Marcin Stolarski

WLAN - mechanizmy ochrony i sposoby ich łamania.

Artykuł do prezentacji.

Politechnika Warszawska

Warszawa 2004

Wersja 3.4a

Sieci bezprzewodowe stają się coraz popularniejsze. Na półkach sklepowych bez problemu można znaleźć dość tanie urządzenia przeznaczone do użytku domowego, które łatwo się konfiguruje za pomocą przeglądarki WWW. Większość z nich wystarczy jedynie podłączyć by uruchomić sieć. Artykuł ten pokaże szczegółowo jak działają obecne mechanizmy bezpieczeństwa, gdzie są ich słabe punkty, jak wykorzystywać te słabe punkty w celu obejścia zabezpieczeń oraz jakie praktyki należy wdrażać w sieciach, aby niwelować niedoskonałości standardu. Na koniec będą pokazane proponowane rozwiązania, które być może pojawią się w sieciach bezprzewodowych w formie znormalizowanych standardów w ciągu kilku najbliższych lat.

1. Wstęp

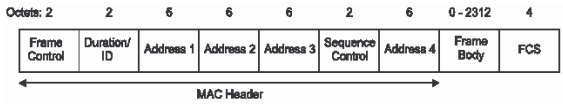
Gdy powstawały sieci WLAN, nie miały one dużej popularności ze względu na wolną transmisję oraz wysokie ceny na urządzenia. Twórcy standardu zdefiniowali jedynie słabe mechanizmy autoryzacji oraz szyfrowania, aby nie podrażać i tak drogich urządzeń. Wraz ze standardem 802.11b pojawiła się większa prędkość transmisji, co wpłynęło na gwałtowne zainteresowanie się tymi sieciami przez rynek, co z kolei spowodowało gwałtowny spadek cen urządzeń. Kiedy sprzęt trafił pod strzechy szybko okazało się, że sieci WiFi są niebezpieczne, oraz że istnieją problemy w stosowaniu ich w rozwiązaniach biznesowych. Niestety na kolejne unormowania trzeba będzie poczekać.

2. Opis protokółu 802.11

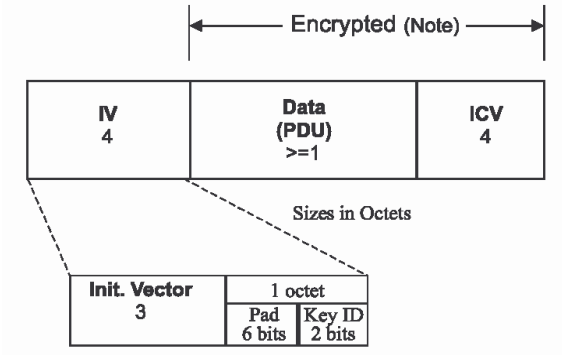
Sieci WLAN pojawiły się już w latach 80-tych. Brak jednolitego standardu powodował wzajemną niekompatybilność rozwiązań różnych firm. W roku 1997 pojawił się pierwszy standard w postaci normy 802.11. Zakładała ona transmisję ramek z prędkościami 1 i 2 Mbps na wolnej częstotliwości 2.4 GHz. Jako mechanizmy bezpieczeństwa stosowano identyfikator SSID oraz szyfrowanie kluczem WEP. Z czasem opracowano poprawki do normy w postaci norm 802.11a oraz 802.11b, które pozwoliły na większe prędkości (54Mbps dla standardu „a", 11Mbps dla standardu „b") oraz na wykorzystanie innych częstotliwości (5.6 GHz dla standardu „a"). Potem pojawił się standard 802.11g, który dzięki zastosowaniu modulacji kwadraturowej ze standardu „a" umożliwił osiągnąć prędkości 54Mb na częstotliwości 2.4GHz będąc kompatybilna ze standardem „b". Jak widać platforma sprzętowa rozwijała się, czego nie można powiedzieć o bezpieczeństwie. W roku 2000 pojawiły się pierwsze prace i artykuły mówiące o problemach i słabych punktach protokołu. W 2001 powstał ruch zwany „)(Warchalking" zajmujący się włamaniami do sieci radiowych. Mimo wyraźnych sygnałów ze świata nadal nic nie zmieniono w kwestii bezpieczeństwa. Jedyna ochroną nadal są mechanizmy: SSID oraz WEP. Na rok 2005 planowane jest pojawienie się unormowanego standardu 802.11i, w którym główny nacisk kładzie się na sprawy bezpieczeństwa. W miedzy czasie pojawiły się rozwiązania autorskie takie jak np. CISCO TKIP.

3. Budowa ramki

Na rysunku poniżej przedstawiono budowę ramki protokołu 802.11. Składa się ona z nagłówka, typu, adresu MAC, numeru ramki, pola z danymi oraz sumy kontrolnej.



W przypadku, kiedy zostanie włączone kodowanie WEP, pole z danymi jest podzielone na 3 sekcje. Pierwsza to nr klucza RC4, druga to pole z danymi, trzecia to suma kontrolna pola danych. Części druga i trzecia są kodowane algorytmem WEP.



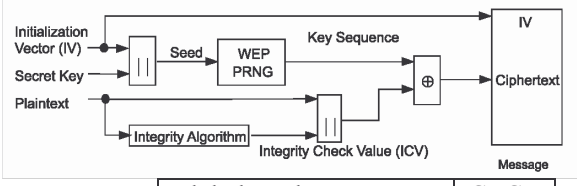
4. Bezpieczeństwo 802.11

W ramach protokołu 802.11 stworzono parę mechanizmów ochrony sieci tj: autentyfikację, SSID, WEP oraz MAC.

Podczas pierwszego połączenia stacji klienckiej musi nastąpić najpierw autoryzacja stron. Stosowane są dwa algorytmy. Typ 0 (open system - domyślny) polega jedynie na wymianie informacji kto z kim ma się połączyć i następuje uwierzytelnienie. W algorytmie typu 1 (shared-key) autoryzacja jest wykonywana przy wykorzystaniu kluczy WEP, tak więc obie strony muszą mieć taki sam klucz.

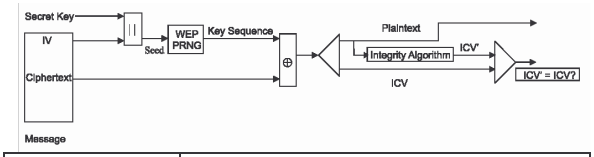
Kolejny mechanizmem ochrony jest identyfikator SSID. Mechanizm ten początkowo był wykorzystywany do wydzielenia oddzielnego VLAN-u w sieciach WiFi, aby uniemożliwić innym dostęp do danej podsieci. Każde urządzenie posiada identyczne hasło do sieci (SSID). Aby mogło transmitować pakiety, musi do pakietu dołączyć SSID jawnym tekstem, co powoduje wydzielenie podsieci. Niestety, jeśli zostanie uruchomione oprogramowanie nasłuchujące, to identyfikator SSID zostanie bardzo szybko znaleziony. Dodatkowo w Acccess Point-ach jest usługa wysyłania ramek rozgłoszeniowych (broadcast) z identyfikatorem SSID, aby inne urządzenia mogły pobrać sobie identyfikator, w celu przyłączenia do sieci. Jak widać, jeśli medium jest powietrze, to każdy praktycznie może nasłuchiwać i wysyłać pakiety w pobliżu naszej sieci. Oznacza to, że może bez problemów uzyskać identyfikator SSID i dołączyć się do naszej sieci.

Mechanizm WEP służy do szyfrowania danych w pakietach sieci 802.11. Aby zaszyfrować dane, wykonujemy operacje XOR na danych (wraz z sumą kontrolną CRC) oraz ciągu szyfrującym.



	Blok danych	CRC
XOR	Ciąg szyfrujący RC4(V, K)	
Wektor inicjujący	Blok zaszyfrowany	

Ciąg szyfrujący generowany jest przy wykorzystaniu algorytmu RC4, który na podstawie zmiennego 24b wektora inicjującego (V) i stałego klucza (K, 40b dla WEP 64b) generuje funkcja jednokierunkową pseudolosowy ciąg szyfrujący. Tak zaszyfrowany blok danych jest przesyłany wraz z wektorem inicjującym. Jeśli strona odbiorcza posiada identyczny klucz K, to na podstawie przysłanego wektora V jest w stanie wygenerować ciąg szyfrujący i po wykonaniu operacji XOR na ciągu szyfrującym oraz zaszyfrowanych danych otrzymuje oryginalne dane wraz z sumą kontrolną.



Wektor inicjujący	Blok zaszyfrowany	
XOR	Ciąg szyfrujący RC4(V, K)	
	Blok danych	CRC

Matematycznie można to przedstawić za pomocą równań:

P XOR RC4(V,K)=C
C XOR RC4(V,K)=P

Wektor V po każdej operacji jest zmieniany (zwykle inkrementowany) i ma długość 24b niezależnie od długości klucza K. Daje to 2^24 (16.777.216) kombinacji ciągu szyfrującego. Zgodnie z rachunkiem poniżej oznacza to, że dla sieci 11Mbps co około 5 godzin powtarza się ciąg szyfrujący.

11Mbps / (1500B [na pakiet] * 8b [na B])=91667 [pakietów na sekundę]

16777216 [kombinacji V]/ 91667 [pakietów na sekundę]=18302,41745 [sek. bez powtórki V]

18302,41745[sek bez powtórki V] / (60[sek na min] * 60[min na godz])=5,0840048[godz bez powtórki V]

Matematyka ukazuje nam słabość WEP-a, a mianowicie:

P XOR RC4(V,K)=C
C XOR RC4(V,K)=P

C1 = P1 XOR RC4(V, K)
C2 = P2 XOR RC4(V, K)
C1 XOR C2 = (P1 XOR RC4(V, K)) XOR (P2 XOR RC4(V, K)) = P1 XOR P2
(P2 XOR RC4(V, K)) = P1 XOR P2

Oznacza to, że jeśli zostaną przechwycone dwie ramki z identycznym ciągiem szyfrującym (wiemy to na podstawie V) i jest znana zawartość danych jednej z nich, to można bez większych problemów wyliczyć zawartość danych drugiej ramki. Do tego dochodzi fakt, że w polu danych przenoszone są ramki innych protokołów, które mają ściśle określone wartości na określonych polach.

Kolejnym problemem algorytmu WEP są tak zwane słabe klucze, które pozwalają złamać klucz główny WEP. Np. przy kodowaniu 64b, aby złamać klucz potrzeba przechwycić około 15 słabych kluczy z puli 1280 (1280 to 0.008% wszystkich kluczy). Na uwagę zasługuje fakt, że pula słabych kluczy rośnie wraz ze wzrostem długości klucza

głównego i tak np. przy kluczu 128b pula ta stanowi 0.020% wszystkich kluczy.

Ostatnim mechanizmem ochrony jest filtrowanie adresów MAC kart sieciowych. Adresy dozwolone bądź zabronione można wpisywać na listy, nie mniej ponieważ listy te nie są zbyt duże, nie pozwalają na budowę dużych mobilnych sieci. Poza tym adres MAC można zmienić w karcie za pomocą specjalnego oprogramowania, co pozwala się podszyć pod autoryzowane urządzenie.

5. Atak 802.11

Widząc słabość mechanizmów ochrony w sieciach bezprzewodowych, można pokusić się po parę scenariuszy ataku na taką sieć.

Jeśli sieć ma ustawiony tryb autoryzacji na 0, to wystarczy zostawić u siebie puste pole SSID i domyślny protokół autoryzacji wypełni to pole dając nam dostęp do sieci. Gdy w sieci jest uruchomiony serwer DHCP, to w zasadzie samo oprogramowanie karty radiowej podłącza nas do takiej sieci. Jeśli będzie ustawione wymaganie na podanie identyfikatora SSID wystarczy go podsłuchać od innych użytkowników sieci, ponieważ jest nadawany jawnym tekstem.

Jeśli sieć jest zabezpieczona kodowaniem WEP, możemy do sprawy podejść na wiele sposobów.

Pierwszy najprostszy to atak brutalny na klucz. Łapiemy ramkę, a następnie próbujemy ja zdekodować kolejno generowanymi kluczami. Jeśli zgadza się zakodowana suma kontrolna, to na kolejnych ramkach sprawdzamy czy tez się uda sprawdzić sumę i jeśli nam się to udaje to mamy klucz. Gdy następne ramki się nie dekodują, to szukamy dalej klucza aż do skutku. Na maszynie typu P4 2GHz dla klucza 40b taka operacja zajmie około 1 roku. Jeśli jednak klucz WEP zostanie wpisany nie jako fraza zapisana w postaci liczb o podstawie 16 (HEX), ale jako fraza ASCII to jego przedział zostanie zmniejszony do 2^21, co łamie się w przeciągu 10 sekund. Do tego, jeśli w ASCII jest napisana jakaś fraza słowna (np. nazwa firmy) możemy posiłkować się słownikiem (acz atak słownikowy należało by stosować do dłuższych kluczy).

Kolejna formą ataku na WEP jest wpuszczenie w sieć znanego tekstu (np. poczty elektronicznej) i zebraniu zestawu wszystkich kluczy sesyjnych do dekodowania innych ramek. Metodę te można rozwijać przez poszukiwanie w szyfrogramach znanych fragmentów protokołów komunikacyjnych takich jak http i łamania kolejnych kawałków kluczy sesyjnych. Wymaga to jednak posiadania pojemnych twardych dysków. Jeden zestaw kluczy to ok. 20MB.

Sieć bezprzewodową można też atakować wysyłając specjalnie spreparowane ramki. Metoda polega na przechwyceniu zakodowanej ramki, ingerencje w jej treść tak by np. zmienić adres jej przeznaczenia np. na własny komputer podłączony do Internetu, tak manipulując danymi, aby zgadzała się zakodowana suma CRC i jeśli zostanie odebrana ze strony internetu zdekodowana ramka można sobie wyliczyć określony klucz sesyjny.

Kolejnym miejscem, w które można uderzyć to filtrowanie adresów MAC, przez podsłuchanie autoryzowanych adresów, a następnie podmienienie takiego adresu we własnej karcie radiowej.

Ostatnim proponowanym atakiem na sieć radiową jest atak DoS, który może przybrać formę od zaawansowanej wpuszczając w sieć wadliwe pakiety lub blokując sieci przez nasycenie jej ramkami wysyłanymi ciągłym strumieniem z własnej karty, a kończąc na brutalnej przesterowującej stopnie wejściowe odbiorników radiowych silnym polem radiowym pochodzącym np. z otwartej kuchenki mikrofalowej.

Poniżej pokazane są dwa przykładowe ataki na sieć 802.11. Pierwszy pokazuje, jak możemy sprawdzać zawartość ramek nie posiadając klucza, a drugi jak można manipulować zawartością ramki tak by zachować zgodność z sumą kontrolną CRC

Przykład „Atak na WEP”

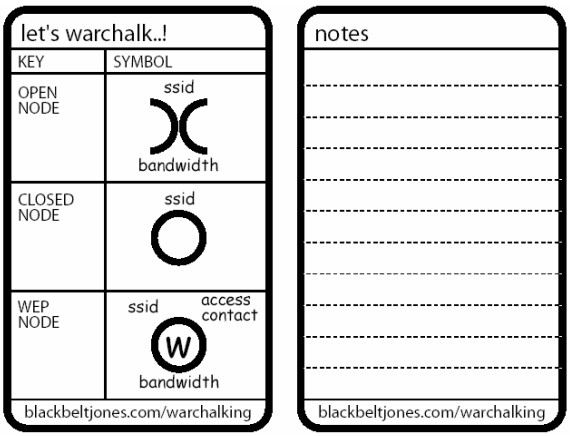
P „a” 01100001 K „n” 01101110 XOR ”a” 00001111	P „b” 01100010 K „n” 01101110 XOR ”b 00001100
XOR ”a” 00001111 XOR ”b” 00001100 XOR ”XaXb” 00000011	P „a” 01100001 P „b” 01100010 XOR ”PaPb” 00000011

Przykład „Atak na CRC”

Sieć	Haker
Data CRC-8 P „b” 01100001 00101001 K „n” 01101110 01101110 XOR ”b 00001100 01000111	
	Data CRC-8 XOR ”b” 00001100 01000111 Zmiana 00000011 00001001 XOR XOR ”b” 00001111 01001110
Data CRC-8 XOR XOR ”b” 00001111 01001110 K „n” 01101110 01101110 Wynik ”a” 01100001 00100000	

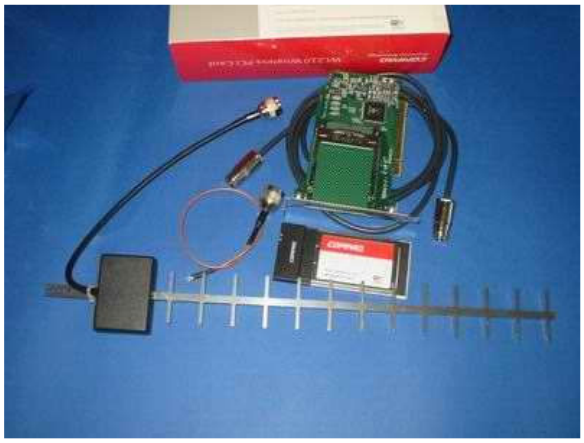
6. Atak w praktyce

Przed atakiem na daną sieć, można się rozejrzeć czy przypadkiem ktoś już tego nie zrobił wcześniej i nie zostawił stosownych informacji na murze czy płocie posesji. Poniżej jest pokazana karta z notacją znaków.



Aby przeprowadzić atak w praktyce należy zaopatrzyć się w:

- komputer (najlepiej przenośny)
- kartę radiową
- antenę
- przewód antenowy nisko stratny
- ewentualne przejściówki i złączki (kart radiowe mają różna złącza antenowe)
- odpowiednie oprogramowanie



Przy wyborze anteny należy się zastanowić skąd i w jakich warunkach sieć będzie podsłuchiwana. Są do wyboru anteny dookólne oraz kierunkowe (YAGI, panele, talerze).

Kolejną sprawą jest wybór karty radiowej. Pojawia się tutaj problem, który co prawda obecnie zanika, ale jest jeszcze obecny i generuje różne problemy. Chodzi o to, że w zależności od środowiska (Windows, Linux) programiści stosownych aplikacji preferują dwa różne chipsety kart. W Linux oprogramowanie było tworzone pod chipset PRISM2, a w Windows pod chipset HERMES. Stąd też wybierając środowisko pracy, należałoby pod system zakupić stosowną kartę. Poniżej tabela sprawdzonych rozwiązań rynkowych w zależności od chipset-u.

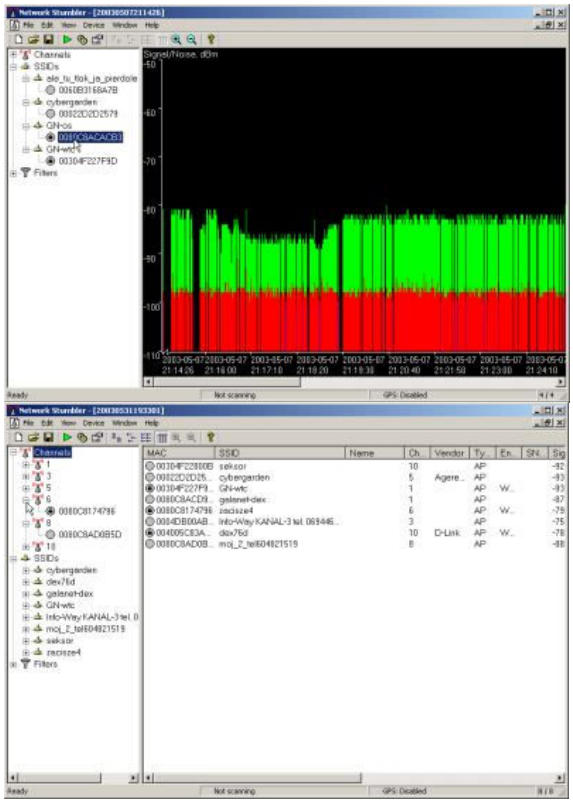
Chipset HERMES
• ORINOCO (Lucent PC) Card (FC-WD-11Ch, ETS-EU-13Ch) • Dell TrueMobile 1150 • Avaya Wirless PC Card • Compaq WL110 • Enterasysy Roamabout • Elsa Airlancer MC-11 • Arterm CC-WL11 • IBM High Rate Wirles LAN • Buaffalo WLI-PCM-L11 • 1stWave 1ST-PC-DSS11IS, DSS11IG, DSS11ES, DSS11EG • D-Link DWL-660 • Compex WL11A+ • Compex WL11B+ (Hermes II)

Chipset PRISM2
• Addtron AWP-100 • Ambicom WL100B-PC • Bromax Freeport • Compaq WL100 • D-Link DWL-650 • GemTek WL-211 • Intalk/Nokia WL201 • Linksys WPC11 • Samsung SWL2000-N • SMC 2632W • Teletronic WL1000 • YDI Diamond • Z-Com XI300 • Zoom Telephonics ZoomAir 4100

Aktualnie popularne oprogramowanie posiada stosowne poprawki umożliwiające prace na obydwu kartach, nie mniej chipset hermes zasługuje na szczególną uwagę, ponieważ podczas skanowania sieci nasycenie pola podaje w decybelach, a nie w bliżej nieokreślonych jednostkach porównawczych. Liderem na rynku jest firma Orinoco (dawniej Avaya) i najbardziej polecaną kartą jest karta Orinoco Gold Clasic (Gold oznacza możliwość kodowania WEP do 128b, a Clasic możliwość pracy w Access Poincie firmy Orinoco). Charakteryzuje się bardzo dużą stabilnością oraz popularnością wśród programistów. Niestety jest też bardzo droga (ok. 350 zł) i dość trudno dostępna w wersji europejskiej (13 kanałów). Można się też posiłkować tak zwanym klonem Orinoco czyli kartą, która elektronicznie jest kartą identyczną z Orinoco, a różni się jedynie frameware-m oraz sterownikami. Okazuje się bowiem, że klony często można uruchomić ze sterownikami Orinoco bądź Agree, które dają im pełną funkcjonalność Orinoco przy niższej cenie. (Np. Compex WL11B+ kosztuje ok. 130 zl)

Kolejna rzeczą, którą będziemy potrzebować jest oprogramowanie. Spośród wielu wyróżnić należy darmowe oprogramowanie pod Windows NetStumbler oraz pod Linux AirSnort oraz Wepcrack.

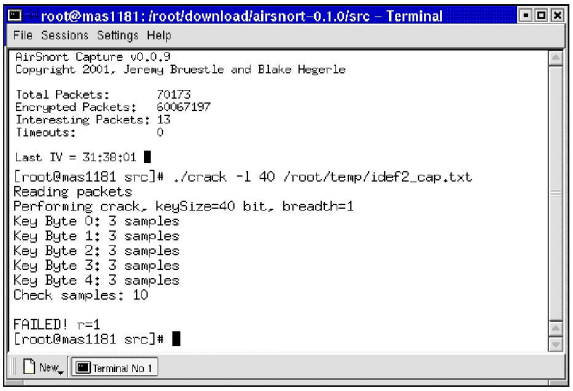
Program NetStumbler należy zaliczyć do zaawansowanych skanerów.



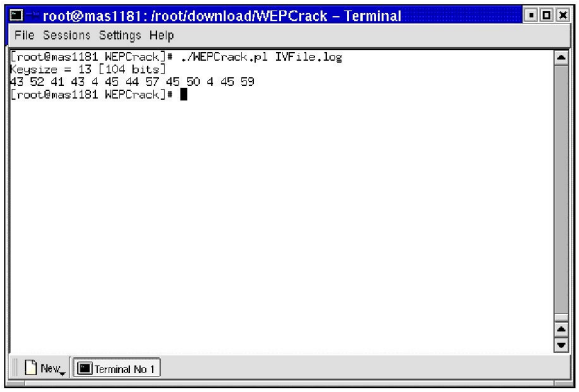
Pozwala na pokazanie, na jakich kanałach są określone sieci (po SSID) i jakie urządzenia (po adresach MAC). Dodatkowo pokazuje, czy dana sieć jest kodowana algorytmem WEP. Skaner ten jest chyba najczęściej wykorzystywaną aplikacją przez instalatorów urządzeń, ponieważ pokazuje wykres stosunku sygnału (kolor zielony) do szumu (kolor czerwony), co pozwala określić jakość i stabilność linku. Dodatkowym atutem oprogramowania jest możliwość podłączenia do niego GPS-a, który podaje dokładną swoją pozycję geograficzną. Jeśli byśmy taki zestaw (laptop z NetStumblerem, kartą radiową, GPS-em i anteną samochodową) umieścili w samochodzie i przejechali się po mieście, dostajemy mapę lokalizacji sieci radiowych w danym mieście. Jeśli sieć jest niechroniona (a tak jest w około 75% przypadków), pozostaje wpisanie stosowych parametrów do sterownika karty sieciowej.

Jeśli jednak sieć jest chroniona kodowaniem WEP, możliwy jest atak statystyczny na słabe klucze. Taki atak może przeprowadzić program AirSnort bądź Wepcrack.

Program AirSnort to w zasadzie aktywny skaner, który zbiera ramki 802.11 a następnie poszukując w nich słabych kluczy stara się złamać klucz WEP.



Program Wepcrack to skrypt w Perlu poszukujący klucza WEP na podstawie słabych kluczy. Aby można było z niego skorzystać należy najpierw zapisać na dysku stosowną ilość ruchu za pomocą snifera. Poniżej pokazane jest, jak Wepcrack złamał klucz WEP 128.



Jak widać, sieci oparte o standard 802.11 nie są bezpieczne. Aby się do nich włamać potrzebny jest niezbyt drogi sprzęt i odrobina wolnego czasu. Aby ta odrobina była jak najdłuższa, zamieszczono poniżej parę sugestii, którymi należy się kierować budując sieci bezprzewodowe. Pamiętać jednak należy o tym, że sieć radiową należy traktować jako słabo zabezpieczoną i jeśli zamierzamy w niej umieścić jakieś cenne dane, musimy posiłkować się dodatkowymi zabezpieczeniami takimi jak szyfrowane tunele SSH czy IPSec.

7. Przykazania administratora WLAN

- **Nie należy bezgranicznie ufać bezpieczeństwu WEP-a (może zostać bardzo szybko złamany)**
- **Należy separować sieci WiFi (stosując tunele VPN)**
- **Nie należy używać opisowych nazw SSID oraz urządzeń WiFi (są one łamane za pomocą słownika)**
- **Jeśli to możliwe, to należy blokować MAC adresy (zabezpiecza to przed amatorami)**
- **Należy zmieniać klucze WEP możliwie często (może komuś już nie będzie się chciało po raz kolejny łamać WEP-a skoro 75% sieci w sąsiedztwie nie stosuje WEP-a)**
- **Należy wyłączyć bacon (aby nie rozsyłać zaproszenia innym by się włamali)**
- **Powinno się instalować AP centralnie (AP ma ograniczony zasięg, czym dalej jest od ogrodzenia tym trudniej jest za ogrodzeniem uzyskać użyteczny sygnał do podsłuchiwania sieci)**
- **Należy zmieniać domyślne hasła i nr IP (hakerzy maja listy z takimi hasłami i będą próbować zmienić konfigurację sieci)**
- **Należy unikać słabych kluczy WEP (powinno się wpisywać losowe kody HEX jako klucz, unikać zapisu ASCII, a w szczególności unikać jako klucza haseł słownikowych)**
- **Nie powinno się używać w WLAN serwera DHCP (jeśli jest dosępny tryb autoryzacji 0 i serwer DHCP, to każdy kto włączy komputer z kartą WiFi zaloguje się automatycznie do sieci)**
- **Należy usuwać z sieci obce urządzenia WiFi (nie pozwalać pracownikom uruchamiać własnych komponentów WiFi. Zwykle uruchamiają je w konfiguracji domyślnej, która dla ułatwienia ma wyłączone wszystkie mechanizmy ochrony)**
- **Jeśli to możliwe należy włączyć dodatkowe zabezpieczenia producentów (zwykle oprogramowanie hakerskie nie potrafi sobie z nimi poradzić, a poza tym takie rozwiązania są skuteczne, gdyż sięgają do przyszłych standardów).**

8. Przyszłość

Dzisiejszy standard 802.11 nie zapewnia mocnego bezpieczeństwa. Producenci na rynku stosują nowsze rozwiązania (niestety niekompatybilne miedzy różnymi producentami).

Największą bolączką WEP-a jest czas życia kluczy oraz ich dystrybucja. Ponieważ są to klucze statyczne i aby je zmienić administrator musi wpisywać ręcznie nowe klucze na wszystkich urządzeniach danej sieci, daje to czas na łamanie tych kluczy. Z pomocą przychodzi tu protokół TKIP, który do kodowania pakietów nie używa statycznego klucza WEP, ale krótkoterminowe klucze sesyjne, nie dając czasu na ich złamanie. Gdyby protokół TKIP stał się kolejnym rozszerzeniem standardu 802.11, sieci bezprzewodowe były by bardzo trudne do złamania. Dodatkowo taka zmiana nie pociągnęłaby potrzeby wymiany urządzeń, a jedynie oprogramowania na nich.

Kolejną rzeczą, jaką się proponuje, jest wymiana kodowania WEP na AES. Niestety AES przez to, że jest znacznie bardziej obciążający obliczeniowo, wymaga wymiany sprzętu, co niestety w związku z faktem, że sporo tego typu sprzętu już jest na rynku, nie wróży mu dobrze na popularną przyszłość.

Oba powyższe mechanizmy prawdopodobnie będą zawarte w nowym standardzie bezprzewodowym 802.11i zwanym też WEP2. Nie mniej standard ten planowany jest dopiero na rok 2005, tymczasem sieci WiFi powstają teraz. Czołowi operatorzy telefonii komórkowej wprowadzają dostęp do internetu przy wykorzystaniu WiFi i myślę, że ciężko będzie ten standard wprowadzać, ponieważ ze względu na kodowanie AES będzie potrzeba wymiana sprzętu. Ewentualna emulacja AES-a za pomocą oprogramowania biedzie się wiązała z drastycznym obniżeniem wydajności sieci (kiedy kodowanie WEP nie było popularne i traktowano je jako opcja w AP to realizowano je programowo, co powodowało że przepustowość sieci spadała z 11Mb do 2Mb). Mówiąc krótko standard ten pojawia się za późno i jest niekompatybilny ze

starym sprzętem. Dodatkowo pojawiają się artykuły na podstawie wersji roboczej standardu, że tutaj też są problemy z bezpieczeństwem oraz Atakami DoS (proponuje się, aby reakcją AP na atak było jego tymczasowe milknięcie, jeśli atak będzie polegał na zalaniu AP błędnymi ramkami spowoduje to wstrzymanie pracy AP). Zapotrzebowanie rynku na bezpieczne sieci radiowe jest jednak duża i widać już pierwsze ruchy firm w celu przynajmniej częściowego wdrożenia tego standardu, a mianowicie autoryzacji WPA, a w ramach niej szyfrowania TKIP. Pojawiła się nawet lista sprzętu zgodnego w WPA. Standard WPA składa się z mechanizmów 802.11x (omówiony w następnym akapicie), TKIP, EAP (nowy sposób na autoryzacji AP-APC) oraz MIC (nowy sposób sprawdzania integralności pakietów, ponieważ CRC32 nie jest bezpieczny). Jako ciekawostkę można podać, że wymienione mechanizmy już dość długo można znaleźć w urządzeniach CISCO.

Standard 802.11x zajmuje się on transportem danych związanym z autoryzacją klientów w AP w oparciu o centralną bazę danych klientów opartą o serwer Radius-a. Jego uniwersalność pozwala użyć go także do innych celów np. do transportu kluczy sesyjnych TKIP. Działanie tego mechanizmu autoryzacji w AP w oparciu o 802.11x jest proste:

- klient prosi o autoryzację i podaje swoją nazwę
- AP wysyła do klienta ciąg znaków i prosi o zakodowanie algorytmem jednokierunkowym przy wykorzystaniu klucza, jaki jest trzymany na serwerze Radius-a
- AP podobne zapytanie wysyła do serwera Radius-a dołączając nazwę klienta.
- kiedy AP otrzyma odpowiedzi z obu stron i są one identyczne, autoryzuje klienta

Standard 802.11x jest odpowiedzią na słabą autoryzacje 802.11 oraz pozwala na centralne zarządzanie baza danych o klientach. Standard ten jest bardzo chętnie wdrażany przez producentów i obecnie każde nowe urządzenie jest z nim zgodne.

9. Podsumowanie

Podsumowując powtórzę jeszcze raz. Standard 802.11 jest niebezpieczny. Trzeba pamiętać, że nawet kodowanie WEP nie zapewnia bezpieczeństwa, a jedynie szyfrowane tunele mogą rozwiązać ten problem. Można też posiłkować się rozwiązaniami autorskimi firm zapewniający odpowiedni poziom bezpieczeństwa, ale należy pamiętać, że o ile rozwiązania te wydają się skuteczne, to nie są kompatybilne z urządzeniami innych firm oraz, że nie zostały one gruntownie przetestowane na „światowym" poziomie. Ciekawie przedstawia się sprzęt zgodny z WPA (fragmentem standardu 802.11i w wersji draft). Można powiedzieć, że o ile w większości jest zainstalowany sprzęt zgodny z 802.11b, to na pólkach sklepowych leży sprzęt zgodny z 802.11g i WPA. W ciągu roku powinien pojawić się sprzęt zgodny z WPA2. Na sam koniec napiszę to, czego nie wolno robić, a co robi 75% użytkowników sieci 802.11 licząc na to, że może się opamiętają. **NIE MOŻNA ZOSTAWIAĆ W URZADZENIACH KONFIGURACJI DOMYŚLNEJ,** ponieważ każdy, kto w okolicy włączy komputer wyposażony w kartę WiFi, automatycznie zaloguje się do naszej sieci jako pełnoprawny użytkownik. Należy o tym pamiętać bezwzględnie. Znam osobiście jednego administratora, który w ten sposób połączył dwie siedziby firmy myśląc (za przewodnictwem instrukcji), że bezpieczeństwo zapewnia unikalny identyfikator SSID ☺. Na stronach Warchalking-gu można znaleźć statystyki, że nie jest osamotniony, a wręcz należy do większości.

Statystyki (Dane na rok 2002)

- Manhattan

263 sieci z czego szyfrowanie WEP miało 65 sieci (25%)

- Północna Virginia

114 sieci z czego szyfrowanie WEP miało 32 sieci (28%)

- Warszawa (rok 2004)

149 sieci – WEP 53 sieci (36%) – Ustawienia domyślne 18 sieci (12%)

Więcej informacji

Marcin Stolarski mstolars@elka.pw.edu.pl

http://warchalking.xo.pl/
http://www.ieee.org
news:news.radiowe.sieci.chipdrive.pl

Literatura

1. Michael Sutton
„Hacking the Invisible Network. Insecurities in 802.11x", 2002r.
2. Normy:
802.11 IEEE Computer Society, 1999r.
802.11a IEEE Computer Society, 1999r.
802.11b IEEE Computer Society, 1999r.
802.11i IEEE Computer Society, 2002r.
802.11x IEEE Computer Society, 2001r.