driver della scheda stessa, o attraverso un floppy disk che contiene la chiave in

qualche formato non conosciuto. In ogni caso nessuna di queste soluzioni rientra nelle specifiche WEP.

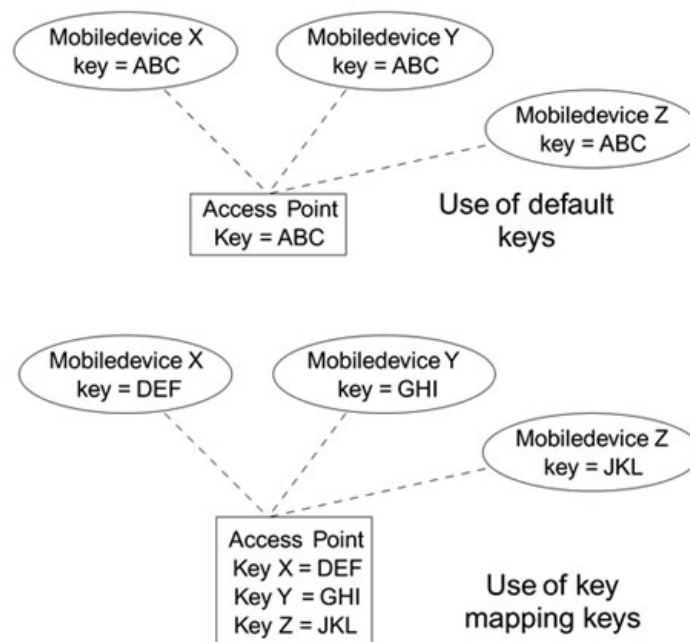
Ci sono due differenti approcci nell'uso di chiavi sotto WEP. Quando si è redatto lo standard non si è trovato un accordo per cui sono stati specificati entrambi i metodi, assumendo che il mercato deciderà quale dei due sia il migliore.

Nel primo caso, tutti i dispositivi mobili e l'AP usano un singolo set di chiavi. Queste chiavi sono chiamate **default keys**.

Nel secondo caso, ogni dispositivo mobile possiede una chiave che è unica. In altre parole la chiave usata tra ogni client e l'AP è specifica della connessione e non è conosciuta degli altri client. Queste chiavi sono chiamate **key mapping keys**.

Le due modalità sono illustrate nella figura seguente :

Figure . Difference Between Default and Key Mapping Keys



Nel primo caso tutti i dispositivi devono sapere solo una chiave tra di loro. Nel secondo i client devono sapere una chiave, ma l'AP deve avere una tabella di tutte le chiavi.

Default Keys

Molte case produttrici presentano solo questa modalità di inserimento delle chiavi, quindi tal volta ci si trova di fronte ad una non scelta.

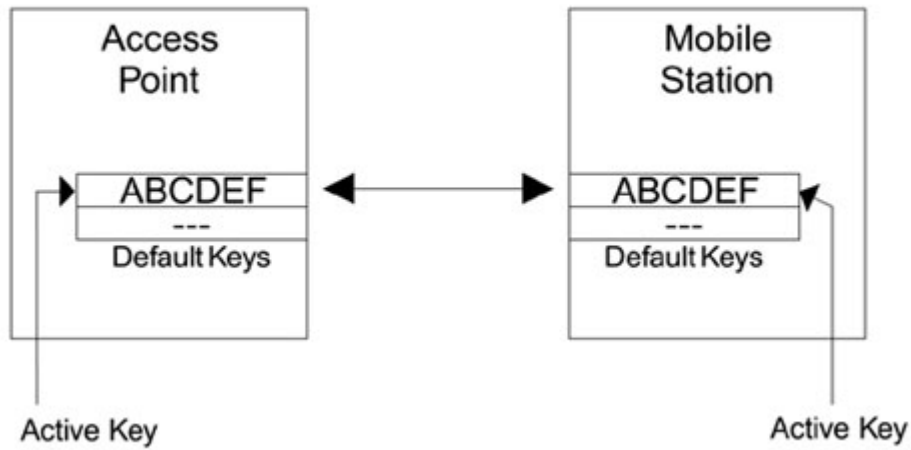
Lo standard prevede che ci possono essere fino a 4 chiavi WEP per ogni device. Questo si è rivelato una grande fonte di confusione tra gli utenti, perché non riuscivano a capire se devono essere impostate obbligatoriamente tutte e quattro, e se devono essere le medesime per ogni dispositivo. A causa di queste incertezze molti utenti hanno optato per non utilizzare il WEP.

La possibilità di avere chiavi multiple è stata introdotta per non dover interrompere le comunicazioni in rete nel momento in cui si cambia la chiave dell'AP. L'utilizzo di una singola chiave si rileva quindi un forte collo di bottiglia.

Quando sono definite chiavi multiple invece, tutte le trasmissioni utilizzano la chiave di default (active key), ma vi è la possibilità di decriptare in fase di ricezione con qualsiasi chiave specificata.

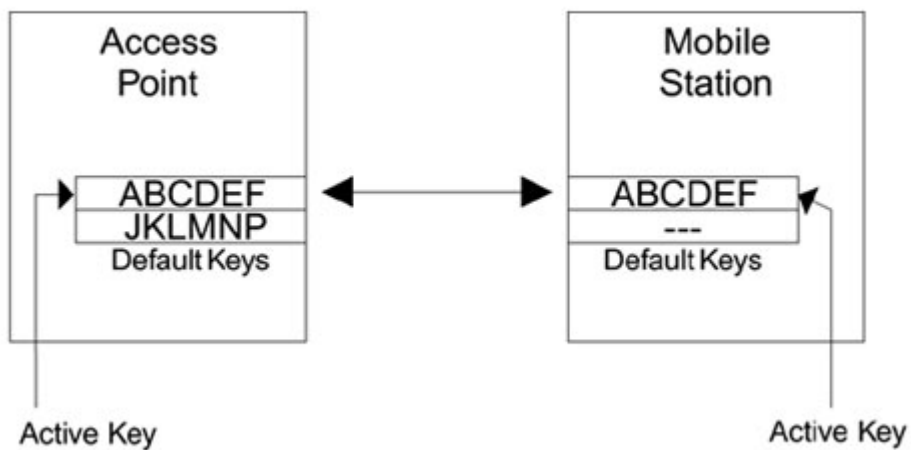
La tecnica a chiave multipla permette che l'aggiornamento delle chiavi sia molto più facile, vediamo come.

Figure A. Before Changing Keys



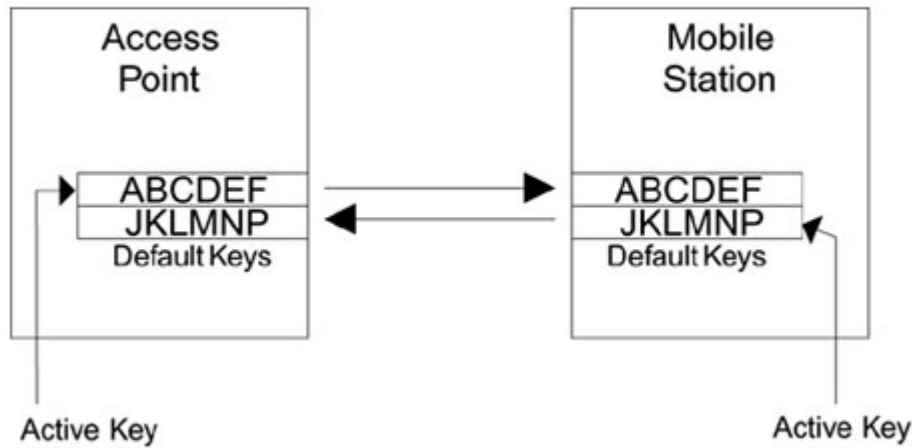
Inizialmente i client e l'AP utilizzano la chiave di default ABCDEF(active key).E' da notare che nessuna altra chiave è stata specificata ---- (fig A)

Figure B. Adding a Second Default Key



Successivamente l'amministratore decide di cambiare le chiavi, inserisce quindi una nuova chiave nell'AP JKLMNP come seconda chiave di default. In questo momento la trasmissione continua ad utilizzare ancora la prima chiave.

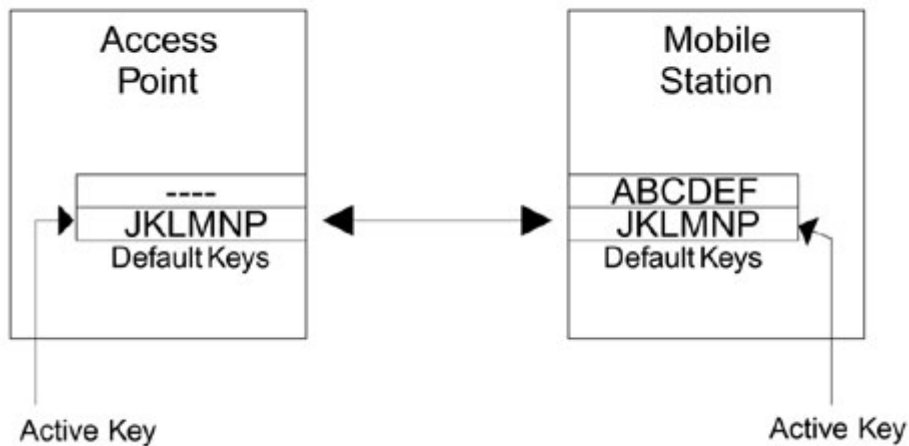
Figure C. Use of Both Old and New Keys



Successivamente si inserisce la seconda chiave di default su tutti i client, e la si rende attiva. In questo momento il cliente sta utilizzando la nuova chiave JKLMNP (fig C).

Ma l'AP deve utilizzare ancora la vecchia chiave per permettere a tutti i device presenti in rete, di poter aggiornare la loro chiave. In ogni caso anche i dispositivi che hanno aggiornato la chiave dispongono di una copia della vecchia.

Figure 6.6D. Completed Key Update



Logicamente c'è un limite di tempo per effettuare il cambiamento delle chiavi, alla fine di questo sarà sera attiva la seconda chiave JKLMNP , mentre la prima verrà rimosso (fig D) .

Quando si opera con più chiavi si possono usare chiavi differenti in ogni direzione, ma la trasmissione dei frame avverrà sempre usando la active key.

La active key è utilizzata usando un numero: 0,1,2,3 che è presente in un campo del frame chiamato **KeyID** bits. In questo modo il destinatario conoscerà la chiave da utilizzare in fase di decrittazione.

Non per forza l'utente deve inserire tutte e quattro le chiavi, logicamente come abbiamo descritto l'utilizzo di una sola chiave porterà ad un collasso, sebbene momentaneo, della rete.

Key Mapping Keys

Il meccanismo che è alla base del key mapping keys è che ogni dispositivo possiede un proprio valore di chiave. I benefici di questo approccio sono maggiori per le reti che hanno una base di macchine installate molto alta.

Non tutti i dispositivi presenti in commercio dispongono di questa caratteristica, perciò bisognerà stare molto attenti in fase di acquisto.

L'utilizzo di chiavi differenti comporta però alcune modifiche sulla gestione del traffico di broadcast.

In una LAN condivisa vi sono tre tipi di messaggio:

- Unicast Messages : sono mandati ad una singola destinazione
- Group Messages : sono inoltrati verso alcuni destinatari della rete
- Broadcast Messages : sono sentiti da tutti i dispositivi della rete.

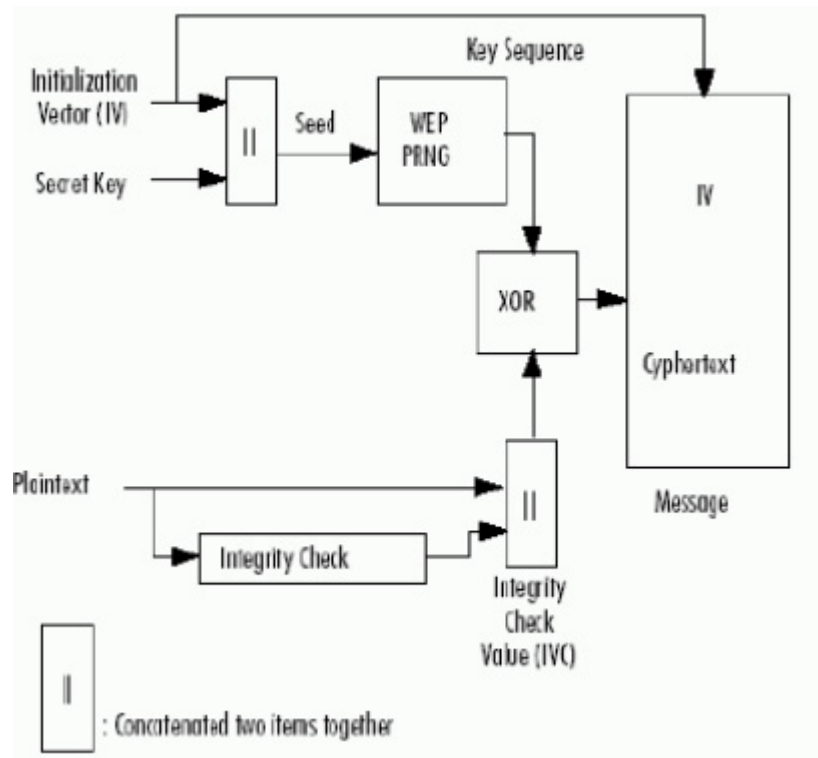
Ma se ogni dispositivo utilizza una chiave diversa, come fa l'AP a mandare un messaggio di broadcast ?

Il traffico multicast è inoltrato usando una chiave condivisa da tutti i dispositivi(default key). Solo i messaggi unicast sono inoltrati con la chiave unica. In virtù di queste caratteristiche vi devono essere almeno due chiavi in ogni dispositivo. A parte questo non c'è nessun'altra differenza rispetto alla prima modalità.

Sul lato AP le cose si complicano un po', perché ci deve essere una tabella che associa ad ogni dispositivo(individuato dal MAC address) la chiave unica, per poter decifrare in maniera corretta il messaggio. Inoltre tutto questo richiede uno spazio di memoria aggiuntiva, e se vi è una comunicazione tra 2 AP, ogni AP deve avere la stessa tabella.

Il key mapping key risulta quindi una buona soluzione, ma come visto non è sviluppata per tutti i dispositivi, inoltre sono stati introdotti nel tempo altri meccanismi come il WPA che garantiscono una maggiore sicurezza.

CAP 2 - I Meccanismi del WEP



2.1 - Frammentazione

Andiamo ad analizzare adesso il funzionamento dei pacchetti criptati con il WEP all'interno delle reti wireless .

Un pacchetto di dati è chiamato MSDU (MAC service data unit), se tutto andrà bene questo sarà inoltrato verso il sistema operativo e sarà consegnato all'applicazione target.

Durante questo processo, il pacchetto MSDU viene spezzettato in pezzi più piccoli prima di arrivare alla trasmissione radio. Questo processo è chiamato Frammentazione.

Ogni frammento viene processato per criptazione WEP, inoltre viene aggiunta un intestazione MAC all'inizio del pacchetto e una checkword alla fine.

Ognuno di questi pacchetti più piccoli è chiamato MPDU (MAC protocol data unit).

Il processo di frammentazione tratta i dati come un blocco di bytes non formattati, la loro dimensione dipende dall'MSDU originale e dalle politiche di frammentazione. Solitamente il range tipico è compreso tra i 10-1500 bytes.

Il primo passo di criptazione è quello di aggiungere alcuni bytes chiamati Integrity Check Value.

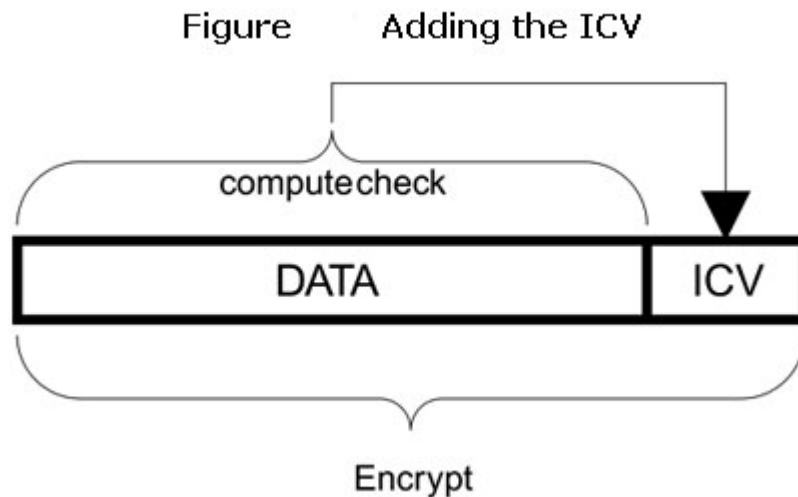
2.2 - Integrity Check Value (ICV)

L'idea che sta alla base dell'ICV è quella di evitare a chiunque di alterare il messaggio in transito. Durante le fasi di criptazione viene effettuata una verifica per vedere se alcuni bit sono stati corrotti durante la trasmissione. Tutti i bytes del messaggio sono combinati in un risultato chiamato CRC. Questo è un valore di 4 byte che è aggiunto alla fine del pacchetto poco prima di essere trasmesso. Se un solo bit nel messaggio è corrotto, il ricevitore individua che il valore del CRC non corrisponde e rigetta il messaggio.

Questo però non dà sicurezza, perché un attaccante potrebbe ricalcolare facilmente il CRC dopo aver alterato il messaggio.

ICV è simile al CRC eccetto per il fatto che è calcolato e aggiunto prima della fase di criptazione. Il CRC convenzionale lo fa dopo. L'intento dell'ICV è ottimo, ma è stato fatto notare che la sua implementazione è risultata sbagliata. Vediamo come funziona.

L'ICV è calcolato combinando tutti i dati di byte, il suo valore finale viene aggiunto in 4 byte alla fine, come vediamo nella figura seguente :



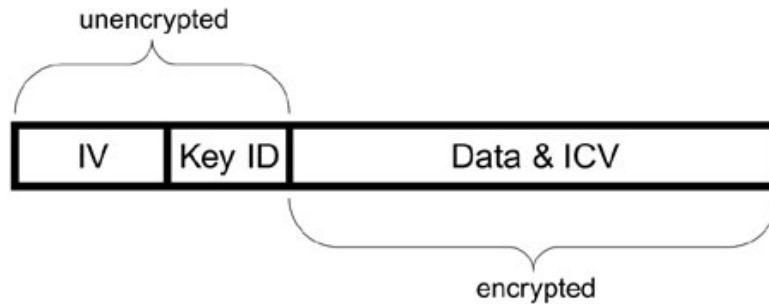
2.3 - Preparazione del frame per la trasmissione

Dopo che l'ICV è stato apposto, il frame è pronto per la fase di criptaggio. Adesso il sistema deve selezionare l'IV e concatenarlo con la chiave WEP scelta. Dopo inizializza l'RC4, ricordiamo che è uno stream cipher di tipo simmetrico, quindi le due fasi sono identiche.

Il ricevente, deve conoscere sia l'IV che il numero di chiave usata, quindi queste informazioni devono essere immessi all'inizio del messaggio e devono essere passate in chiaro .

Come vediamo dalla figura i primi 3 byte indicano il valore di IV, e l'ultimo byte contiene il numero di KeyID (0,1,2,3) .

Figure Adding the IV and KeyID bits



In ultimo viene attaccata, alla fine del pacchetto, l'intestazione MAC ed il valore di CRC per poter riscontrare errori. Un bit indica al ricevitore se il frame è stato criptato con WEP o meno.

Il ricevitore che vede il WEP attivo, saprà tutto IV il numero di chiave, ed inizierà il processo di decriptaggio dei dati è specularmente simmetrico. In ultimo calcolerà l'ICV e verificherà la corrispondenza dei valori.

2.4 - L'algoritmo RC4

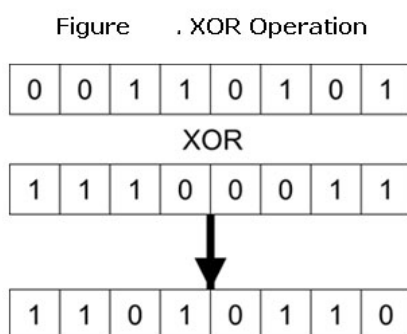
Un algoritmo di criptazione è insieme di operazioni che applicate ad un testo in chiaro permettono di avere come risultato finale un testo cifrato.

RC4 è uno Stream Cipher ideato nel 1987 da Ron Rivest. Tale algoritmo è stato un segreto industriale fino al 1994, anno in cui fu pubblicata in maniera anonima una sua versione su un newsgroup, e da lì fu analizzato.

In RC4, come già accennato, si utilizza lo stesso algoritmo sia per la fase di criptazione che per quella di decriptazione. I punti forza di questo algoritmo sono la sua relativa robustezza ma soprattutto l'essere molto facile da implementare. L'algoritmo è considerato molto forte se usato nel modo giusto, viene utilizzato in molti protocolli quali TLS/SSL (Transport Layer Security / Secure Sockets Layer). In questi ambiti il suo utilizzo è molto robusto e sicuro, oltre che risultare semplice e veloce, purtroppo come vedremo di seguito questo non succede in WEP.

RC4 parte da una **chiave** (lunga da 1 a 256 ottetti), genera una sequenza pseudocasuale (**keystream**) utilizzata per cifrare e decifrare (mediante **XOR**) un flusso dati.

Come vediamo dalla figura lo XOR è un operatore molto semplice che restituisce 0 se i valori sono uguali, negli altri casi 1 .



Solitamente lo XOR dal punto di vista matematico è scritto usando questo simbolo :

⊕

Una caratteristica importante dello XOR risiede nel fatto che se applicato due volte restituisce esattamente il messaggio iniziale.

Questa proprietà può essere sfruttata in RC4 in quanto

Encryption: Plaintext ⊕ Random = Ciphertext

Decryption: Ciphertext ⊕ Random = Plaintext

Il numero pseudorandom è generato da RC4, e deve essere comune ad entrambi gli interlocutori.

Una caratteristica importante dello pseudorandom key stream è che per poter calcolare il prossimo byte nella sequenza bisogna essere a conoscenza della chiave usata per generare lo stream.

Lo XOR è un'operazione facile da implementare per qualsiasi computer, quindi l'unica difficoltà è quella di generare un buon numero pseudocasuale.

In RC4 ci sono 2 fasi :

- KEY setup
- Pseudo-random generation

Nella prima fase si alloca un array(S box) di 256 byte permutazioni di numeri da 0-255, che sono tutti i numeri presenti nell'array ma con ordine sparso.

Inizialmente l'S-box è in ordine. Dopo i numeri vengono scambiati attraverso il seguente processo. Si crea un secondo array K-box, che viene riempito con la chiave, poi ogni byte dell'S-box è scambiato con un altro byte dell'S box stesso.

E' svolta la seguente computazione :

$j = (\text{Value in first byte of S-box}) + (\text{Value in first byte of K-box})$

j is a single byte value and any overflow in the addition is ignored.

Adesso la j è usata con indice dell'array S-box, ed il valore presente in quest'indice è scambiato con il valore della prima locazione.

Questa procedura è ripetuta 255 volte, così ogni byte dell'S-box è scambiato.

Questo processo può essere descritto con il seguente pseudocodice:

$i = j = 0;$

For $i = 0$ to 255 do

$j = (j + S_i + K_i) \bmod 256;$

Swap S_i and $S_j;$

End;

Una volta che l'S-box è stato inizializzato, la prossima fase dell'RC4 è la generazione di un numero pseudocasuale.

Questa fase prevede molti swap di byte nell'S-box, ed alla fine la generazione di un numero pseudo casuale.

$$i = (i + 1) \bmod 256$$

$$j = (j + S_i) \bmod 256$$

Swap S_i and S_j

$$k = (S_i + S_j) \bmod 256$$

$$R = S_k$$

RC4 quindi può trovarsi in $256! \times 256^2$ stati diversi (sono quasi 2^{1700}), questo assicura elevati livelli di sicurezza.

Per generare il testo cifrato ogni byte viene messo in XOR con R.

In linea teorica RC4 non è completamente sicuro perché i numeri non sono veramente random. In ogni caso risulta sufficientemente sicuro per la maggior parte delle applicazioni.

CAP 3 - Perché il WEP non è sicuro ?

IL WEP fu incluso nello standard originale IEEE 802.11 nel 1997, ma solo nel 1999 con lo IEEE 802.11b divenne stabile, quando si iniziarono ad adottare chiavi a 104-bit (128 se si conta l'IV).

Fin dall'inizio furono notate le problematiche della fase di autenticazione, infatti subito dopo venne abbandonata del tutto.

Inizialmente i problemi della sicurezza, non vennero presi neanche in considerazione perché la tecnologia era poco diffusa, e la velocità di trasmissione molto bassa, quindi non se ne vedeva neanche un grande futuro. Nel momento in cui grossi enti (università e pubblica amministrazione) iniziarono ad installare dispositivi wireless, ci si chiese subito se questo tipo di reti fossero a "prova di bomba".

Nei primi mesi del 2000 vennero pubblicati alcuni articoli (Walker, 2000; Arbaugh et al., 2001; Borisov et al., 2001), che dimostrarono come fosse possibile ottenere le chiavi ascoltando il canale, di una rete mediamente occupata, per poche ore indipendentemente dalla lunghezza della chiave.

Questo creò imbarazzo nei produttori dei dispositivi, e fece arrabbiare non poco gli utenti che avevano adattato tale tecnologia.

In generale i meccanismi necessari per la sicurezza sono :

- Authentication
- Access control
- Replay prevention
- Message modification detection
- Message privacy
- Key protection

Sfortunatamente WEP fallisce in tutte queste aree, vediamo perché .

3.1 - Authentication

La fase di autenticazione consiste nel dimostrare agli altri di essere quel che si è dichiarato di essere. Questo processo logicamente porta via del tempo.

Nel mondo wireless, solitamente è necessaria un autenticazione reciproca. La rete vorrà sapere l'identità del client che si sta unendo, ma anche il client si vorrà accertare della validità del network a cui si sta associando.

Gli esperti di sicurezza indicano che è essenziale l'utilizzo di chiavi diverse in fasi di autenticazione e criptaggio dei dati.

Gli aspetti cruciali dell'autenticazione nelle reti wireless sono :

- Metodo robusto per provare l'identità della macchina
- Metodo per preservare l'identità su una sottosequenza di transazioni
- Autenticazione reciproca
- Utilizzo di una chiave indipendente da quella di criptazione.

Sfortunatamente in WEP tutti queste fasi falliscono miseramente.

La fase di autenticazione si basa su un meccanismo di challenge/response che fornisce preziose informazioni per un attaccante.

La chiave usata in questo processo è la stessa di quella usata per la criptazione. Inoltre non vi è un identificazione dell'AP, questo permette di avere un Rogue AP che non può essere rilevato dal client.

Non vi è una riconferma dell'autorizzazione "per un sotto insieme di operazioni", questo fa sì che l'intero processo di autenticazione sia inutile.

Inoltre come già discusso prima, sfruttando le caratteristiche dello XOR ed il fatto che il l'IV è trasmesso in chiaro, un attaccante può sapere il key stream corrispondente ad un dato IV.

A questo punto, effettuerà una richiesta di autenticazione, aspetterà il challenge text, lo metterà in XOR con il key stream precedentemente catturato, e ritornerà il risultato.

L'AP a questo punto svolgerà le sue fasi di decriptaggio, e come per magia i risultati combaceranno. Quindi l'attaccante sarà autenticato alla rete, però non conoscendo ancora la chiave WEP, sarà impossibilitato nella comunicazione.

Per queste ragioni molti sistemi non implementano più la fase di autenticazione in nessun modo.

In 802.11 un vero protocollo di autenticazione non è specificato, inoltre l'adozione di nuovi standard pone problemi di compatibilità verso il basso, infatti la base installata di dispositivi è già molto alta, ragion per cui questa problematica deve essere presa in forte considerazione .

3.2 - Access control

Il controllo di accesso è quel processo che autorizza o nega un device mobile a comunicare con la rete. Molto spesso si confonde la fase di controllo di accesso con quella di autenticazione. Nella fase di autenticazione ci viene chiesto chi siamo, la fase di controllo di accesso non fa questo, perché noi siamo già stati autenticati, dovrebbe invece autorizzare l'accesso.

Lo standard IEEE 802.11 non definisce in che modo questa fase deve essere implementata. In ogni caso l'identificazione di un device è possibile solo attraverso il suo MAC address, quindi da qualche parte dovrà essere presente una lista con gli indirizzi MAC dei device che sono autorizzati ad accedere alla rete.

Solitamente questa lista può essere inserita sull'AP, e funziona persino nel momento in cui non operiamo attraverso WEP.

Come abbiamo già menzionato il numero MAC può essere facilmente modificato, quindi questa soluzione dà solo una falsa sensazione di sicurezza.

3.3 - Replay Prevention

Ci sono molti esempi in cui gli attacchi di replica possono violare la sicurezza della rete, un protocollo di sicurezza dovrebbe consentire una e una sola copia di un messaggio accettato.

Purtroppo questo non accade in WEP, semplicemente perché non è stato considerato affatto!!!

C'è solo una sequenza di numeri nel frame di livello MAC che è incrementata monotonicamente, quindi risulta facile modificare la sequenza di numeri.

3.4 - Message modification detection

WEP è un meccanismo che è stato disegnato per prevenire l'alterazione dei messaggi inviati in rete. L'alterazione dei messaggi può essere usata in modo subdolo.

Come abbiamo visto in WEP si utilizza l'ICV, proprio perché l'utilizzo del CRC diveniva inappropriato in considerazione del fatto che l'intestazione IP del frame era presente in un particolare posizione che non cambiava mai, quindi facilmente ricalcolabile.

L'idea alla base dell'ICV è che essendo criptato, l'attaccante non riesce a svolgere il processo inverso. Il vero problema si pone però nel momento in cui si è a conoscenza della chiave WEP, a quel punto riesce a modificare il messaggio, ricomputare l'ICV e inoltrare il pacchetto criptato.

Inoltre il metodo CRC usato per computare l'ICV è un linear method. Con questo tipo di approccio è possibile prevedere il modo in cui l'ICV cambierà nel momento in cui si cambiano alcuni bit del messaggio.

L'ICV è di soli 32 bits. Supponiamo che il messaggio sia di 8000 bits(1000 bytes), e cambiamo il bit in posizione 5244. Successivamente possiamo calcolare come l'ICV cambia.

Solitamente non vengono cambiati singoli bit ma una sequenza di questa.

C'è da notare che non è necessario conoscere il testo in chiaro, ma solo sapere il modo in cui cambiano i valori in una certa posizione dei dati, paradossalmente si può mantenere l'ICV valido alterando un insieme di bit.

Tutto questo è possibile per le caratteristiche dello XOR precedentemente descritte.

Quindi l'aver voluto criptare il CRC, introducendo l'ICV si è rivelato uno sforzo inutile.

CAP 4 - Debolezze nell'utilizzo di RC4 in WEP

Ci sono 3 punti di debolezza nel modo in cui RC4 è usato in WEP :

- Riutilizzo IV
- Chiavi deboli RC4
- Attacco diretto alla chiave

4.1 - Riutilizzo IV

Un primo punto di debolezza fu scoperto da Jesse Walker dell'Intel . In un suo articolo pubblicato nell'Ottobre del 2000, egli metteva in evidenza alcune lacune del WEP, in particolar modo il riutilizzo dell' IV. L'intento dell'IV è quello di assicurare che due messaggi identici non producono lo stesso testo cifrato.

Se supponiamo per un momento che non ci sia IV, per ogni frame spedito viene inizializzato l'algoritmo RC4 con il key value prima di generare il numero pseudocasuale.

Ma se la chiave rimane fissa, RC4 è inizializzato allo stesso stato in qualsiasi momento. Quindi il key stream produrrà la stessa sequenza di byte per ogni frame.

Con l'aggiunta dell'IV al valore della chiave, RC4 è inizializzato in modo diverso per ogni frame, e così produrrà un key stream differente.

L'unico problema riguarda l'utilizzo di IV, risiede nel fatto che devono essere per forza differenti, ma come vedremo il WEP non fa questo.

Nello standard originale IEEE 802.11 non è specificato il modo in cui devono essere generati gli IV. Intuitivamente verrebbe da pensare che il modo migliore per minimizzare il riutilizzo dell'IV sarebbe quello di generare l'IV in maniera random. Dal punto di vista matematico questo è totalmente sbagliato, cadremmo in quello che viene chiamato come **paradosso del compleanno**.

Il miglior modo per allocare gli IV è quello di incrementare di uno il valore per ogni frame inoltrato. In ogni caso essendo l'IV un numero di 24 bit, avremmo la certezza di una ripetizione dopo meno di 17 milioni di frame (2^{24}) che solitamente vengono trasmessi in sette ore.

In verità la collisione si verifica molto prima, questo perché gli il contatore dell'IV viene azzerato nel momento in cui la scheda è rimossa oppure ogni volta che si verifica una collisione di pacchetti. Quindi avremmo maggiori collisioni per IV bassi.

Se sappiamo in keystream corrispondente ad un dato IV, possiamo immediatamente decodificare qualsiasi sottosequenza di frame che utilizzano lo stesso IV (e la stessa chiave che come visto cambia molto poco di frequente).

Per decodificare ogni messaggio, dovremmo conoscere il keystream di ogni possibile IV.

Come detto gli IV sono quasi 17 milioni, questo potrebbe sembrare un compito scoraggiante, ma se ci pensiamo bene per immagazzinare ogni keystream (1500 byte) servono 23 Gbytes, e attualmente anche i computer più economici possiedono queste capacità di memorizzazione.

Quindi con un tale database possiamo decodificare ogni messaggio senza sapere la chiave segreta.

Supponiamo adesso di avere catturato 2 messaggi con lo stesso IV e stessa chiave.

Sappiamo che il keystream è lo stesso in entrambi i casi

Vediamo come riusciamo a sfruttare le proprietà dello XOR

$$C_1 = P_1 \oplus K_s \quad (\text{Ciphertext msg1} = \text{Plaintext msg1 XORed Keystream})$$

and

$$C_2 = P_2 \oplus K_S \quad (\text{KS è lo stesso in ogni caso})$$

Se si fa lo XOR di C_1 and C_2 , K_S scompare :

$$C_1 \oplus C_2 = (P_1 \oplus K_S) \oplus (P_2 \oplus K_S) = P_1 \oplus P_2 \oplus K_S \oplus K_S = P_1 \oplus P_2$$

Quest'ultima espressione risulta vera perché lo XOR applicato 2 volte torna lo stesso valore originale.

Così adesso un attaccante possiede un messaggio che è lo XOR di 2 messaggi in chiaro.

Ora se un attaccante fosse in grado di conoscere uno dei due Plaintext, sarebbe in grado di ottenere l'altro con un semplice XOR

$$P_1 \oplus (C_1 \oplus C_2) = P_1 \oplus (P_1 \oplus P_2) = P_2$$

Non solo, conoscendo un Plaintext ed il corrispondente Ciphertext, si può ottenere di nuovo con un XOR la Chiave di Cifratura

$$P_1 \oplus C_1 = P_1 \oplus (P_1 \oplus K) = K$$

Alcuni valori del testo in chiaro sono conosciuti, per esempio certi campi di intestazione oppure il valore non è noto ma lo scopo dei campi si .

Quindi su un periodo di tempo abbastanza ampio è possibile avere molte ripetizioni, e poter indovinare una parte sostanziale del keystream.

4.2 - RC4 Weak Keys

La parte fondamentale dell'RC4 non è quella relativa alla criptazione dei dati ma quella relativa alla generazione di una sequenza di numeri casuali.

Come visto RC4 fa sì che vi siano $512 * 256!$ (factorial) possibilità, ed è veramente difficile distinguere una sequenza random da una generata in questo modo.

Vi sono però delle debolezze di RC4 scoperte da Fluhrer, egli ha dimostrato come per alcuni valori di chiave, chiamati weak key, vi sia un numero sproporzionato di bits nei primi pochi bites del keystream (in teoria pseudorandom) che sono determinati da pochi bit nella chiave stessa.

Idealmente se cambio un bit nella chiave, il keystream dovrebbe essere totalmente differente. Ci dovrebbe essere il 50% di possibilità di avere un keystream totalmente differente.

Fluhrer ha dimostrato che non è proprio così, alcuni bit della chiave hanno un grande effetto rispetto ad altri. Alcuni bit addirittura non hanno effetto. Quindi se si riducono il numero di bit effettivi, è più facile attaccare la chiave. Inoltre c'è da dire che i primi byte del testo in chiaro sono solitamente molto facili da indovinare. Per esempio, in WEP l'intestazione LLC parte con il valore esadecimale "AA". Se noi sappiamo il testo in chiaro, possiamo derivare il keystream ed attaccare la chiave.

Con un po' di sforzo ulteriore e l'utilizzo di tecniche di crittoanalisi differenziale, si può risalire alla chiave WEP e così rompere completamente la sicurezza.

Una raccomandazione dell'RSA è quella di scartare i primi 256 byte del keystream, ma questo logicamente in WEP non risulta possibile.

4.3 - Direct Key Attacks

Fluher nelle sue pubblicazioni ha mostrato che l'utilizzo di un IV in chiaro fa sì che siano molte problematiche di sicurezza, inoltre consente ad un attaccante di mettersi in ascolto aspettando una weak key e successivamente attaccare direttamente la chiave.

Si assume che sappiamo i primi byte del testo in chiaro, come per esempio alcuni campi di intestazione che si trovano solitamente nell'IEEE 802.11 LLC SNAP header.

Si ascolta la trasmissione per cercare di identificare la weak key. Sappiamo che c'è correlazione tra testo in chiaro quello criptato e chiave. Quindi ci sono solo alcuni valori che la chiave può assumere affinché testo in chiaro e criptato combaciano.

Dopo la cattura di 60 messaggi simili, l'attaccante può indovinare i primi byte della chiave con assoluta certezza.

Pian piano può essere estratta tutta la chiave. Incrementando la lunghezza della chiave da 40 a 104 bits, si allunga solo di 2 volte e mezzo il tempo di estrazione, in altre parole il tempo per crackare la chiave cresce in maniera proporzionale rispetto la sua lunghezza, piuttosto che in maniera esponenziale.

Attualmente ci sono molti tool che permettono la scoperta della chiave, sono presenti su Internet ormai da un paio di anni ed hanno mandato a monte investimenti di milioni di dollari.

CAP 5 - Regole di base per una corretta configurazione degli apparati di rete

5.1- Configurazione dei dispositivi

Sicuramente una configurazione appropriata e non banale degli apparati di rete permetterà di nascondere dettagli preziosi per i malintenzionati rendendo l'attacco più difficile .

Vediamo in dettaglio cosa si può fare :

Cambiare gli SSID di default .

Il SSID (Service Set Identifier) è un identificatore che consente di distinguere un punto di accesso da un altro (o su scala più vasta da un'organizzazione da un'altra);esso può essere considerato come l'equivalente del nome di dominio per le reti Wireless.

Tramite una configurazione opportuna soltanto i dispositivi che utilizzano un corretto SSID possono comunicare con gli AP. Alcuni AP hanno di default SSID generici facilmente reperibili, riporto qui sotto un elenco dei

SSID	Produttore
tsunami	Cisco
101	3Com
Compaq	Compaq
intel	Intel
linksys	Linksys

Inoltre molte altre marche utilizzano SSID quali “default” o “wireless” .

Come ben capite se pur il campo SSID è trasmesso in chiaro è opportuno cambiare fin dall’inizio il SSID pre impostato dal produttore, cercando di non utilizzare nomi descrittivi della zona di copertura ed utilizzare mix di lettere e numeri .

Disabilitazione Funzioni di Broadcast SSID

Questa operazione logicamente ha senso se viene disabilitato la funzione di Broadcast SSID sull’AP .

Gli Ap normalmente mandano costantemente un Beacon Frame ad intervalli regolari di tempo che permettono la risincronizzazione della macchina Client, i beacon però sono trasmessi in chiaro, possono essere rilevati con i più comuni sniffer e contengono il SSID della rete .

Disabilitando il Broadcast SSID, la macchina client dovrà in ogni caso conoscere il SSID corretto per poter associarsi alla rete, prima dell’associazione nessuna operazione è permessa.

Cambiare le password di default

Così come per il SSID è buona norma cambiare le password di default degli AP, solitamente anche queste sono molto comuni, il che potrebbe avere un forte impatto sulla sicurezza della rete.

Aggiornare il Firmware

Molto spesso, per ragioni puramente economiche, vengono rilasciati apparati di rete che non funzionano perfettamente ed hanno falle incredibili, solitamente la casa produttrice rilascia costantemente firmware nuovi che sarà opportuno aggiornare sui nostri dispositivi

Quindi anche nella loro scelta, è fortemente consigliato acquistare schede che consentano di modificare il firmware.

Chiave WEP

Nonostante tutte le problematiche del WEP, esso risulta comunque un forte deterrente per gli intrusi occasionali. Come abbiamo visto servono grosse quantità di dati ascoltati per cui il malintenzionato deve essere ben motivato ad effettuare l'attacco.

Inoltre cambiare spesso la chiave WEP, anche se è un'operazione che richiede molto tempo, risulta essere un modo per far sì che la rete non si comprometta per un tempo indeterminato.

Abilitare il MAC filtering

Sebbene il controllo degli accessi a livello MAC, non sia stato previsto nella specifica dell'802.11. Quando si utilizza il controllo degli accessi a livello MAC, l'amministratore definisce una lista di indirizzi MAC approvati, cui è consentito connettersi al punto di accesso.

In verità l'indirizzo MAC non costituisce un valido meccanismo di sicurezza, poiché esso è facilmente osservabile e riproducibile..

Inizialmente molti fornitori di schede di rete, permettevano la possibilità di riconfigurare l'indirizzo MAC direttamente dalla proprietà dell'interfaccia. Ultimamente questa funzionalità è stata disattivata, ma sono state create piccole utility quali Bwmachack, che consentono di alterare il MAC semplicemente digitando da DOS

```
C:\> Bwmachack.exe "indirizzo MAC nuovo"
```

Per utilizzare tale utility è consigliabile disabilitare la periferica, eseguire il comando suddetto, re-installare la scheda e digitare infine il comando "ipconfig /all"

In molte distribuzioni di Linux è addirittura possibile modificare il MAC tramite l'utilizzo di vari parametri dell'ifconfig.

In conclusione anche questa tecnica è facilmente raggiungibile, in ogni caso risulta efficiente in presenza di intrusi occasionali e con scarse competenze.

Spegnere l'AP quando non serve

Molto spesso gli intrusi agiscono di notte, se si riesce a spegnere il dispositivo si riducono le possibilità di attacco.

Minimizzare l'intensità del segnale.

Solitamente viene sfruttato il fatto che le onde radio non si possono limitare a luoghi ben definiti. E' pertanto importante scegliere un'adeguata collocazione dell'AP all'interno dell'edificio, in modo tale che il collegamento sia possibile solo ed esclusivamente nella zona interessata, eliminando in particolar modo la presenza del campo lungo la strada adiacente l'edificio, per evitare anche problematiche di tipo legale.

Alcuni AP permettono di modificare l'intensità del segnale via software.

Limitare il traffico di broadcast

Alcuni protocolli, in particolare il NetBIOS su TCP/IP usato da windows, usano assiduamente messaggi di broadcast. Questo fa sì che si incrementi inutilmente il valore dell'RTT, riducendo in questo modo il tempo di una possibile ripetizione.

Non utilizzare DHCP

Non è consigliato utilizzare il server DHCP per l'assegnazione dinamica degli indirizzi, ma attribuire staticamente l'indirizzo IP. E' inoltre consigliato non utilizzare indirizzi di default comuni quali 192.168.0.1 etc etc.

Come per tutte le soluzioni precedenti queste semplici accorgimenti sono facilmente aggirabili.

5.2 - 802.1x . Una possibile soluzione

Le soluzioni precedentemente elencate, quali l'utilizzo di WEP e piccoli accorgimenti pratici, non garantiscono un livello di sicurezza soddisfacente, motivo per cui le reti 802.11 sono state fortemente criticate dai media sin dalla loro nascita.

Per ovviare a questi problemi è stato messo a punto il protocollo 802.1x, questo affronta il problema dell'autenticazione duale, con il WEP si aveva un handshake client-to-server invece che uno schema cliente-server,server-client.

Il sistema 802.1x è un "Port based access control mechanism" ovvero un sistema in grado di autenticare un utente collegato ad una determinata porta ethernet .

EAP è un framework di autenticazione inizialmente pensato per PPP, che permette di negoziare lo schema di autenticazione tra client e server(tipicamente RADIUS) .

L'EAP è molto versatile in quanto non presuppone l'utilizzo di nessun algoritmo predeterminato, la scelta è libera. Sono stati definiti alcuni schemi di identificazione uno di questi è l'EAP-TLS .

Il Transport Layer Security offre un'autenticazione sicura che sostituisce le password con un'autenticazione basata su certificati digitali quali X.509 .In questo paradigma sia il client che il server vengono verificati, evitando frodi relative all'inserimento di falsi Access Point.

Uno dei maggiori svantaggi dell'EAP-TLS è il costo elevato di questa implementazione, infatti devo essere acquistate particolari licenze software e necessità di personale qualificato per la sua gestione.

Attraverso l'EAP, lo standard 802.1x permetta la distribuzione di una o più chiavi WEP al client, risulta così possibile utilizzare chiavi diverse per sessioni diverse.

802.1x risolve alcuni problemi del WEP, quali un'autenticazione sicura ed il cambio di chiave, come visto però il problema di fondo è il WEP che ha crittografia debole, sarà sempre possibile quindi derivare le chiavi anche se adesso occorrerà sicuramente un maggior tempo di ascolto del canale.

Per ovviare a questo problema sarebbe necessaria un ulteriore livello di crittografia attraverso IPSec.

802.1x non affronta per niente gli attacchi derivanti al dirottamento delle sessioni, è sempre possibile per un intruso mandare una richiesta di disassociazione per tutte le macchine del BSS, semplicemente falsificando gli header 802.11 . Sfortunatamente non esiste una soluzione semplice a questo problema, esso non può essere risolto aggiungendo semplicemente un altro schema di autenticazione, né creando un metodo sicuro di schedulazione continua delle chiavi .

L'utilizzo di 802.1x risulta quindi sicuramente il miglior metodo di autenticazione su reti Ethernet in quanto non introduce overhead nei frame, inoltre si integra perfettamente con WEP per la distribuzione automatica delle chiavi attraverso il framework EAPOL-Key.

Per contro il server Radius dovrà supportare EAP, uno schema di autenticazione (TSL), il costo di distribuzione e mantenimento dei certificati. Non tutti i Sistemi Operativi supportano 802.1x nativamente, gli unici sono il WINDOWS 2000 e il WINDOWS XP, gli altri hanno bisogno di un client aggiuntivo con maggiori costi sotto molti punti di vista. Quest'ultimo problema sarebbe marginale se si utilizzasse il PPPoE, che però comporta altri svantaggi .