Mechanizmy bezpieczeństwa sieci 802.11

1 Funkcje warstwy MAC w 802.11

Główne funkcje warstwy MAC to skanowanie, uwierzytelnianie, przyłączanie i transmisja.

Skanowanie

Skanowanie wykorzystywane jest podczas szukania punktu dostępowego przez stację kliencką. Skanowanie może być pasywne i aktywne.

Skanowanie pasywne polega na przeglądanie przez stację kliencką wszystkich kanałów w poszukiwaniu ramek typu *beacon*, rozsyłanych co jakiś czas przez punkt dostępowy. W takiej ramce znajdują się informacje między innymi o identyfikatorach **ESSID** i **BSSID**, kanale pracy, dostępnych szybkościach transmisji, czy sile sygnału.

Skanowanie aktywne polega na wysyłaniu przez stację kliencką ramki rozgłoszeniowej *probe request* na którą odpowiadają wszystkie punkty dostępowe będące w zasięgu ramką *probe response*. Dzięki aktywnemu skanowaniu stacja nie musi czekać na ramkę *beacon*.

Procedura wyboru AP

Klient najczęściej wyszukuje sieć na podstawie identyfikatora **ESSID**, który pełni rolę identyfikatora sieci bezprzewodowej, która może się składać z wielu punktów dostępowych (AP – access point). Każdy z tworzących daną sieć AP rozgłasza w ramkach beacon przynależność do danego ESSID, oraz własny identyfikator BSSID.

Identyfikator **BSSID** identyfikuje z kolei konkretną „komórkę" danej sieci bezprzewodowej, tzn. punkt dostępowy stanowiący część sieci złożonej identyfikowanej przez ESSID.

Klient wyszukuje wszystkie AP rozgłaszające informacje o przynależności do ESSID do którego chce się podłączyć i wybiera ten, którego sygnał jest najsilniejszy. Ponieważ AP rozgłaszają zarówno ESSID jak i BSSID, klient ustala w ten sposób identyfikator BSSID punktu dostępowego do którego zdecydował się podłączyć. W dalszych etapach (uwierzytelnianie, przyłączenie, praca w sieci, odłączenie,…) jako identyfikator sieci do której należy klient, używany jest identyfikator BSSID wybranego AP.

Uwierzytelnianie

Uwierzytelnianie to proces ustalania tożsamości między stacjami. W podstawowym standardzie IEEE 802.11 wyróżniamy dwa rodzaje systemów: system otwarty i system z kluczem dzielonym, który opiera się na szyfrowaniu protokołem WEP. Ogólnie stacja wysyła ramkę *authentication request*, w odpowiedzi na którą AP odpowiada ramką *authentication reply*, zawierającą informacje o przyznaniu, bądź odmowie dostępu.

Przyłączanie

Przyłączanie to proces przyłączenia się stacji klienckiej do AP, potrzebny do synchronizacji obu stron, następujący po poprawnym uwierzytelnieniu. Stacja kliencka inicjuje proces przyłączenia przez wysłanie ramki typu *association request*, w której zawiera informacje na temat obsługiwanych przepływności, czy identyfikatora SSID sieci do której chce się przyłączyć. AP rezerwuje dla danego połączenia obszar w pamięci i przydziela tzw. identyfikator przyłączenia, który jest wysyłany w ramce typu *association response*. Identyfikator przyłączenia jest używany podczas przesyłania danych.

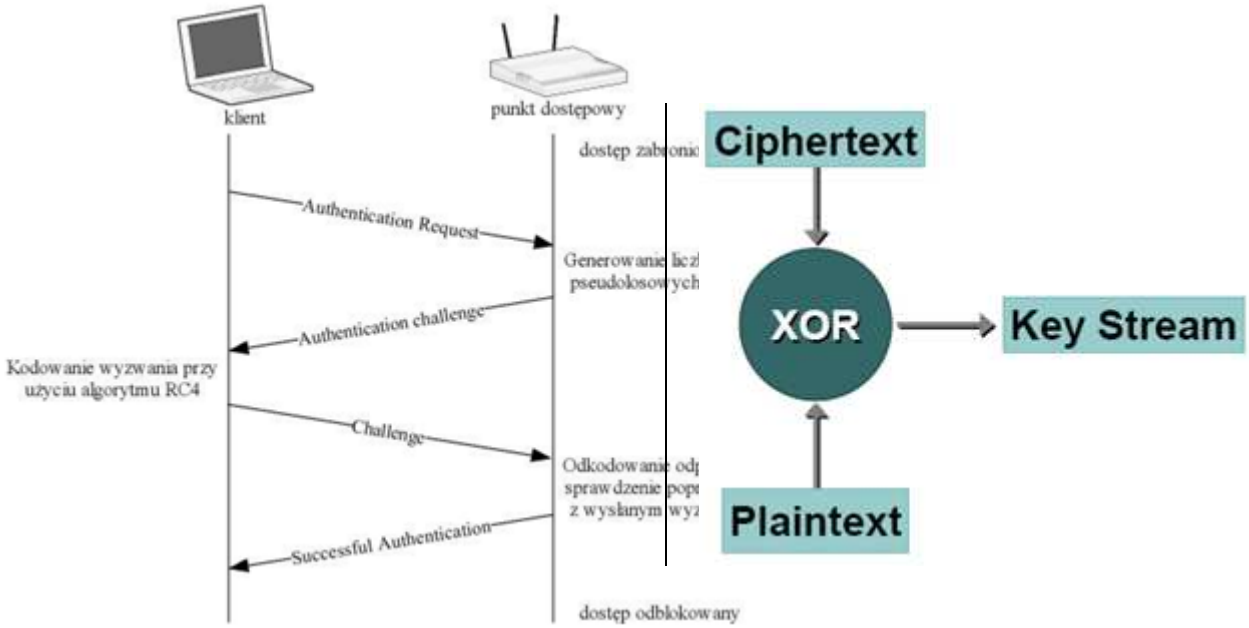
Transmisja

Proces obsługi stacji bezprzewodowych, pozwalający im na wymianę informacji z wykorzystaniem mechanizmów ochrony integralności (CRC-32) i poufności danych (RC-4).

Należy zwrócić uwagę, iż proces uwierzytelnienia i ochrony poufności (szyfrowania) danych to dwa zupełnie różne mechanizmy.
W sieciach WEP mechanizm uwierzytelniania typu shared-key wykorzystuje ten sam klucz tajny (a nawet algorytm) co mechanizm szyfrowania danych, przez co nie oferuje dodatkowego poziomu bezpieczeństwa. Prowadzi natomiast do tragicznego w skutkach zagrożenia bezpieczeństwa, gdyż opiera się na:

- przesłaniu przez AP losowych danych do klienta,
- klient szyfruje te dane swoim kluczem tajnym WEP i odsyła wynik do AP,
- AP wykonuje te same operacje i porównuje wynik z otrzymanym od klienta – jeśli są identyczne oznacza to, że klient użył poprawnego hasła i zostaje uwierzytelniony pozytywnie. Jeśli wyniki się nie zgadzają, to klient nie użył poprawnego hasła i zostaje odrzucony.

Choć w ten sposób samo hasło nie jest przesyłane przez sieć, to przesyłane są te same dane w postaci odszyfrowanej i zaszyfrowanej. Z pomocą prostego przekształcenia XOR, można w ten sposób odczytać ciąg szyfrujący – poprawny również z punktu widzenia mechanizmów ochrony poufności.



Rys. Uwierzytelnianie shared-key i metoda uzyskania ciągu szyfrującego.

W związku z tym, najczęściej rezygnuje się z etapu uwierzytelniania, wprowadzając uwierzytelnianie typu open-system. W jego przypadku na ramkę authentication-request otrzymaną od klienta, AP zawsze odpowiada zgodą na podłączenie. Liczymy tu na fakt, iż bez znajomości klucza WEP, nawet uwierzytelniony klient nie zdoła pracować w naszej sieci, bo:

- nie zdoła odszyfrować danych przesyłanych przez inne stacje,
- nie zdoła wysłać żadnych danych, bo nikt nie zdoła odszyfrować jego transmisji, jeśli nie będzie używał obowiązującego w danej sieci klucza WEP.

2 Tryby promiscous i RF monitoring mode

Interfejs bezprzewodowy może pracować w jednym z trzech trybów:

1. tryb zwykły - w zwykłym trybie pracy interfejs odbiera ramki, których adres docelowy MAC pokrywa się z adresem MAC interfejsu. Pozostałe ramki są odrzucane, a tym samym nie są przekazywane do wyższych warstw w stosie protokołów.
Przykładowy wynik komendy ***ip a*** może wyglądać następująco:

```
wlan0: <BROADCAST,MULTICAST,UP> mtu 576 qdisc pfifo_fast qlen 1000
      link/ether 00:80:c8:1c:6a:51 brd ff:ff:ff:ff:ff:ff
      inet 192.168.0.10/24 brd 192.168.0.255 scope global wlan0
```

2. tryb promiscous - w trybie pracy promiscous interfejs odbiera wszystkie ramki danych, które do niego docierają ***z sieci bezprzewodowej do której jest podłączony***, a więc również te, których adres docelowy MAC nie pokrywa się z adresem MAC interfejsu. Ramki te są następnie przekazywane do wyższych warstw w stosie protokołów. Najczęstszym zastosowaniem tego trybu jest sniffing, czyli podsłuchiwanie ruchu sieciowego w swojej sieci.

Przykładowy wynik komendy ***ip a*** może wyglądać następująco:

```
wlan0: <BROADCAST,MULTICAST,PROMISC,UP> mtu 576 qdisc pfifo_fast qlen 1000
    link/ether 00:80:c8:1c:6a:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.10/24 brd 192.168.0.255 scope global wlan0
```

Wyróżnione pola PROMISC oraz ether wskazują, że karta pracuje w trybie promiscous.

3. tryb RFMON- jest to specjalny tryb „RF monitoring mode" (tryb monitora), występujący jedynie w kartach bezprzewodowych, w którym interfejs potrafi odbierać wszystkie ramki 802.11 będące w powietrzu ***(z dowolnej, słyszalnej sieci bezprzewodowej)***, także ramki kontrolne i sterujące. Nie wszystkie drivery potrafią obsłużyć opisywany tryb. W czasie pracy w trybie RFMON interfejs nie jest podłączony do żadnej sieci bezprzewodowej.
W przypadku trybu zwykłego i promiscous, kanał może być ustawiany automatycznie, zgodnie z informacjami rozgłaszanymi przez punkt dostępowy lub klientów już należących do określonej sieci ad-hoc (patrz 1 - skanowanie). Wystarczy podać tylko identyfikator sieci (SSID) która nas interesuje.
W przypadku pracy w trybie monitora, konieczne jest odpowiednie (ręczne) ustawienie kanału pracy karty, gdyż nie jesteśmy podłączeni do żadnej sieci. Stąd wszystkie parametry należy ustawiać ręcznie.

Przykładowy wynik komendy ***ip a*** może wyglądać następująco:

```
wlan0: <BROADCAST,MULTICAST,PROMISC,UP> mtu 576 qdisc pfifo_fast qlen 1000
    link/[802] 00:80:c8:1c:6a:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.10/24 brd 192.168.0.255 scope global wlan0
```

Wyróżnione fragmenty są charakterystyczne dla interfejsu działającego w trybie RF monitoring mode.

3 Narzędzia wykorzystywane w czasie laboratorium

3.1 Obsługa sterowników karty bezprzewodowej – Ath5k (Lab 142)

Sterowniki Ath5k w systemie Fedora udostępniają pojedynczy interfejs sieciowy dla każdej zainstalowanej karty bezprzewodowej. Nazwa interfejsu określana jest na podstawie sposobu jego typu oraz sposobu podłączenia do komputera. Interfejsy bezprzewodowe posiadają nazwy rozpoczynające się od liter „**wl**" (Wireless LAN).

Interfejsy bezprzewodowe konfigurujemy przy użyciu, opisanego poniżej, polecenia ***iwconfig***.

3.2 Włączanie i wyłączanie interfejsu

Interfejsy sieciowe włączamy za pomocą polecenia:
ip link set <*interfejs*> up
a wyłączamy za pomocą polecenia:
ip link set <*interfejs*> down

W wielu wypadkach wyłączenie i ponowne włączenie interfejsu pozwala na przywrócenie go do poprawnego działania w przypadku niestabilnego zachowania (np. braku reakcji na wprowadzone zmiany konfiguracji nakazujące mu na połączenie się z określoną siecią bezprzewodową).

3.3 Polecenie: iwconfig

Polecenie służy do konfiguracji karty bezprzewodowej.
iwconfig – podaje listę interfejsów oraz ich parametrów konfiguracyjnych dotyczących sieci bezprzewodowej.
Polecenie to pozwala sprawdzić czy podłączyliśmy się do właściwego AP. Wyświetla, w drugiej linii, informację „**Access point: <adres MAC>**”. Gdzie **adres MAC** zawiera same zera (lub opis: ***Not-Associated***) jeśli nie jesteśmy podłączeni, lub identyfikator **BSSID** sieci bezprzewodowej do którego się podłączyliśmy (równy najczęściej adresowi MAC punktu dostępowego – patrz 1).

iwconfig <interfejs> [essid <nazwa_sieci_bezprzewodowej>] [key <klucz_wep_hexalnie>] [channel <nr_kanału>] [mode managed|monitor|ad-hoc]
Opcjonalny parametr ***essid*** nakazuje podanemu interfejsowi podłączyć się do sieci bezprzewodowej o podanej nazwie (duże i małe litery są rozróżniane).
Jeśli sieć wymaga podania klucza WEP, używamy do tego opcjonalnego parametru ***key***, po którym podajemy klucz WEP w formie ciągu znaków w kodzie szesnastkowym. Jeśli chcemy użyć klucza WEP w formie ciągu ASCII to należy poprzedzić go prefiksem ***s:***, np. ***key s:haslo***.
Jeśli konieczne jest określenie kanału pracy to można użyć opcjonalnego parametru ***channel*** i podać po nim numer kanału (lub wartość ***auto***, w celu włączenia automatycznego wyszukiwania sieci o podanej nazwie). Ręczne ustalenie kanału pracy konieczne jest w trybie RFMON i zalecane w sieciach ad-hoc, w sieciach z punktem dostępowym wystarczy podać essid, resztę danych karta ustali automatycznie na podstawie informacji rozgłaszanych przez AP.
Parametr ***mode*** określa tryb pracy interfejsu bezprzewodowego i może przyjąć (między innymi) wartości:

- ***managed*** – tryb pozwalający na podłączenie się do sieci bezprzewodowej wykorzystującej punkt dostępowy i transmisję danych,
- ***monitor*** – tryb RFMON. W tym trybie nie należy ustawiać wartości żadnych z wymienionych powyżej parametrów, poza kanałem (channel). Ponieważ w tym trybie nie podłączamy się do żadnej sieci, należy pamiętać o ręcznym określeniu kanału, na którym ma pracować karta bezprzewodowa.
- ***ad-hoc*** – tryb pozwalający na pracę w sieci złożonej wyłącznie ze stacji roboczych (bez punktu dostępowego).

UWAGA: W razie wystąpienia problemów z wykonywaniem powyższych komend, objawiających się np. komunikatami o błędach w rodzaju „*SET failed on device wlp9s1 ; Device or resource busy.*” należy:

- posłużyć się poleceniami zawierającymi tylko jedną opcję konfiguracyjną, czyli np. zamiast polecenia „**iwconfig wlp9s1 essid ‘test’ key 1234567890**” użyć 2 osobnych poleceń: „**iwconfig wlp9s1 essid ‘test’**” oraz „**iwconfig wlp9s1 key 1234567890**”.

- spróbować wykonać dane polecenie zmieniwszy stan interfejsu bezprzewodowego, tzn. jeśli nie działa ono przy wyłączonym interfejsie, to należy spróbować wykonać je przy włączonym (i odwrotnie).

3.4 Zmiana adresu MAC karty

Znane polecenie **ip** może posłużyć również do zmiany adresu MAC interfejsu sieciowego.
Składnia:
ip link set <*interfejs*> down
ip link set <*interfejs*> address <*Adres MAC*>
ip link set <*interfejs*> up

Jak widać, zmiany adresu MAC należy dokonywać przy wyłączonym interfejsie.

3.5 Wireshark (opisany dodatkowo w innych materiałach)

Wireshark jest najpopularniejszym narzędziem do przechwytywania ramek w sieci i do ich późniejszej analizy. Obsługuje formaty bardzo dużej liczby protokołów. Pracuje w środowisku graficznym i jest bardzo przyjazny dla użytkownika. Współpracuje z plikami zapisywanymi przez inne programy np. Kismet.

Informacje podstawowe:

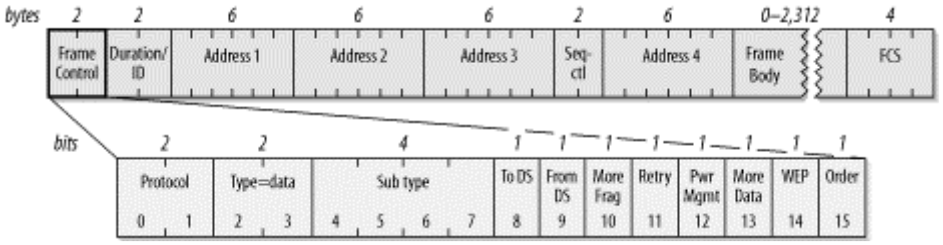
- Aby interfejs bezprzewodowy widoczny był dla programu Wireshark, musi on być podniesiony (UP).
- Aby wykorzystać ten program do obserwacji w trybie RFMON, należy najpierw przełączyć interfejs w ten tryb i ustawić właściwy kanał, a dopiero potem uruchomić program Wireshark.

Przydatne funkcje:

- „**Follow TCP stream**" dostępna w menu kontekstowym dowolnego przechwyconego pakietu TCP – pozwala ona na zrekonstruowanie treści całego dialogu w danym połączeniu TCP między dwoma stacjami.
- „**Mark packet**" dostępna w menu kontekstowym dowolnego przechwyconego pakietu – pozwala na zaznaczenia danego pakietu. Zaznaczone pakiety można następnie np. zapisać do innego pliku (File->SaveAs Marked packets).
- **Filtry** – można stosować je zarówno do ograniczania ilości zbieranych danych (capture filter), jak i wyświetlania danych już zebranych (display filters).

Poniżej zamieszczono tabelę podającą wartości pól type i subtype pola Frame Control ramki sieci 802.11. Wartości te będą niezbędne w realizacji zadań, do wyfiltrowania zbędnego ruchu i prezentacji wyników. Interesujące nas wartości zaznaczono na żółto.
Filtr wireshark'a pokazujący tylko ramki określonego typu/podtypu ma postać:
wlan.fc.type_subtype == 0x20 (ramki danych)
Filtr wireshark'a pokazujący wszystkie ramki za wyjątkiem określonego typu/podtypu ma postać:
!(wlan.fc.type_subtype == 0x20) (wszystko poza danymi)

Filtry można łączyć (wielokrotnie) słowami kluczowymi **and** (ramka pokazana gdy oba warunki spełnione) lub **or** (ramka pokazana gdy dowolny z warunków spełniony):
!(wlan.fc.type_subtype == 0x20) and !(wlan.fc.type_subtype == 0x08) and !(wlan.fc.type_subtype == 0x1d)
(wszystko poza danymi, beaconami i ACK)



Rys. Struktura ramki 802.11 z wyróżnionym polem Frame Control.

Subtype	Description
Management frames (type=00)	
0000	Association request (0x00)
0001	Association response (0x01)
0010	Reassociation request
0011	Reassociation response
0100	Probe request (0x04)
0101	Probe response (0x05)
1000	Beacon (hex 08)
1001	Announcement traffic indication message (ATIM)
1010	Disassociation (0x0a)
1011	Authentication (0x0b)
1100	Deauthentication (0x0c)
Control frames (type=01)	
1010	Power Save (PS)-Poll
1011	RTS
1100	CTS
1101	Acknowledgment (ACK) (0x1d)
1110	Contention-Free (CF)-End
1111	CF-End+CF-Ack
Data frames (type=10)	
0000	Data (0x20)
0001	Data+CF-Ack
0010	Data+CF-Poll
0011	Data+CF-Ack+CF-Poll
0100	Null data (no data transmitted) (0x24)
0101	CF-Ack (no data transmitted)
0110	CF-Poll (no data transmitted)
0111	Data+CF-Ack+CF-Poll

Czyli np.: Beacon to wartość 001000 = 0x08; Data+CF-ACK: 100001 = 0x21.

Tabela. Wartości type/subtype pola Frame Control ramki 802.11.

3.6 ping

Polecenie ping sprawdza poprawność łączności sieciowej IP, poprzez wysłanie komunikatu ICMP echo request pod podany adres i oczekiwanie na zwrotny komunikat ICMP echo reply.

ping ***[opcje]*** **<*adres*>**

Przydatne opcje:

-s <wielkość> pozwala określić wielkość pola danych wysyłanych pakietów (w bajtach),

-f powoduje wysyłanie komunikatów tak szybko jak to możliwe oraz przedstawia graficznie liczbę pozostałych bez odpowiedzi – dla każdego wysłanego żądania wypisywany jest znak „.”, a otrzymanie każdej odpowiedzi powoduje usunięcie jednego znaku „.”.
Jest to doby sposób na generację ruchu sieciowego dla potrzeb ćwiczenia – nie wymaga żadnych serwerów (np.: WWW, FTP) i generuje dużo małych ramek (a o to nam chodzi).

-I <*interfejs*> wysłanie pakietów z użyciem podanego interfejsu.

3.7 scp

Umożliwia szyfrowaną transmisję plików pomiędzy komputerami.

scp <*źródło*> <*cel*>

gdzie <*źródło*> i <*cel*> mogą przyjąć postać: <*username*>@<*adres*>:<*plik*>
czyli np:

```
scp root@komp1:/root/kismet/test.dump /root/pliki/
```

3.8 aircrack-ng

Umożliwia analizę zebranego ruchu sieciowego i w efekcie odtworzenie używanego w sieci bezprzewodowej klucza WEP lub klucza uwierzytelniającego WPA-PSK, dzięki połączeniu metod statystycznych i brute-force.

W przypadku protokołu WEP, wykorzystuje się analizę statystyczną zebranych wcześniej innym programem ramek danych sieci 802.11 (lub samych pól IV nagłówka ramki), w celu określenia zbioru najbardziej prawdopodobnych kluczy szyfrujących. Następnie zbiór ten jest przeszukiwany w celu odnalezienia konkretnego klucza.

W przypadku WPA-PSK przeprowadzany jest atak słownikowy (i ewentualnie brute-force) optymalizowany na podstawie zarejestrowanych wcześniej prób uwierzytelnienia legalnych użytkowników. Analiza ramek danych nie jest tu użyteczna i o łatwości odszukania klucza decyduje ilość przechwyconych, udanych prób uwierzytelnienia.

Składnia:

dla WEP:
aircrack-ng -a 1 *[opcje]* <*plik_z_ramkami_lub_wektorami_IV*>

dla WPA:
aircrack-ng -a 2 -e <*nazwa sieci*> -w <*plik_z_hasłami*> <*plik_z_ramkami*>
lub
<*polecenie_generujące_listę_haseł*> | aircrack-ng -a 2 -e <*nazwa sieci*> -w - <*plik_z_ramkami*>

Opcje:

-a <typ zabezpieczenia> 1-WEP, 2-WPA-PSK

-n <bity> Dla WEP: umożliwia podanie długości szukanego klucza (w razie właściwego ustawienia znacznie przyśpiesza obliczenia)

-z Dla WEP: umożliwia zastosowanie dodatkowych algorytmów przydatnych tylko w przypadku analizy ruchu wygenerowanego w

	wyniku ataku aktywnego z użyciem protokołu ARP.
-K	Dla WEP: powoduje rezygnację z wykorzystania w analizie części algorytmów. Wspomniane algorytmy skutkują znaczącym przyspieszeniem poszukiwań, lecz w określonych przypadkach mogą skutkować niemożnością odnalezienia klucza.
-e <ESSID>	Dla WPA: pozwala na określenie nazwy sieci, którą analizujemy
-w <nazwa_pliku>	Dla WPA: pozwala na określenie nazwy pliku z którego pobierane są hasła do weryfikacji (plik słownika) Jeśli podamy zamiast nazwy pliku znak myślnika (-) to można posłużyć się poleceniem generującym listę haseł, bez zapisywania jej do pliku – patrz alternatywna wersja składni polecenia powyżej oraz sekcja 3.11.

Dla WEP:

```
                                 Aircrack 2.4

                          [00:03:06] Tested 674449 keys (got 96610 IVs)

 KB    depth   byte(vote)
  0    0/  9   12(  15) F9(  15) 47(  12) F7(  12) FE(  12) 1B(   5) 77(   5) A5(   3) F6(   3) 03(   0)
  1    0/  8   34(  61) E8(  27) E0(  24) 06(  18) 3B(  16) 4E(  15) E1(  15) 2D(  13) 89(  12) E4(  12)
  2    0/  2   56(  87) A6(  63) 15(  17) 02(  15) 6B(  15) E0(  15) AB(  13) 0E(  10) 17(  10) 27(  10)
  3    1/  5   78(  43) 1A(  20) 9B(  20) 4B(  17) 4A(  16) 2B(  15) 4D(  15) 58(  15) 6A(  15) 7C(  15)

                                 KEY FOUND! [ 12:34:56:78:90 ]
```

Tested X keys – aktualnie sprawdzono X kluczy.
(got X IVs) – do analizy wykorzystano X wektorów inicjalizacyjnych.
KB – numer kolejny bajtu klucza (Key Byte)
depth X/Y – **Y:** liczba możliwych wartości danego bajtu klucza ustalona po wstępnej analizie danych; **X:** numer aktualnie sprawdzanej wartości bajtu klucza z Y możliwych.
Obecność wartości Y większych od 15 oznacza małe szanse na szybkie odnalezienie klucza.
byte(vote) – **byte:** proponowana przez program wartość danego bajtu klucza; **(vote):** oszacowana waga prawdopodobieństwa danej propozycji.
Propozycje wartości kolejnych bajtów poszukiwanego klucza przedstawiane są w kolejnych liniach. W każdej z linii, propozycje programu posortowane są od najbardziej do najmniej prawdopodobnych wg przeprowadzonej analizy.

Dla WPA:

```
                          Aircrack-ng 1.1


                [00:00:22] 134564 keys tested (7015.70 k/s)


                       KEY FOUND! [ 12345678 ]


      Master Key     : AE DD 76 03 2D 25 BC 23 E5 B8 E3 66 6F 38 A1 BB
                       F4 49 BC 45 71 0B 73 22 0F AF C4 7D CD 81 E7 5F

      Transient Key  : 5E E0 1D EA 28 89 C9 F8 4D 3C B7 62 62 FA 2A F4
                       B7 10 B4 C9 D3 96 55 6B 69 1E D3 6C 2E DF 52 B5
                       80 EF 0B 4A 24 8B FB 12 EC FB 4A D5 A1 41 C6 2F
                       9B 38 6A E9 92 E0 C9 E2 63 CE B0 C4 C5 D9 90 3C

      EAPOL HMAC     : 07 4A 05 D7 5F 30 B4 4B FE 19 75 1C 56 7F 78 26
```

Informacje podawane w przypadku WPA są mniej przydatne w procesie śledzenia postępów obliczeń. Podawane są klucze typu Master i Transient, które są aktualnie weryfikowane, aktualnie weryfikowane hasło („Current passphrase:") w którego miejscu pojawia się ewentualna informacja o znalezieniu hasła („KEY FOUND! […]"), oraz czas obliczeń, liczba sprawdzonych kluczy („X keys tested") oraz szybkość obliczeń w kluczach na sekundę („X k/s").

3.9 airdecap-ng

Służy do odszyfrowania ruchu sieciowego, zapisanego wcześniej w postaci pliku w formacie pcap (obsługują go np. Kismet i WireShark).

Składnia:
airdecap-ng *[opcje]* <*plik_pcap*>

Przydatne opcje:

-b <MAC AP>	przetwarzaj tylko ruch z danego AP
-e <essid>	przetwarzaj tylko ruch z sieci bezp. o podanym ESSID.
-w <klucz WEP hex>	używaj podanego klucza WEP (w postaci heksadecymalnej)
-p <hasło WPA>	użyj podanego hasła WPA
-l	nie usuwaj nagłówka 802.11 z rozszyfrowanych danych.

3.10 airodump-ng

Polecenie pozwala na przeszukiwanie pasma radiowego w poszukiwaniu aktywnych punktów dostępowych oraz klientów. Umożliwia także zapisywanie słyszanego ruchu do pliku w formacie pcap (obsługują go np. Kismet i WireShark) i ivs (zawiera wyłącznie nagłówki ramek – możliwy do zastosowania w niektórych atakach pasywnych z użyciem aircrack-ng).

Składnia:
airodump-ng *[opcje]* <*interfejs*>
<interfejs> - interfejs bezprzewodowy który wykorzystujemy, powinien pracować w trybie monitora (RFMON). Jeśli zamierzamy zgrywać ruch do pliku powinniśmy użyć opcji *--channel*, a sam interfejs powinien zostać wcześniej (przed uruchomieniem programu airodump-ng) ustawiony na ten sam kanał, co podany w opcji *--channel*.
<opcje>:
--channel <*nr_kanału*> - słuchaj na kanale o podanym numerze. Bez tego parametru program będzie przeskakiwał po wszystkich kanałach.
-w <*nazwa_pliku*> - zapisuj dane do pliku. Utworzony plik będzie miał nazwę: *<nazwa_pliku>-<nr_kolejny>.cap* – na przykład: *plik-01.cap*. Domyślnym formatem zapisu jest pcap.
--ivs – zapisuj plik w formacie IVS (tylko nagłówki ramek). Plik będzie miał rozszerzenie *ivs* zamiast *cap*.

3.11 Crunch

Polecenie pozwala na wygenerowanie listy haseł wg zadanego wzorca. Lista ta może zostać wykorzystana jako element ataku typu brute-force, w którym zawarte na niej hasła są kolejno weryfikowane, w celu sprawdzenia czy któreś z nich nie odpowiada poszukiwanemu hasłu wykorzystywanemu przez użytkownika (patrz sekcja 3.8).

Składnia:
crunch <*min*> <*maks*> *[<lista_znaków>] [opcje]*
<*min*> - WYMAGANY - minimalna długość generowanego hasła
<*maks*> - WYMAGANY - maksymalna długość generowanego hasła
<*lista_znaków*> - OPCJONALNY – lista znaków z których generowane są hasła. Należy podawać znaki w grupach oddzielanych spacjami: małe litery, duże litery, cyfry, inne znaki. Jeśli któraś z grup

jest pusta, należy zastąpić ją znakiem „**+**”. Jeśli pusta grupa jest na końcu listy, można ją całkiem pominąć. Np.: **aer + 4678** (małe litery: aer, brak dużych liter, cyfry: 4678, brak innych znaków).

<opcje>:
-t <*wzorzec*> - definiuje wzorzec wg którego tworzone są hasła. We wzorcu wykorzystujemy znaki specjalne:

- **@** - mała litera
- **,** - duża litera
- **%** - cyfra
- ^ - inne.

Np. wzorzec „**,abc%**” wygeneruje hasła zaczynające się od dużej litery, po której następuje ciąg „abc”, a na końcu pojedyncza cyfra.
Jeśli podajemy wzorzec, to wartości <min> i <maks> muszą być równe jego długości – czyli w przypadku przykładu powyżej, będą wynosiły 5.

Przykład:
crunch 6 6 abc XYZ 469 + -t H%a@,
Powyższe polecenie wygeneruje 5 literowe hasła, w których pierwszą literą jest „H“, po niej następuje jedna z cyfr „4”, „6” lub „9”, następnie litera „a“, po niej jedna z liter „a”, „b” lub „c”, a na końcu jedna z liter „X”, „Y” lub „Z”.

crunch 1 4 1234567890 + + +
Powyższe polecenie wygeneruje hasła o długości od 1 do 4 znaków, złożone z samych cyfr.

---

4 Ataki aktywne: aireplay-ng

Jest to narzędzie pozwalające na realizację ataków aktywnych. Mogą one mieć na celu, np.: sztuczne wygenerowanie ruchu do późniejszej pasywnej analizy, przeprowadzenie ataków denial of service lub odkrycie nieaktywnych sieci bezprzewodowych z wyłączonym rozgłaszaniem SSID.

UWAGA: W przypadku ataków aktywnych, gdzie transmitując dane podszywamy się pod inny adres MAC, zalecana jest wcześniejsza, ręczna zmiana adresu MAC naszej karty bezprzewodowej na ten obcy adres (patrz 3.4). Jeśli tego nie zrobimy, program wyświetli komunikat z ostrzeżeniem, a sam atak może się powieść lub nie – w zależności od właściwości sterowników naszej karty bezprzewodowej.

Składnia:
aireplay-ng <opcje> <interfejs>
<interfejs> - interfejs bezprzewodowy który wykorzystujemy, powinien pracować w trybie monitora (RFMON).
<opcje> można podzielić na kilka grup:

- opcje rodzaju ataku – pozwalające na wybór ogólnego trybu działania programu,
- opcje ogólne – modyfikujące działanie programu i możliwe do zastosowania w większości lub wszystkich trybach pracy,
- opcje właściwe dla danego trybu pracy.

Poniżej opiszemy tylko niektóre z nich, konieczne do realizacje zadań laboratoryjnych.

Opcje wyboru funkcji – należy wybrać jedną z nich. Od tego wyboru zależą dalsze opcje, opisane w kolejnych podrozdziałach.

-0 <num> – odłączenie użytkowników od sieci <num> razy (0 – bez końca). [deauth]
-1 <czas> – fałszywe uwierzytelnianie się w sieci co <czas> sekund. [fakeauth]
-2 – interaktywny wybór generowanego ruchu. [interactive]
-3 – generowanie ruchu ARP. [arpreplay]
-4 – bezpośrednie odszyfrowanie ramki danych WEP. [chopchop]
-5 – ustalenie ciągu szyfrującego. [fragment]
-9 – test generacji ruchu.

Opcje ogólne (poprawne przy różnych rodzajach ataków):
-x <pps> – OPCJONALNA – ustawienie szybkości generowania ruchu na <pps> ramek/s. Odpowiedni dobór tego parametru pozwala przyśpieszyć generację ruchu. Czasem ZMNIEJSZENIE tej wartości przyspiesza działanie – jest to zależne od możliwości sterownika i urządzeń bezprzewodowych. Zbyt duża szybkość transmisji może spowodować zawieszenie niektórych punktów dostępowych, pozwalając w efekcie na przeprowadzenie ataku typu DoS.
-r <plik> – OPCJONALNA – pobieranie ramek do analizy z pliku, zamiast z interfejsu bezprzewodowego. Może służyć do analizy wcześniej przechwyconego ruchu (np. odszyfrowania zapisanych ramek).

4.1 Odłączanie użytkowników od sieci (Deauthentication)

Powoduje wysłanie żądania odłączenia się od sieci do wszystkich lub wybranych klientów. Przydatne w przypadku:

- ataku DoS,
- wykrywania i ustalania SSID sieci, które go nie rozgłaszają i w których aktualnie nie ma żadnego ruchu, który pozwoliłby łatwo je wykryć,
- wymuszania ponownego uwierzytelniania się do sieci, co ma kluczowe znaczenie w przypadku ataku na WPA-PSK,
- wymuszania generowania żądań ARP (przydatne w ataku ARPREPLAY) – klienci pracujący pod Windows kasują zapamiętane tablice ARP po odłączeniu od sieci.

Opcje:
-0 - WYMAGANA - wybór funkcji ***deauthentication***,
-a <MAC> - WYMAGANA – adres MAC punktu dostępowego.
-c <MAC> - OPCJONALNA – adres MAC klienta do odłączenia. W przypadku jej braku żądanie zostanie wysłane na adres broadcast (do wszystkich klientów).

Przykład:
aireplay-ng -0 5 –a 00:47:05:34:65:43 –c 00:11:22:33:44:55
Co 5 s. nakazuje odłączenie klienta o adresie MAC 00:11:22:33:44:55 od AP o adresie MAC 00:47:05:34:65:43.

4.2 Fałszywe uwierzytelnianie się w sieci (Fake authentication)

Możliwe tylko w sieciach WEP (niemożliwe w przypadku WPA/WPA2). Pozwala na zasocjowanie się i uwierzytelnienie korzystając z jednego z 2 mechanizmów WEP: open-system lub shared-key.
Przydatne jako punkt wyjściowy do innych ataków aktywnych, gdyż wymagają one obecności choć jednego klienta bezprzewodowego zasocjowanego z danym punktem dostępowym.
Powodem jest fakt, iż punkt dostępowy nie będzie retransmitował ramek pochodzących od klientów, którzy nie są zasocjowani, a zmuszenie go do takiej retransmisji (i tym samym użycia nowych wartości wektora inicjalizacyjnego IV) jest celem większości tych ataków.

Jeśli w sieci są zasocjowani klienci, to możemy przeprowadzić atak aktywny wykorzystując ich adresy MAC jako źródło naszego ruchu. Natomiast jeśli chwilowo w sieci takich klientów brak, można sztucznie uwierzytelnić wybrany adres MAC z punktem dostępowym (fake authentication) i używać go następnie do przeprowadzenia ataku.

Opcje:
-1 <czas> - WYMAGANA - wybór funkcji ***fake authentication***, jest ona powtarzana co ***<czas>*** podany w sekundach,
-e <SSID> – WYMAGANA – nazwa (SSID) sieci bezprzewodowej do której się łączymy,
-a <MAC> – WYMAGANA – adres MAC punktu dostępowego z którym się asocjujemy,
-h <MAC> – WYMAGANA – adres MAC klienta, za którego się podajemy (najlepiej zmienić też adres MAC naszej karty sieciowej na ten adres),
-y <plik> - wymagana tylko przy uwierzytelnianiu shared-key – nazwa pliku zawierającego bity ciągu szyfrującego (patrz atak 4.6).

Przykład:
aireplay-ng -1 120 –e test –a 00:11:43:65:34:76 –h 00:14:6C:7E:40:80 –y plik.xor ath0
Powoduje powtarzanie co 2 minuty procesu uwierzytelnienia stacji o adresie 00:14:6C:7E:40:80, do sieci o ESSID „test" obsługiwanej przez AP o adresie 00:11:43:65:34:76, z użyciem uwierzytelniania shared-key i ciągu szyfrującego podanego w pliku plik.xor.

4.3 Interaktywny wybór generowanego ruchu (Interactive packet selection)

Jak już wspomniano, celem większości ataków aktywnych jest zmuszenie AP do retransmisji wysyłanego do niego przez atakującego ruchu, która to retransmisja odbywa się z użyciem nowych wektorów inicjalizacyjnych (IV). W ten sposób otrzymujemy duży zbiór ramek zaszyfrowanych znanymi IV co pozwala na przeprowadzenie pasywnej analizy i np. odczytanie klucza szyfrującego.
Aby AP retransmitował daną ramkę, musi być spełnione kilka warunków:

- docelowy adres MAC musi znajdować się w sieci bezprzewodowej i być zasocjowany, lub ramka musi być zaadresowana na adres BROADCAST (FF:FF:FF:FF:FF:FF),
- Flaga „ToDS" w nagłówku (oznaczająca ramkę która powinna być retransmitowana przez AP) musi być ustawiona na 1.

Możemy zastosować 2 podejścia:

- **Natural packet replay:** znaleźć ramkę, która spełnia powyższe warunki i po prostu wysyłać ją do AP,
- **Modified packet replay:** znaleźć ramkę, która spełnia tylko cześć warunków, zmodyfikować ją odpowiednio i dopiero następnie wysyłać do AP.

Natural packet replay
Aby znaleźć ramkę odpowiednią do wysyłania bez żadnych modyfikacji, stosujemy następujące opcje filtrujące:
-2 - WYMAGANA - wybór funkcji ***IPS***,
-b <MAC> - adres MAC AP którym jesteśmy zainteresowani,
-d <MAC> - adres docelowy w ramkach, najlepiej adres broadcast: FF:FF:FF:FF:FF:FF,
-t 1 – ustawiona flaga ToDS.

Przykład:
aireplay-ng -2 –b 00:11:43:65:34:76 –d FF:FF:FF:FF:FF:FF –t 1 ath0

Modified packet replay
Stosujemy tu mniej restrykcyjne filtry:
-2 - WYMAGANA - wybór funkcji ***IPS***,
-b <MAC> - adres MAC AP którym jesteśmy zainteresowani,
-t 1 – ustawiona flaga ToDS.

A następnie dodajemy opcje modyfikujące:
-p 0841 – ustawiamy wartość pola FCF (Frame Control Field) na mówiąca, że jest to ramka od klienta bezprzewodowego do AP,
-c FF:FF:FF:FF:FF:FF – ustawiamy adres docelowy ramki na adres broadcast, aby wymusić na AP retransmisję.

Przykład:
aireplay-ng -2 –b 00:14:6C:7E:40:80 –t 1 –p 0841 –c FF:FF:FF:FF:FF:FF ath0

Po wydaniu tych poleceń, nasz komputer zacznie szukać w eterze ramki odpowiadającej naszym kryteriom i, gdy ją znajdzie, przedstawi ją nam do akceptacji.

```
Read 4 packets...

      Size: 68, FromDS: 0, ToDS: 1 (WEP)

           BSSID  =  00:14:6C:7E:40:80
       Dest. MAC  =  FF:FF:FF:FF:FF:FF
      Source MAC  =  00:0F:B5:34:30:30

      0x0000:  0841 de00 0014 6c7e 4080 000f b534 3030  .A....l~@....400
      0x0010:  ffff ffff ffff 4045 d16a c800 6f4f ddef  ......@E.j..oO..
      0x0020:  b488 ad7c 9f2a 64f6 ab04 d363 0efe 4162  ...|.*d....c..Ab
      0x0030:  8ad9 2f74 16bb abcf 232e 97ee 5e45 754d  ../t....#...^EuM
      0x0040:  23e0 883e                                #..>

Use this packet? y
```

Jeśli potwierdzimy, zmodyfikuje ją (stosowanie do opcji modyfikujących które podaliśmy) i zacznie wysyłać do AP, który powinien zacząć ją retransmitować z użyciem nowych IV. Jeśli zaprzeczymy, zacznie szukać dalej.
Warto wybierać jak najmniejsze ramki (Size), gdyż można ich wysłać więcej w krótszym czasie, a o łatwości analizy pasywnej decyduje liczba zgromadzonych ramek, a nie ich objętość.

Ten tryb pracy może znaleźć zastosowanie w wielu atakach o zróżnicowanych celach (nie tylko w celu generacji ruchu do analizy), gdyż umożliwia wysyłanie poprawnych ramek o zmodyfikowanych parametrach do zabezpieczonej sieci.

4.4 Generowanie ruchu ARP (ARP Request Replay Attack)
Ma na celu wygenerowanie ruchu w zabezpieczonej sieci, który następnie możemy poddać analizie. Można uznać go za odmianę poprzedniego ataku, gdyż polega po prostu na wysyłaniu do AP ramek protokołu ARP, które to ramki zawsze spełniają warunki konieczne do przeprowadzenia ataku ***Natural packet replay***.

Opcje:

-3 - WYMAGANA - wybór funkcji ***ARP Replay***,

Opcje (filtrujące):
-b <MAC> - WYMAGANA - adres MAC AP którym jesteśmy zainteresowani,

Opcje wysyłania:
-h <MAC> - WYMAGANA - adres MAC dowolnego klienta zasocjowanego z tym punktem dostępowym – adresu tego użyjemy jako źródła generowanego ruchu.

Komputer rozpocznie nasłuchiwanie w celu znalezienia zapytania ARP odpowiadającego naszym filtrom (odpowiedni AP i klient nadający), po czym automatycznie zacznie generować kopie takiego zapytania. Będą one retransmitowane przez AP, a tym samym wygenerujemy interesujący nas ruch sieciowy do analizy.

Przykład:
aireplay-ng -3 –b 00:14:6C:7E:40:80 –h 00:14:6C:7E:40:80 ath0

4.5 Odszyfrowanie danych (KoreK chopchop)

Atak ma na celu odszyfrowanie danych zawartych w ramce WEP oraz określenie ciągu szyfrującego, bez znajomości klucza szyfrującego WEP. Potencjalnie sprawdza się nawet w przypadku mechanizmu WEP korzystającego z dynamicznie zmienianego klucza.

Atak bazuje na słabościach sumy kontrolnej ramki (ICV – Integrity Check Value) obliczanej z pomocą funkcji CRC-32.
Jego punktem wyjścia jest fakt, iż jeśli przechwycimy prawidłową ramkę pochodzącą z interesującej nas sieci, a następnie (nie rozszyfrowując jej) skrócimy jej pole danych o jeden bajt, to oczywiście stara, zaszyfrowana wartość ICV przestanie być prawidłowa. Dodatkowo wiemy, że konieczność jej zmiany wynika wyłącznie z faktu odrzucenia przez nas wspomnianego ostatniego bajtu pola danych (jako że innych zmian nie było).
Bazując na tym, okazuje się, że gdybyśmy znali niezaszyfrowaną wartość bajtu który odrzuciliśmy, to bylibyśmy w stanie skonstruować nowe, zaszyfrowane pole ICV, pasujące do naszej skróconej ramki.
Przyjmujemy więc, że interesujący nas bajt, w rozszyfrowanej postaci ma określoną wartość i na tej podstawie tworzymy nową wartość zaszyfrowanego pola ICV. Następnie tak spreparowaną ramkę wysyłamy do AP w celu retransmisji. Jeśli przyjęliśmy nieprawidłową wartość odrzuconego bajtu, to zrekonstruowane ICV będzie niepoprawne i AP odrzuci ramkę. Jeśli przyjęliśmy dobrą wartość rekonstrukcja ICV będzie poprawna i AP ramkę retransmituje potwierdzając nasz domysł dot. rozszyfrowanej wartości danego bajtu danych.
Mamy więc prosty sposób ustalenia rozszyfrowanej wartości ostatniego bajtu pola danych danej ramki (a mając jego zaszyfrowaną i rozszyfrowaną wartość, łatwo policzymy też odpowiadający mu bajt ciągu szyfrującego).
Aby rozszyfrować resztę ramki, bierzemy naszą nową skróconą ramkę (teraz już z prawidłowym ICV) i traktujemy ją jako punkt wyjścia – tzn. skracamy o jeden bajt i powtarzamy cały proces. W ten sposób jesteśmy w stanie rozszyfrować dowolną ramkę i dodatkowo uzyskać jej ciąg szyfrujący.

Pewnym problemem w zastosowaniu tego ataku może być fakt, iż niektóre AP nie przyjmują bardzo krótkich ramek, co uniemożliwia określenie początkowych bajtów pola danych. Program aireplay-ng próbuje w takim odgadnąć brakujące dane, opierając się na złożeniu, iż na początku pola danych znajduje się zwykle nagłówek warstwy wyższej (patrz 4.6).

Opcje:
-4 - WYMAGANA - wybór funkcji ***chop-chop***,

Opcje (filtrujące):
-b <MAC> - adres MAC AP którym jesteśmy zainteresowani,
-h <MAC> - adres MAC dowolnego klienta zasocjowanego z tym punktem dostępowym, którego ramki analizujemy.

Przykład:
aireplay-ng -4 -h 00:09:5B:EC:EE:F2 -b 00:14:6C:7E:40:80 ath0

4.6 Ustalenie ciągu szyfrującego (Fragmentation Attack)

Atak pozwala na uzyskanie ciągu szyfrującego, bez znajomości klucza szyfrującego WEP.
Oparty jest na tym, iż sieć 802.11 obsługują fragmentację, tzn. przesyłanie większych jednostek warstwy wyższej modelu ISO-OSI za pomocą kilku jednostek warstwy niższej, które są następnie składane. W naszym przypadku interesuje nas fakt, iż gdy prześlemy do ramkę 802.11 przeznaczoną do retransmisji przez AP w postaci wielu fragmentów, to AP złoży je w całość i retransmituje ją w postaci pojedynczej ramki 802.11.
Drugą informacją czyniącą ten atak możliwym, jest fakt, iż znamy odszyfrowaną zawartość początkowych 8 bajtów pola danych każdej ramki – jest to nagłówek warstwy wyższej (tzw. SNAP header) o znanej wartości. Wynika stąd, iż słysząc zaszyfrowaną ramkę, możemy od razu ustalić 8 pierwszych bajtów ciągu szyfrującego (znamy postać odszyfrowaną i zaszyfrowaną, ich XOR to ciąg szyfrujący).
Mając te 8 bajtów ciągu szyfrującego, możemy szyfrować i wysyłać ramki o 8 bajtowym polu danych – muszą one oczywiście także zawierać nagłówek SNAP, co czyniłoby tą metodą niezbyt użyteczną (zdołalibyśmy wysłać tylko nagłówek SNAP), gdyby nie możliwość fragmentacji. Po prostu wysyłamy większą ramkę w postaci serii ramek z 8 bajtowym polem danych (tylko pierwsza zawiera SNAP), a AP składa je w jedną i retransmituje.
Wyłapując z kolei retransmitowaną przez AP ramkę, złożoną z kawałków które przesłaliśmy, dysponujemy: jej postacią zaszyfrowaną (słyszymy retransmisję AP), oraz odszyfrowaną (znamy rozszyfrowane pole danych, gdyż jego zawartość przesłaliśmy w postaci wielu ramek z 8 bajtowymi polami danych). Mając tą informację ustalamy ciąg szyfrujący całej ramki prostym przekształceniem XOR.

Opcje:
-5 - WYMAGANA - wybór funkcji ***fragmentation***,

Opcje (filtrujące):
-b <MAC> - WYMAGANA - adres MAC AP którym jesteśmy zainteresowani,
-h <MAC> - WYMAGANA - adres MAC dowolnego klienta zasocjowanego z tym punktem dostępowym, którego ramki analizujemy.

Przykład:
aireplay-ng -5 -h 00:09:5B:EC:EE:F2 -b 00:14:6C:7E:40:80 ath0

Po wydaniu tego polecenia narzędzie rozpocznie nasłuchiwanie i da nam do wyboru ramkę, którą chcemy analizować. Jeśli potwierdzimy chęć analizy danej ramki to (opisanym powyżej

algorytmem) zostanie ustalony jej ciąg szyfrujący. Po zakończeniu pracy, ciąg szyfrujący zostanie zapisany w pliku na dysku.

---

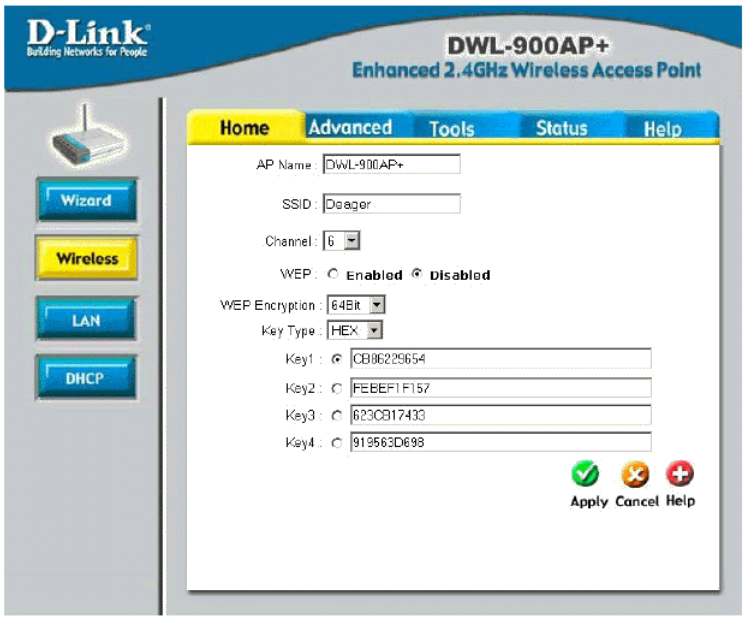
5 Konfiguracja punktów dostępowych

5.1 Konfiguracja AP firmy D-Link

Instrukcja konfigurowania punktu dostępowego firmy D-Link Dwl-900AP+ znajduje się w oficjalnej instrukcji do tego urządzenia. Istotny jest rozdział 5 zatytułowany „Using the Configuration Menu”. Dokument zawiera zrzuty ekranu, co znacznie ułatwia zapoznanie się z możliwościami AP.
Punkt dostępowy konfiguruje się z poziomu przeglądarki internetowej. Poniżej podane są potrzebne podczas zajęć opcje konfiguracyjne:

- SSID, kanał, oraz klucz WEP możemy ustawiać w zakładce **Home-> Wireless**
- Filtrację MAC ustawiamy w zakładce **Advanced-> Filters**

<u>Nie należy wprowadzać zmian w innych zakładkach interfejsu WWW punktu dostępowego.</u>



Rys. Strona konfiguracyjna D-Link Dwl-900AP+