BEZPIECZEŃSTWO SIECI BEZPRZEWODOWYCH WI-FI

Data napisania: 2007

Spis Treści

WSTĘP 3

Rozdział I: Ogólne informacje o sieciach bezprzewodowych 6

1.1 Historia powstania 6
1.2 Najważniejsze standardy 802.11 7
1.3 Zasada działania 9
1.4 Zalety sieci Wi-Fi 11

Rozdział II: Wardriving – badanie zabezpieczeń sieci Wi-Fi 14

Rozdział III: Zagrożenia wynikające z korzystania z sieci Wi-Fi 18

3.1 Ataki i włamania do sieci 19
3.1.1 Podsłuch 19
3.1.2 Podszywanie się pod adres IP 20
3.2 Nieświadomość administratorów o zagrożeniach 21
3.3 Zagrożenia fizyczne 22

Rozdział IV: Bezpieczeństwo sieci bezprzewodowych 24

4.1 Ukrycie SSID 25
4.2 Filtracja MAC 25
4.3 WEP 26
4.3.1 Zasada działania 26
4.3.2 Wady protokołu WEP 28
4.3.3 Firmowe rozszerzenia protokołu 30
4.3.4. Dlaczego stosuje się WEP 31
4.4. WPA 31
4.4.1 Zasada działania mechanizmu WPA 32
4.4.2. Wady i problemy protokołu 34
4.5. WPA2 (802.11i) 35
4.6. Uwierzytelnianie i szyfrowanie (w sieciach bezprzewodowych) 38
4.6.1. Standard IEEE 802.1x 38
4.6.2. EAP 39
4.6.3. PPPoE (Point-to-Point Protocol over Ethernet) 40
4.6.4. VPN (Virtual Private Network) 40
4.7. WPS (Wi-Fi Protected Setup) 41
4.8. Dekalog administratora sieci 43
4.9. Fizyczne zabezpieczenia sieci 44
4.9.1 Zabezpieczenia przed kradzieżą 44
4.9.2 Zabezpieczenia przed działaniem czynników atmosferycznych. 45

Rozdział V. Utworzenie dobrze zabezpieczonej sieci Wi-Fi w praktyce. 47

5.1 Sieć niezabezpieczona 48
5.2 Wyłączenie rozgłaszania nazwy SSID sieci 50

5.3 Filtracja MAC 51
5.4 Szyfrowanie WEP 53
5.5 Szyfrowanie WPA 54
5.6 802.11i – najlepsze zabezpieczenie 55

Rozdział VI: Inne sieci bezprzewodowe 56

6.1. Podczerwień (IrDA) 56
6.2. Bluetooth 56
6.3. Wimax 57
6.4. VectraStar 58
6.5. LMDS i MMDS 59
6.7. FSO 59
6.8. Porównanie technologii bezprzewodowych 60

Wnioski 61

Bibliografia 62

Wykaz rysunków 63

WSTĘP

Celem mojej pracy jest przedstawienie zagrożeń, z jakimi można się spotkać korzystając z sieci bezprzewodowych oraz pokazanie w jaki sposób się przed nimi zabezpieczyć. Zagrożenia te związane są najczęściej z próbą nieautoryzowanego dostępu do sieci lub przechwytywaniem przesyłanych danych. Sieci standardu 802.11, nazywane popularnie Wi-Fi, są obecnie jedną z najprężniej rozwijających się technologii IT. Dziesięć lat temu mało kto słyszał o bezprzewodowym Internecie, a dzisiaj sprzedaż urządzeń obsługujących sieci standardu 802.11 sięga milionów sztuk i obroty firm produkujących sprzęt sieciowy liczone są w miliardach dolarów. Nie ma chyba miasta, w którym nie byłaby zainstalowana chociażby jedna sieć Wi-Fi. Dzięki sieci bezprzewodowej Internet zaczyna pojawiać się coraz częściej w małych miasteczkach i wsiach, gdzie połączenie z globalną siecią było wcześniej zbyt kosztowne ze względu na problemy z doprowadzeniem kabli. Można powiedzieć, że sieci Wi-Fi powstają jak „grzyby po deszczu" i w większych miastach liczba zainstalowanych sieci bezprzewodowych może dochodzić nawet do tysiąca. W pierwszym rozdziale chciałbym przedstawić podstawy działania sieci standardu 802.11 oraz pokazać, dlaczego stały się one tak popularne.

Mimo tak wielkiej ilości sieci bezprzewodowych w miastach, nie są one zabezpieczone w odpowiedni sposób. Według danych zawartych w książce „Wi-Foo Sekrety bezprzewodowych sieci komputerowych" w 2002 roku spośród znalezionych 580 punktów dostępowych tylko 30% było zabezpieczone mechanizmem WEP, 19% używało domyślnego identyfikatora SSID a lekko ponad 18% sieci nie posiadało żadnego zabezpieczenia i posługiwało się domyślnym SSID. Badania te były przeprowadzone w Stanach Zjednoczonych 5 lat temu, jednak od tego czasu niewiele się zmieniło. Chcąc sprawdzić jak to wygląda dzisiaj, zdecydowałem się na przeprowadzenie podobnych badań w mojej miejscowości. Wyniki tych badań przedstawione w rozdziale „Wardriving – wyszukiwanie sieci" pokazują jak szybko rozwija się technologia Wi-Fi oraz jak mało ludzi zwraca uwagę na bezpieczeństwo sieci bezprzewodowych. Wielu właścicieli punktów dostępowych, z których korzysta mała ilość użytkowników twierdzi, że nie ma się czego obawiać i nawet jeśli ktoś

skorzysta z jego sieci do przeglądania stron i sprawdzenia poczty to nic się nie stanie. Niestety sporo osób popełnia ten sam błąd myśląc - jeżeli nic się złego nie dzieje z połączeniem to znaczy, że jest dobrze. Jest to błędne przekonanie i niektórzy mogą sobie zdać z tego sprawę dopiero po fakcie. Jeśli ktoś wykorzysta nasze łącze do nielegalnych celów do akcji może wkroczyć organ ścigania a spotkanie z nimi nie należy do przyjemności. Dokładniej opiszę to w rozdziale III książki zatytułowanym: „Zagrożenia wynikające z korzystania z sieci Wi-Fi".

Na szczęście przed nieautoryzowanym połączeniem idzie się w łatwy sposób obronić, wystarczy tylko poświęcić trochę czasu na ustawienia zabezpieczeń, jakie oferują punkty dostępowe. Pierwszym dobrym zabezpieczeniem, jaki zastosowano w sieciach standardu 802.11 był protokół WEP (Wired Equivalent Privacy). Chciałbym w tym miejscu podkreślić słowo „był" ponieważ w roku 2001 zabezpieczenie to zostało złamane i w dzisiejszych czasach zapewnia tylko minimalny stopień ochrony. Mimo to poświęciłem sporo miejsca szyfrowaniu WEP, dlatego że jest to w dalszym ciągu najczęstsze zabezpieczenie stosowane w sieciach Wi-Fi. O wiele lepszym poziomem bezpieczeństwa może pochwalić się protokół WPA, który opiera się na podobnym działaniu co WEP, jednak pozbawiony jest większości wad poprzedniego systemu. Prace nad WPA (Wifi Protected Access) rozpoczęły się zaraz po pierwszych doniesieniach o złamaniu WEP, a jakiś czas później został on wdrożony do działania. Mechanizm WPA jeśli zostanie poprawnie zaimplementowany i dobrze zarządzany, jest bardzo silnym zabezpieczeniem oraz bardzo trudnym do złamania. W późniejszym czasie pojawił się kolejny mechanizm szyfrowania - 802.11i, który jest rozszerzeniem WPA i dlatego często jest nazywany WPA2. Wprowadzony w styczniu bieżącego roku system WPS, pozwala na bardzo łatwą konfigurację zabezpieczeń sieci Wi-Fi. Ponieważ technologia ta jest bardzo przyjazna dla użytkownika można się spodziewać, że będzie stosowana coraz częściej. Zasadę działania systemu WPS opisuję w kolejnym podrozdziale**.**

W rozdziale V pokazuję w praktyce słabości opisanych przeze mnie zabezpieczeń. Do tego celu wykorzystałem zrobioną specjalnie do tej prezentacji sieć bezprzewodową składającą się z punktu dostępowego i 2 komputerów. Trzeci komputer – laptop posłużył mi do zademonstrowania, w jaki sposób omijać kolejne zabezpieczenia. Z przeprowadzonych badań wynika, że tylko szyfrowanie WPA2 może skutecznie zabezpieczyć sieć Wi-Fi przed nieautoryzowanym dostępem.

W ostatnim rozdziale opisałem stopień bezpieczeństwa innych sieci bezprzewodowych niż te oparte na standardzie 802.11, są to sieci wykorzystujące podczerwień oraz fale radiowe na różnych częstotliwościach i pomimo, że do popularności Wi-Fi im wiele brakuje to za kilka lat może któryś z tych standardów będzie najczęściej używany.

Rozdział I: Ogólne informacje o sieciach bezprzewodowych

1.1 Historia powstania

W XX wieku najistotniejszą technologię stanowiło gromadzenie, przetwarzanie i dystrybucja informacji. Dzięki temu powstała ogólnoświatowa sieć telefoniczna, radio i telewizja, narodził się i w zawrotnym tempie rozwijał przemysł komputerowy, zaczęto tworzyć sieci by wymieniać się informacjami. Pod koniec XX wieku bardzo szybko zaczęła rozwijać się komunikacja bezprzewodowa, która non stop jest ulepszana. Chociaż może wydawać się to dziwne, jednak łączność bezprzewodowa nie jest wcale niczym nowym. Już w 1901 roku włoski fizyk G. Marconi zademonstrował bezprzewodowy telegraf łączący statek z lądem za pomocą kodu Morse'a.[1] Teraz, 100 lat później, można powiedzieć, że idea przesyłu informacji falami radiowymi została w pełni wykorzystana. Historię narodzin bezprzewodowych sieci komputerowych opisał bardzo dokładnie Jeff Duntemann w swojej książce „Przewodnik po sieciach Wi-Fi":

„Sieci bezprzewodowe mają swoją historię. Pracę nad bezprzewodowymi lokalnymi sieciami komputerowymi zostały rozpoczęte w roku 1971 na uniwersytecie na Hawajach eksperymentem o nazwie ALOHANET. System zbudowany w ramach tego eksperymentu był drogim, wyposażonym w duże anteny systemem mającym na celu rozwiązanie dosyć poważnego problemu – przesyłania danych między wydziałami uniwersytetu rozmieszczonymi na czterech wyspach. Jednak zasady budowy były takie same jak zasady rządzące przesyłaniem danych między komputerem zainstalowanym w pracowni a komputerami zainstalowanymi w pokojach dziecinnych. W 1992 roku firma SUN Microsystems zaprojektowała niewielki podręczny komputer o nazwie Star 7 mający możliwości tworzenia sieci bezprzewodowych na częstotliwości 900 MHz. Produkt ten nigdy jednak nie pojawił się na rynku. (…)Zademonstrowany na pokazie handlowym na targach COMDEX w 1994 roku system WaveLAN (…) składał się z laptopa z zainstalowaną kartą PCMCIA, połączonym z komputerem osobistym

[1] „Sieci komputerowe" – Andrew S. Tanenbaum

oddalonym o kilka kroków. Przepustowość systemu wynosiła 1,6 Mb/s, co na tamte czasy było wielkością znaczącą.

(…) System WaveLAN działał i to bardzo dobrze. Mimo że był bardzo drogi, znaleźli się jednak odbiorcy, którym był niezbędnie potrzebny. Głównie byli to wysoko opłacani konsultanci tworzący niestandardowe rozwiązania pewnych problemów w dużych korporacjach. Dzięki nim ten system, jak i wiele podobnych systemów, stał się początkiem rozwoju sieci bezprzewodowych. Każda z firm zajmujących się sieciami bezprzewodowymi miała własny schemat łączenia danych w pakiety i wysyłania ich za pośrednictwem fal radiowych. Niestety, żaden z tych schematów nie był w stanie porozumiewać się z innymi."

W latach 90'tych zaprojektowano wiele technologii bezprzewodowych, ale z powodu różnych standardów i braku współpracy między dwoma sieciami żadna nie zyskała większej popularności. Wszystko zmieniło się w 1997 roku, kiedy to Instytut Inżynierii Elektrycznej i Elektronicznej (IEEE) opublikował standard 802.11. Od tamtej pory nastąpił bardzo gwałtowny rozwój sieci Wi-Fi. Kolejno pojawiały się coraz to szybsze standardy: 802.11, 802.11b, 802.11a, 802.11g, a niedawno 802.11n. Obecnie do budowy sieci najczęściej wykorzystuje się standard 802.11g, który pracuje na częstotliwości 2,4 GHz i może teoretycznie pracować z prędkością 54 Mb/s. Jeszcze szybszy standard 802.11n, już powoli zaczyna wypierać poprzedników i najprawdopodobniej za rok lub dwa to właśnie ten standard będzie najczęściej stosowany w sieciach Wi-Fi, a za parę lat z pewnością pojawi się nowy.

1.2 Najważniejsze standardy 802.11

Grupa standardów 802.11 dotyczących sieci bezprzewodowych została sporządzona przez organizację IEEE w celu stworzenia wspólnego standardu zapewniającego kompatybilność i niezawodność urządzeń wytwarzanych przez różnych producentów. Poniżej przedstawiam krótką charakterystykę najbardziej istotnych standardów rodziny 802.11.

- 802.11 – zatwierdzony w 1997 roku był pierwszym standardem, w celu odróżnienia od grupy 802.11 później nazywany 802.11y. Zastosowana

częstotliwość fal radiowych wynosiła 2,4 GHz natomiast dostępna przepustowość mieściła się w przedziale od 1 do 2 Mb/s.

- 802.11b – wprowadzony dwa lata później standard został znacznie poprawiony pod względem przepustowości, pozwalał na przesyłanie danych z maksymalną prędkością 11 Mb/s. Dzięki temu sieci bezprzewodowe zaczęły się cieszyć coraz większym zainteresowaniem. Podobnie jak poprzedni standard, 802.11b korzystał z częstotliwości 2,4 GHz.
- 802.11a – zatwierdzony przez IEEE w 1999 roku, jednak wprowadzony do użytku dopiero w 2001 roku. Do przesyłu danych drogą radiową zastosowano częstotliwość 5 GHz, co pozwoliło na zwiększenie przepustowości do 54 Mb/s. Standard ten pomimo wyższej prędkości nie zyskał na popularności, ponieważ był za późno wprowadzony, pobierał więcej mocy, był droższy od pozostałych i miał mniejszy zasięg niż 802.11b.
- 802.11g – powstał z połączenia niektórych technik poprzednich standardów. Wykorzystuje pasmo 2,4 GHz oraz pozwala przesyłać dane z prędkością do 54 Mb/s. Został zatwierdzony w 2003 roku. Standard 802.11g jest całkowicie zgodny w dół ze standardem 802.11b. Jednak wykorzystanie starszych urządzeń powoduje w praktyce redukcję prędkości do 11 Mb/s. Obecnie standard ten jest najczęściej wykorzystywany do tworzenia sieci bezprzewodowych.
- 802.11n – najnowsze dzieło komitetu IEEE jest aktualnie w trakcie tworzenia. Teoretycznie standard ma pracować z maksymalną przepustowością 540 Mb/s, w praktyce będzie to około 100-200 Mb/s. Planowane zakończenie prac ogłoszono na 2008 rok. Mimo to producenci już zaczęli wprowadzać na rynek urządzenia zgodne z tym standardem oparte na wersji 1.0 szkicu 802.11n. 19 stycznia 2007 roku została zaakceptowana wersja 2.0 tego standardu. Jeżeli uda się zrealizować wszystkie założenia teoretyczne to niewykluczone, że za parę lat 802.11n zastąpi obecnie używany 802.11g.

1.3 Zasada działania

Sieci komputerowe standardu 802.11 działają w wydzielonym widmie fal radiowych o częstotliwości 2,4 GHz lub 5 GHz. W większości krajów widmo to zostało zarezerwowane dla połączeń typu punkt-punkt oraz dla technologii radiowych widma rozproszonego, które nie wymagają licencji. Ponieważ pasmo 2,4 GHz nie jest chronione, mogą korzystać z niego inne urządzenia, niezwiązane z Wi-Fi takie jak: telefony bezprzewodowe i kuchenki mikrofalowe. W Polsce urządzenia radiowe mogą być stosowane bez pozwolenia, jeżeli spełniają następujące warunki:[2]

- w paśmie 2400 ÷ 2483,5 MHz, gdy stosują modulację szerokopasmową i moc wypromieniowywana EIRP nie przekracza 100mW
- w paśmie 5470 ÷ 5725 MHz, gdy pozwalają na sterowanie mocą (w zakresie minimum 3dB) w celu uniknięcia zakłóceń, umożliwiają dynamiczny wybór częstotliwości (DFS) oraz moc wypromieniowywana EIRP nie przekracza 1W

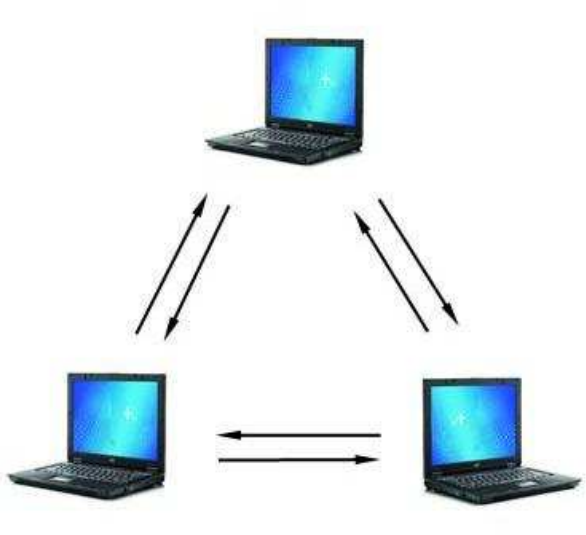
Z pasma 2,4 GHz korzysta większość standardów rodziny sieci 802.11, wyjątkiem jest jedynie 802.11a, w którym to do przesyłu fal radiowych zastosowano częstotliwość 5 GHz. Większość sprzętu Wi-Fi dostępnego obecnie na rynku, oparta jest na standardzie 802.11g, dlatego też w swojej pracy skoncentruję się głównie na sieciach tego typu oraz 802.11b, ponieważ jeszcze sporo sieci działa w starszym systemie.

Pasmo 2,4 GHz zostało podzielone na 14 podczęstotliwości (kanałów), aby umożliwić działanie kilku sieci Wi-Fi na jednym terenie. Nie jest to jednak standard międzynarodowy i każde państwo na świecie może wykorzystywać inne podziały częstotliwości. W Polsce jak i prawie w całej Europie (z nielicznymi wyjątkami) wykorzystywanych jest 13 podczęstotliwości. We Francji na przykład, można korzystać tylko z 4 kanałów. Po drugiej stronie oceanu zakres częstotliwości wykorzystywanych w sieciach standardu 802.11 nieco się różni, w USA kanałów jest 11, natomiast w Japonii można korzystać z wszystkich 14. Częstotliwości wyspecyfikowane dla każdego z tych kanałów są częstotliwościami środkowymi dla pasm o szerokości 22 MHz a odległość między nimi wynosi zaledwie 5 MHz. Powoduje to nakładanie się

[2] Dz.U z 2005r Nr 230, Poz. 1955 „Rozporządzenie Ministra Infrastruktury z dnia 24 października 2005 r. w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia radiowego”

kanałów z kilkoma innymi położonymi wyżej lub niżej. Aby uniknąć interferencji w przypadku działania kilku sieci, odległości pomiędzy kanałami powinny wynosić przynajmniej 25 MHz. Jeżeli ta odległość będzie mniejsza, przepustowość sieci może znacznie się obniżyć. W przypadku działania na przykład 3 sieci bezprzewodowych w jednej okolicy powinno się ustawić kanały 1, 6 i 11.

Sieci Wi-Fi mogą działać w dwóch trybach pracy: w trybie ad hoc (równorzędnym) oraz w trybie infrastrukturalnym. Pierwszy typ sieci jest zwykle stosowany w połączeniach tymczasowych i może się składać się z kilku urządzeń. Klienci łączą się ze sobą „każdy z każdym" i nie mają połączenia z większą lokalną siecią komputerową ani z Internetem.



Rys. 1. Sieć typu ad hoc
Ilustracja własna, wykorzystano zdjęcia z www.hp.com

Z topologią sieci infrastrukturalnych mamy do czynienia wówczas, gdy w sieci znajduje się przynajmniej jeden punkt dostępowy, pozwalający uzyskać połączenie z siecią kablową i całym światem.

Rys. 2. Sieć typu infrastrukturalnego
Ilustracja własna, wykorzystano zdjęcia z www.dlink.com oraz www.hp.com

Większość działających sieci bezprzewodowych pracuje w trybie infrastrukturalnym, ale opisane przeze mnie w dalszej części pracy metody zabezpieczeń odnoszą się do obydwu typów sieci.

1.4 Zalety sieci Wi-Fi

Sieci bezprzewodowe Wi-Fi z dnia na dzień zyskują coraz bardziej na popularności, dzieje się tak, dlatego że rozwiązują kilka problemów, z którymi sieci przewodowe nie mogły sobie poradzić. Instalując sieć standardu 802.11 w budynku, nie musimy tak jak w przypadku zwykłej sieci wiercić dziur w ścianach na kable i ciągnąć ich przez cały dom lub budynek firmy. Oprócz względów estetycznych właściwości sieci bezprzewodowych idealnie znajdują zastosowanie w starszym budownictwie i zabytkach, gdzie jakiekolwiek wiercenie jest prawnie zabronione.

Chcąc połączyć ze sobą dwa budynki znajdujące się po przeciwnych stronach drogi, możemy napotkać na spory problem. Po pierwsze musimy uzyskać od gminy lub

miasta pozwolenie na przekop pod drogą, co nie jest łatwym zadaniem, a po drugie to samo przeciągnięcie kabla pod drogą w ziemi jest kosztownym przedsięwzięciem. W takim wypadku ponownie przychodzą nam z pomocą fale radiowe, można połączyć dwa budynki siecią bezprzewodową bardzo szybko, łatwo i niedrogo.

Kolejnym miejscem gdzie Wi-Fi zdobywa popularność są małe miasta i wsie. Sieci bezprzewodowe pozwalają na wspólne użytkowanie przez kilka osób jednego szerokopasmowego połączenia z Internetem bez konieczności ciągnięcia kabli, co przy luźnej zabudowie domów musiałoby się skończyć na pociągnięciu kilku kilometrów kabla.

Dzięki technologii bezprzewodowej komputery zaczynają powoli odrywać się od biurka. Można siedzieć z laptopem w dowolnym miejscu domu i korzystać z Internetu a pocztę przeglądać siedząc w ogrodzie. Wiele osób korzysta też z sieci standardu 802.11 w czasie podróży, darmowe punkty dostępowe zwane hot spot'ami umieszczane na lotniskach, dworcach i kawiarniach pozwalają za darmo uzyskać dostęp do Internetu. Sieci bezprzewodowe okazały się bardzo przydatne na konferencjach i zebraniach, gdzie użytkownicy mogą łączyć się bez przeszkód i wymieniać notatkami.

Oprócz wymienionych przeze mnie przykładów zastosowań sieci Wi-Fi mogą znaleźć zastosowanie praktycznie wszędzie. Sieci bezprzewodowe mogą obsługiwać także inne urządzenia niż komputery, na przykład kamery, które są montowane w miejscach gdzie doprowadzenie kabli jest utrudnione.

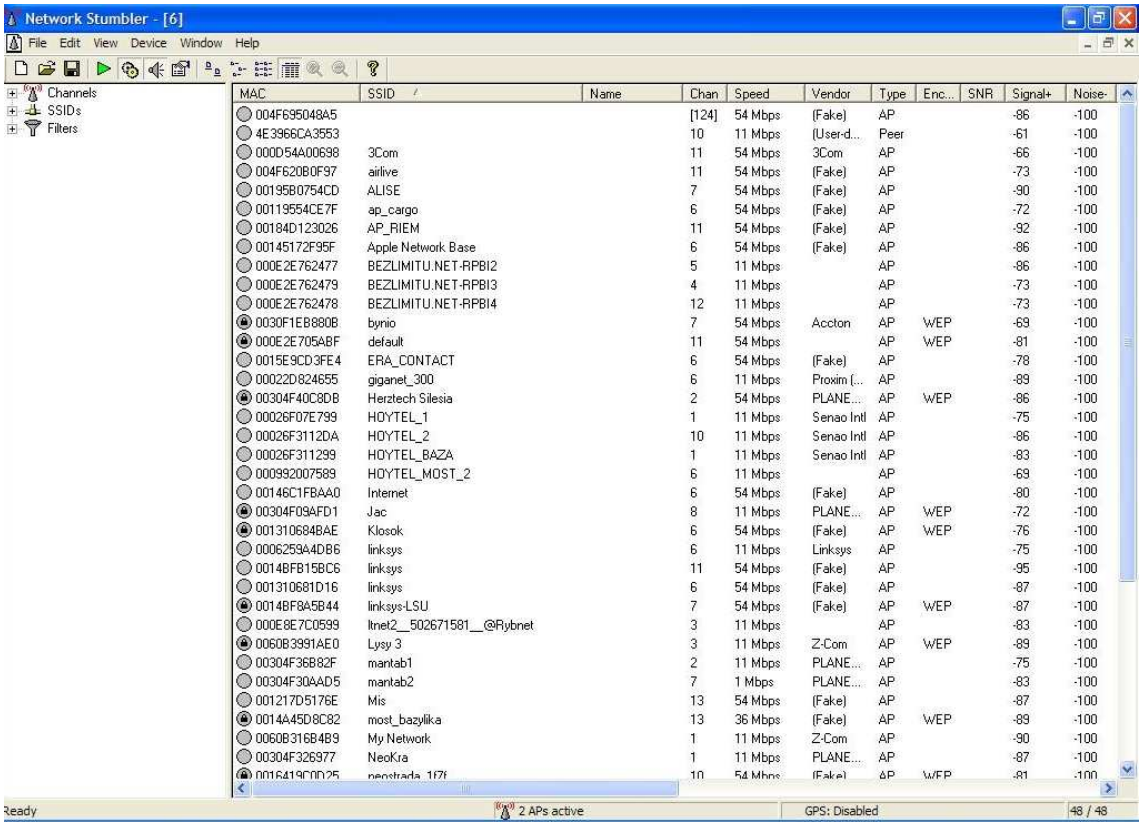
Dużą zasługą wysokiej popularności sieci bezprzewodowych jest także spadająca cena urządzeń oraz bogaty ich wybór. Można odnieść wrażenie, że nie ma miesiąca, w którym nie pojawiłby się na rynku nowy produkt rozwiązujący jakiś problem i udoskonalający komunikację w sieciach standardu 802.11. Kupując dzisiaj najtańszy punkt dostępowy, zapłacimy nieco ponad 100 zł, a cena bezprzewodowych kart sieciowych zaczyna się już od 50 zł wzwyż. Dzięki rozwojowi technicznemu i dużej konkurencji na rynku, ceny w dalszym stopniu będą obniżane a sieci Wi-Fi będzie przybywać coraz więcej.

Oprócz pokazanych zalet związanych z wykorzystaniem sieci bezprzewodowych mają one także wady. Nie da się określić zasięgu ich działania, ponieważ fale radiowe rozchodzą się we wszystkich kierunkach i mogą przenikać przez ściany. Z własnego doświadczenia wiem, że fale radiowe przechodzą nawet przez kilka ścian. Na przykład

sygnał z punktu dostępu umieszczonego na 3 piętrze w budynku dochodzi do mieszkań na parterze i pozwala na korzystanie z Internetu. Osoba nieupoważniona może podłączyć się do naszej sieci i znajdować się w miejscu, w którym najmniej się tego spodziewamy. Potencjalny włamywacz może być nawet oddalony o kilka bądź kilkanaście kilometrów, jeżeli tylko posiada antenę o dużym zysku. Ta właściwość sieci standardu 802.11 powoduje, że bardzo ciężko namierzyć intruza. Można to zrobić za pomocą specjalnych urządzeń korzystających z satelit GPS, ale rozwiązania te są bardzo drogie i mogą sobie pozwolić na nie jedynie wielkie firmy.

Rozdział II: Wardriving – badanie zabezpieczeń sieci Wi-Fi

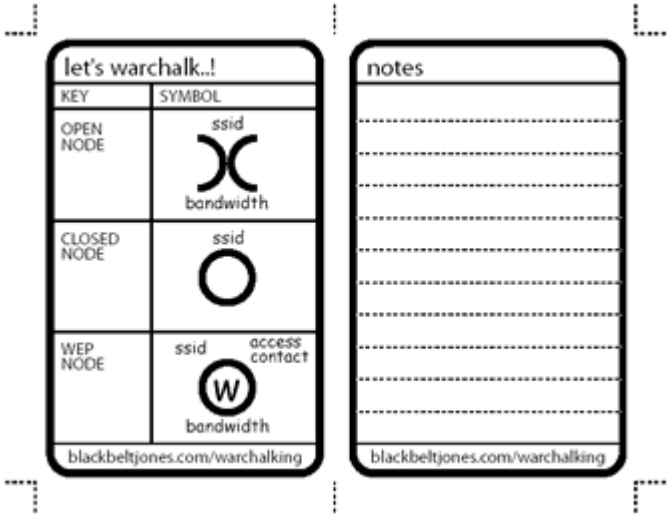
Wardriving to wyszukiwanie miejsc, w których dostępne są sieci bezprzewodowe. Do tego celu wykorzystuje się komputery przenośne (laptop lub palmtop) wyposażone w bezprzewodową kartę sieciową oraz antenę, najczęściej dookólną. Czynność ta polega najczęściej na jeżdżeniu samochodem z włączonym laptopem z zainstalowanym programem do wyszukiwania sieci. Najpopularniejszym programem tego typu jest używany przez większość wardriver'ów darmowy program NetStumbler. Wyszukuje on na bieżąco dostępne sieci bezprzewodowe podając bardzo przydatne informacje: nazwę SSID sieci, standard 802.11 b lub g, typ połączenia (infrastrukturalny lub ad hoc), siłę sygnału, poziom szumów oraz co chyba najważniejsze - poziom zabezpieczenia (brak lub WEP/WPA), jednak nie pokazuje czy zastosowano filtrację MAC



Rys. 3. Program NetStumbler w działaniu

Ilustracja własna.

Oprócz terminu wardriving używa się także warchalking i w zasadzie jest to to samo, tylko że do przemieszczania w tym wypadku zamiast samochodu wykorzystuje się siłę własnych nóg. Osoby wyszukujące sieci Wi-Fi oznaczają czasami miejsca, w których można uzyskać połączenie. Najczęściej rysowane są kredą charakterystyczne znaki, widoczne na rysunku poniżej. Pierwszy oznacza niezabezpieczoną sieć ogólnie dostępną, drugi – sieć zabezpieczoną filtracją MAC, a ostatni, że w sieci włączone jest szyfrowanie WEP lub WPA.



Rys. 4. Znaki warchalking'owe, źródło: www.wardriving.pl

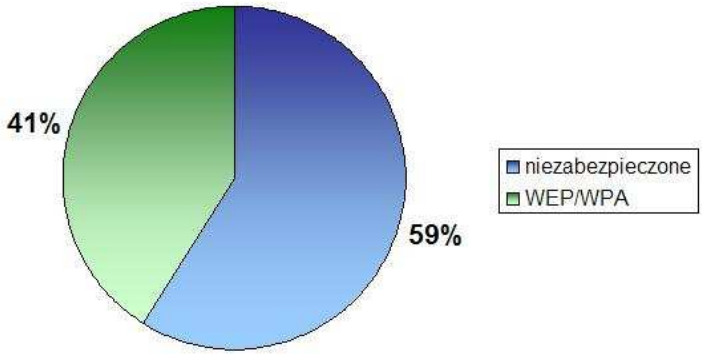
Prawo w Polsce jak i w większości krajach nawet nie wspomina o opisywanym zjawisku. Samo wyszukiwanie dostępnych sieci, nie jest zatem czynnością nielegalną. Korzystanie z sieci niezabezpieczonych w żaden sposób, też jest według prawa dozwolone. Do sieci takich może połączyć się każdy kto chce, a skoro nie ma jakichkolwiek zabezpieczeń to znaczy, że sieć jest udostępniona dla wszystkich.

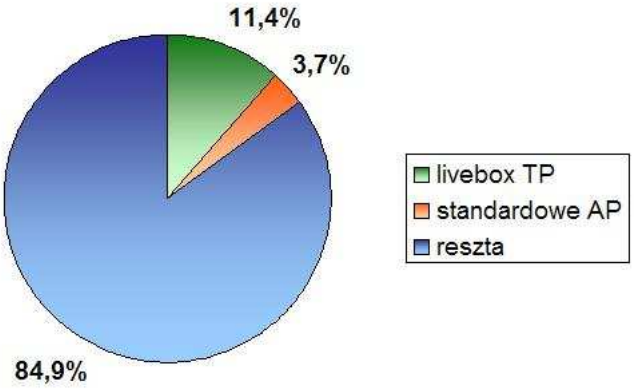
W czasie pisania mojej pracy spotkałem się z wieloma badaniami na temat poziomu zabezpieczeń sieci Wi-Fi. Wyniki tych badań były bardzo różne jednak jak by nie popatrzeć to ilość niezabezpieczonych sieci bezprzewodowych jest ogromna. Poniżej przedstawię wyniki niektórych ze znalezionych badań.

Miejsce	Rok	Ilość sieci	Niezabezpieczone	WEP lub WPA	Źródło
Los Angeles	2002	580	70 %	30 %	„Wi-Foo Sekrety Bezprzewodowych Sieci Komputerowych”
Paryż	2006	1000	29,5 %	70 %	Kaspersky Lab www.viruslist.pl
Londyn	2007	800	35 %	65 %	Kaspersky Lab www.viruslist.pl
Kraków	2007	1449	40 %	60 %	http://2007.confidence.org.pl

Jak widać niezabezpieczonych sieci jest bardzo dużo, nawet w Paryżu gdzie otrzymano najlepsze wyniki to na 1000 sieci około 300 z nich nie posiada żadnych zabezpieczeń. Podobne badania postanowiłem przeprowadzić na terenie mojego miasta i okolic. W trakcie mojej przygody z wardriving’iem korzystałem z laptopa HP nx6325 z wbudowaną kartą sieciową Broadcom 802.11a/b/g WLAN. Do wyszukiwania sieci Wi-Fi skorzystałem z opisanego już programu Netstumbler. Badania przeprowadzałem jadąc samochodem z włączonym komputerem umiejscowionym na fotelu pasażera. Trasa mojej przejażdżki prowadziła przez miasta: Rybnik, Gliwice, Katowice, Sosnowiec i Chorzów. Udało mi się zebrać w tym czasie dane na temat 747 sieci.

Spośród wszystkich sieci tylko 308 (41 %) było zabezpieczonych mechanizmem szyfrowania WEP lub WPA a 439 (59 %) nie posiadało żadnych zabezpieczeń.





Dużą grupę sieci znalezionych przeze mnie stanowiły punkty dostępu Livebox Telekomunikacji Polskiej. Każda z tych sieci ma unikalną nazwę SSID „neostrada_****”, przy czym pierwsza część nazwy jest zawsze taka sama a zamiast gwiazdek są różne znaki. Na uwagę zasługuje fakt, że większość z tych sieci była poprawnie zabezpieczona, tylko 4 spośród 85 znalezionych Livebox’ów nie posiadały zabezpieczeń. Spośród wszystkich 747 sieci aż 28 posiadało standardowe nazwy SSID (np. default, linksys, drink) i nie miały włączonego szyfrowania WEP/WPA. Mogę się domyślać, że login i hasło tych punktów dostępowych jak też adres IP były ustawione standardowo.

Jak widać wyniki moich badań trochę odbiegają od innych ale jest to spowodowane tym, że nie wziąłem pod uwagę filtracji MAC. Program Netstumbler wykrywa sieci, w których zastosowano filtrację adresów MAC jako niezabezpieczone. Z moich obserwacji i przeprowadzonych prób łączenia się z niezabezpieczonymi sieciami wynika, że filtrację MAC zastosowano w około 15 % sieci. Przy takim założeniu procent zabezpieczonych sieci wyniósłby nie 41, a 56 % natomiast z 59 do 44% zmniejszyłaby się ilość sieci niekorzystających z WEP lub WPA.

Wyniki moich badań w postaci pliku badanie.ns1 otwieranego za pomocą programu Netstumbler zamieściłem na płycie CD dołączonej do pracy.

Rozdział III: Zagrożenia wynikające z korzystania z sieci Wi-Fi

W starych dobrych czasach korzystanie z Internetu było przywilejem wąskiego grona osób, a wiele innych próbowało go zdobyć wszelkimi możliwymi sposobami. Powszechnym sposobem uzyskiwania nieautoryzowanego dostępu był wardialing, czyli dzwonienie pod numery telefonów z długiej listy z nadzieją natrafienia na sygnał modemu. Kiedy się to udało, należało „zgadnąć" nazwę użytkownika oraz hasło.[3]

Obecnie podobna technika wykorzystywana jest do poszukiwania sieci bezprzewodowych przez wardriver'ów. Wystarczy przejechać przez miasto z włączonym laptopem i z anteną dookólną, by znaleźć kilka bądź kilkadziesiąt sieci Wi-Fi. Podobnie tak jak kiedyś, by się połączyć, trzeba „zgadnąć" nazwę użytkownika oraz hasło, jednak w przypadku sieci bezprzewodowych uzyskanie połączenia jest o wiele łatwiejsze. Jak już napisałem wcześniej, wiele punktów dostępowych nie posiada żadnych zabezpieczeń i może się z nimi połączyć każdy, kto chce.

Zarówno w tym rozdziale jak i w dalszych będę często używał określeń haker oraz kraker w stosunku do osób, przed którymi należy zabezpieczyć sieć bezprzewodową. Pomiędzy tymi dwoma określeniami jest wielka różnica, jednak nie będę odchodził od tematu pracy i rozpisywał się nad historią użycia słowa haker. Instalując sieć Wi-Fi powinniśmy zabezpieczyć ją przed wszystkimi osobami chcącymi skorzystać z nieautoryzowanego dostępu do łącza niezależnie od tego, jakie mają zamiary.

[3] „Wi-Foo Sekrety bezprzewodowych sieci komputerowych" - Andrew Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky

3.1 Ataki i włamania do sieci

3.1.1 Podsłuch

Jeśli zainstalowaliśmy sieć Wi-Fi bez żadnych mechanizmów bezpieczeństwa, znajdujący się pobliżu haker może bez problemu skorzystać z połączenia internetowego – może przeglądać strony internetowe albo sprawdzać pocztę. Nie jest to jednak działalność zbyt szkodliwa, ale może być uciążliwa. Oprócz tego osoba nieuprawniona może w łatwy sposób przechwycić wysyłane i odbierane dane. Przechwytywanie pakietów przypomina podsłuchiwanie rozmów telefonicznych. Napastnik wyposażony w laptop lub palmtop z obsługą sieci Wi-Fi, może za pomocą programu do przechwytywania pakietów obserwować dyskretnie ruch sieciowy i rejestrować niektóre lub wszystkie przesłane dane w pliku dziennika a następnie w wolnej chwili je przeanalizować. W sieciach kablowych chcąc podsłuchiwać przesyłane informacje trzeba zainstalować program bezpośrednio na interesującym komputerze lub być podłączonym do tej samej sieci LAN.

Sieci bezprzewodowe działające za pośrednictwem fal radiowych otwierają programom przechwytującym pakiety cały wszechświat możliwości. Rozprzestrzenianie się fal radiowych nie ogranicza się tylko do takiego medium jak kabel, w związku z tym wszędzie tam, gdzie docierają sygnały radiowe emitowane przez sieci Wi-Fi, program przechwytujący może je podsłuchiwać bez niczyjej wiedzy. Napastnik nie musi być nawet podłączony do tej samej wewnętrznej sieci, jak to ma miejsce w sieciach kablowych. Stanowi to poważne zagrożenie przede wszystkim wtedy, gdy sygnały sieci bezprzewodowej docierają do miejsc, o których nie wiemy lub nie mamy nad nimi kontroli. Jeśli biura firmy znajdują się na przykład w biurowcu na 10 piętrze, osoby znajdujące się piętro wyżej i piętro niżej najprawdopodobniej mogą odbierać sygnały naszej sieci i przechwytywać pakiety a my nie mamy żadnych możliwości, by się o tym choćby dowiedzieć. Jeżeli posiadamy w domu prywatną sieć lub dostęp do Internetu za pomocą sieci Wi-Fi to osoba mieszkająca w budynku obok, może za pomocą anteny o dużym zysku skierowanej na nasz dom podsłuchiwać przesyłane przez nas dane. Jeszcze gorszą rzeczą jest tzw. manipulacja danymi,

włamywacz może przechwytywać i zmieniać wysyłane lub odbierane przez nas wiadomości.

Aby uniemożliwić hakerom uzyskania poufnych informacji, jakie są przesyłane przez sieci standardu 802.11, należy zaimplementować wiele warstw szyfrowania, co pozwoli na ukrycie danych. Do tego celu należy wdrożyć mechanizmy zabezpieczeń WEP, WPA oraz można użyć wielu technologii, takich jak IPSec, SSH lub SSL. Sposób działania i siłę zabezpieczeń tych technologii przedstawię w dalszej części pracy.

3.1.2 Podszywanie się pod adres IP

Spośród wielu różnych ataków, które może przeprowadzić napastnik najgorszy jest atak o nazwie podszywanie się pod adres IP. W odróżnieniu od ryzyka, że ktoś na przykład podejmie atak typu DoS w stosunku do naszego systemu, ryzyko podszywania się pod adres IP jest dość duże, a nawet poważne. Atak ten wykorzystywany jest często przez osoby chcące zachować anonimowość. Podszywanie się pod inny adres IP jest swego rodzaju kradzieżą tożsamości. Haker korzystający z obcego adresu IP może robić jakieś nieetyczne lub nielegalne operacje, na przykład wysyłać spam lub przesyłać pliki z dziecięcą pornografią. Jeżeli organom ścigania uda się dotrzeć do miejsca, z którego wysyłano dokumenty to odpowiedzialność spadnie na niewinną osobę, pod którą podszył się haker.

W celu lepszego zobrazowania zagrożenia przedstawię przykład osoby wysyłającej spam. Spamer korzystając z laptopa i anteny o dużym zysku może znajdować się nawet kilka kilometrów od naszej sieci. Jeżeli sieć nie jest zabezpieczona lub jest, ale w słabym stopniu, napastnik podłączy się i może podszyć się pod nasz adres IP. Korzystając z programu wysyłającego pocztę elektroniczną rozsyła na cały świat dziesiątki tysięcy listów na godzinę, a każdy z tych listów będzie posiadał nasz adres IP. Jeżeli sprytny napastnik będzie wysyłał spam o drugiej w nocy, kiedy wszyscy śpią, natomiast komputery i połączenie komputerowe są wolne, to jest duża szansa, że nawet się nie zorientujemy, co się wydarzyło. Prawdopodobnie dowiemy się o tym dopiero następnego dnia, kiedy to dostawca usług internetowych odetnie nam dostęp z powodu rozsyłania spamu.

Jeśli nasz adres IP zamiast do rozsyłania „śmieci” posłużył do przesłania pornografii lub do kradzieży poufnych danych, to wtedy zamiast braku Internetu o poranku, może zapukać do drzwi policja, a udowodnienie im, że to nie my wykonaliśmy atak może być trudniejsze niż zdobycie wszystkich szczytów ośmiotysięczników. Nawet, jeżeli ktoś dostrzeże w pobliżu sieci, z której dokonano przestępstwa osobę z laptopem i dodatkową anteną, organy ścigania będą miały duży problem z odnalezieniem tej osoby i udowodnieniem, że to akurat ona dokonała tego przestępstwa. Jeśli przed atakiem napastnik zmienił adres MAC swojej bezprzewodowej karty sieciowej, a po ataku usunął z komputera wszystkie dane i narzędzia do wykonania ataku to dowiedzenie jego winy będzie praktycznie niemożliwe. Jeżeli by nawet udało się nam złapać napastnika na gorącym uczynku, to zdąży on się rozłączyć z siecią, a do czasu przyjazdu policji już go pewnie nie będzie. Może normalnie odejść, sami nie mamy prawa go zatrzymać. W sieciach przewodowych wykonanie takich nielegalnych operacji jest znacznie trudniejsze, dlatego też powinniśmy zadbać by zabezpieczyć sieć Wi-Fi przed zagrożeniami pochodzącymi z różnych stron.

3.2 Nieświadomość administratorów o zagrożeniach

Wiele osób opiera się na nieprawdziwym przekonaniu, że tylko wielkie firmy narażone są na ryzyko płynące ze strony hakerów i krakerów. Jest to mit, jednak szeroko rozpowszechniony. Oczywiście duże firmy to miejsca, w których znajdują się największe pieniądze i najbardziej poufne dane, jednak każdy doświadczony napastnik myśli najpierw o swoim bezpieczeństwie i grożących mu konsekwencjach prawnych, dlatego zawsze na początek wybiera sobie cele łatwiejsze. Poza tym kraker bez żadnych doświadczeń rozpocznie od włamania się do czegokolwiek, bez zwracania uwagi na to czyja to sieć i do czego służy.

Wielkie firmy zwykle posiadają dobrze wyszkolony personel odpowiedzialny za bezpieczeństwo, dobrą i przestrzeganą politykę bezpieczeństwa oraz narzędzia wzmacniające bezpieczeństwo, co oczywiście zwiększa szansę wykrycia napastnika. Z drugiej strony wielkie firmy są bardziej podatne na powstawanie luk w bezpieczeństwie

spowodowanych przez instalowanie w ich sieciach niedozwolonych urządzeń bezprzewodowych oraz są znacznie bardziej podatne na ataki socjotechniczne.

W przypadku mniejszych firm lub sieci domowych wiele ataków nie zostaje wykrytych lub są wykrywane za późno.

Powody, dla których krakerzy interesują się sieciami niewielkich firm oraz sieciami domowymi, zostały już szczegółowo omówione i są oczywiste dla każdego, kto interesuje się bezpieczeństwem systemów informatycznych. Są to: anonimowy dostęp, małe prawdopodobieństwo wpadki, darmowe pasmo oraz łatwość włamania się. Oto problemy związane z bezpieczeństwem, z którymi borykają się niewielkie firmy:

- Przepracowany administrator słabo znający się na sieciach bezprzewodowych albo częsta nieobecność w pracy jedynego wykwalifikowanego administratora.
- Użycie prostych, tanich urządzeń sieci bezprzewodowych z ograniczonymi funkcjami bezpieczeństwa (jeżeli firma nie korzysta z rozwiązań open source może mieć tylko to, na co ją stać).
- Brak scentralizowanego serwera uwierzytelniania.
- Brak bezprzewodowego systemu IDS oraz centralnego rejestru zdarzeń.
- Brak polityki korzystania z sieci bezprzewodowej.
- Brak środków na zlecenie profesjonalnego audytu sieci bezprzewodowej.

3.3 Zagrożenia fizyczne

Zagrożenia związane z funkcjonowaniem sieci standardu 802.11 nie sprowadzają się tylko do ataków hakerów i ludzi chcących skorzystać z naszego łącza. Zakładając sieć bezprzewodową musimy wziąć pod uwagę także zmienne warunki atmosferyczne. Istnieją trzy czynniki, które mogą przerwać łączność a nawet uszkodzić urządzenia sieciowe i każdy z nich jest w takim samym stopniu niebezpieczny. Chodzi tu o wiatr, opady deszczu lub śniegu i temperaturę.

Mocne podmuchy wiatru mogą zniszczyć anteny a także maszty, jeśli są niesolidnie zrobione. Kolejnym niebezpieczeństwem dla sprzętu są opady deszczu oraz

śniegu. W tym wypadku najbardziej narażone są punkty dostępu umieszczone na zewnątrz, nieznajdujące się w dobrze zabezpieczonych skrzynkach. W momencie pojawienia się dziury lub szpary, przez którą woda dostałaby się do środka można być raczej pewnym, że po solidnych opadach deszczu urządzenia zostaną zalane i nasza sieć przestanie działać. Dotyczy to także anten zamkniętych w tubach (yagi). Jeśli do środka dostanie się spora ilość wody to może w znaczącym stopniu zakłócić sygnał, ponieważ woda nie przepuszcza fal radiowych. Jeśli chodzi o temperaturę to sprawa dotyczy tylko punktów dostępu, latem urządzenia wystawione na działanie promieni słonecznych mogą przegrzać się i odmówić działania. W zimie także duży spadek temperatury może powodować zmiany w działaniu tych urządzeń.

Przed niszczącym działaniem pogody na sprzęt sieciowy można się w bardzo łatwy sposób zabezpieczyć, ale o tym później. Jeśli wszystkie urządzenia sieci WLAN znajdują się w budynku to wtedy żadne z wymienionych wyżej zagrożeń fizycznych nie dotyczą.

Rozdział IV: Bezpieczeństwo sieci bezprzewodowych

Pierwszą i najważniejszą czynnością, jaką powinno wykonać się po uruchomieniu sieci Wi-Fi jest zmiana standardowych ustawień punktu dostępu: nazwa użytkownika, hasło, identyfikator SSID oraz numer IP punktu dostępu. Pozwoli to na zabezpieczenie sieci przed bezpośrednimi atakami na nasz access point. Nazwa użytkownika oraz hasło musi być unikalne i złożone, by nie można było go złamać atakami brute force. Jeżeli ustawimy słabe hasło to nawet przy zastosowaniu najbezpieczniejszego szyfrowania WPA2, kraker chcący włamać się do naszej sieci może mieć bardzo łatwe zadanie.

Aby dobrze zabezpieczyć się przed atakami siłowymi, hasło powinno być długie i składać się z liter, liczb i znaków. Jedynym problemem, jaki może tu wystąpić jest trudność zapamiętania takich haseł. Żeby sobie to ułatwić, proponuję zastosować jeden z przykładów przedstawionych poniżej.

Pierwszym sposobem na zapamiętanie hasła jest wymyślenie jakiejś frazy i zamienienie kilku liter na cyfry, na przykład: mając wybrane hasło „onstoiipatrzy” można przekształcić je na „0n100iipa3”. Łatwe do zapamiętania i trudne do złamania.

Drugim sposobem, który także polecam jest zaszyfrowanie wybranej frazy prostym szyfrem. Można przesunąć każda literę alfabetu o 2 pozycje w lewo, wtedy łatwe hasło „marcin” stanie się niezrozumiałym ciągiem liter „octekp”.

Identyfikator SSID także powinien zostać zmieniony w taki sposób by napastnik nie mógł w stanie określić, do kogo ta sieć należy. Nie zaleca się stosowania w nazwie imion i nazwisk oraz nazw firm, zamiast tego można zastosować skróty. Na przykład, gdy w firmie Energo-Elektro zostanie zainstalowany punkt dostępu, sieć można nazwać wifiee1 zamiast rzucającego się w oczy SiecEnergoElektro.

Adres IP punktu dostępu także powinien zostać zmieniony, ochroni to przed atakami z wewnątrz sieci. Domyślne ustawienia urządzeń są łatwo dostępne w Internecie i każdy może znaleźć informację, pod jakim numerem IP kryje się dany access point. Aby uniemożliwić łatwy dostęp takim użytkownikom wystarczy zmienić adres na inny.

4.1 Ukrycie SSID

W sieciach bezprzewodowych każdy punkt dostępowy rozsyła dookoła swoją nazwę gdzie tylko się da. Jej znajomość umożliwia nawiązanie połączenia z siecią, jednak w przypadku, kiedy nie znamy SSID połączenie nie jest możliwe, a więc potencjalny włamywacz nie może uzyskać dostępu do sieci.

Właśnie dlatego już w pierwszych Access Pointach wprowadzono możliwość wyłączenia rozgłaszania nazwy sieci. Być może zabezpieczenie to w przeszłości było skuteczne, jednak dziś zdobycie SSID sieci nie stanowi żadnego problemu. Potencjalny włamywacz może uruchomić program NetStumbler i poczekać aż jeden z klientów nawiąże połączenie z siecią, wtedy bowiem wysyła on czystym tekstem SSID ukrytej sieci.

Ominięcie ukrycia nazwy SSID to kwestia kilku minut, dlatego nie powinno się stosować tego zabezpieczania bez wsparcia innymi, lepszymi metodami autoryzacji.

4.2 Filtracja MAC

Ten rodzaj zabezpieczenia zapewnia większość punktów dostępowych. Funkcję filtrowania adresów MAC można skonfigurować tak, aby tylko wybranym użytkownikom udzielić dostępu do sieci. Można zastosować ją także w drugą stronę: możliwość korzystania z sieci bezprzewodowej mają wszyscy oprócz wybranych użytkowników. Mechanizm ten polega na zapisywaniu do tablicy adresów MAC bezprzewodowych kart sieciowych, które mają (nie mają) mieć dostęp do sieci.

Podobnie jak ukrywanie nazwy SSID, filtracji MAC nie powinno stosować się jako jedyne zabezpieczenie, bowiem za pomocą odpowiednich narzędzi w łatwy sposób można zmienić adres MAC karty sieciowej i podszyć się pod innego użytkownika.

4.3 WEP

Podstawowym środkiem bezpieczeństwa zalecanym przez standard 802.11 jest protokół warstwy łącza danych WEP (ang. Wired Equivalent Privacy), który – zgodnie z nazwą – zapewnić ma sieci bezprzewodowej bezpieczeństwo nie gorsze niż na poziomie standardowego bezpieczeństwa przewodowej sieci LAN.[4] Standardowym poziomem bezpieczeństwa w sieciach przewodowych jest brak jakichkolwiek mechanizmów zabezpieczających, więc zadanie postawione przed protokołem WEP nie jest specjalnie wygórowane i pomimo że w 2001 roku opublikowano już sposób jego złamania to i tak jest on wykorzystywany w większości sieci.

WEP jest to wbudowany program zarówno w punkty dostępu jak i we wszystkie karty sieciowe radiowe. Mechanizm WEP zabezpiecza dane przesyłane w sieci bezprzewodowej, szyfrując to, co przechodzi między bezprzewodowymi punktami dostępu a bezprzewodowymi kartami sieciowymi. Osoba z zewnątrz próbująca się podłączyć do naszej sieci, wyposażona w program do przechwytywania pakietów zamiast konkretnych informacji ujrzy tylko niezrozumiały ciąg liter i znaków. Urządzenia zgodne ze standardem Wi-Fi muszą mieć zainstalowaną kompatybilną postać szyfrowania WEP. Niektórzy producenci sprzętu sieciowego rozszerzają standard WEP po to, by uczynić go bardziej niezawodnym, jednak z powodu niezgodności tych rozszerzeń z innymi, nie zawsze wychodzi to na dobre.

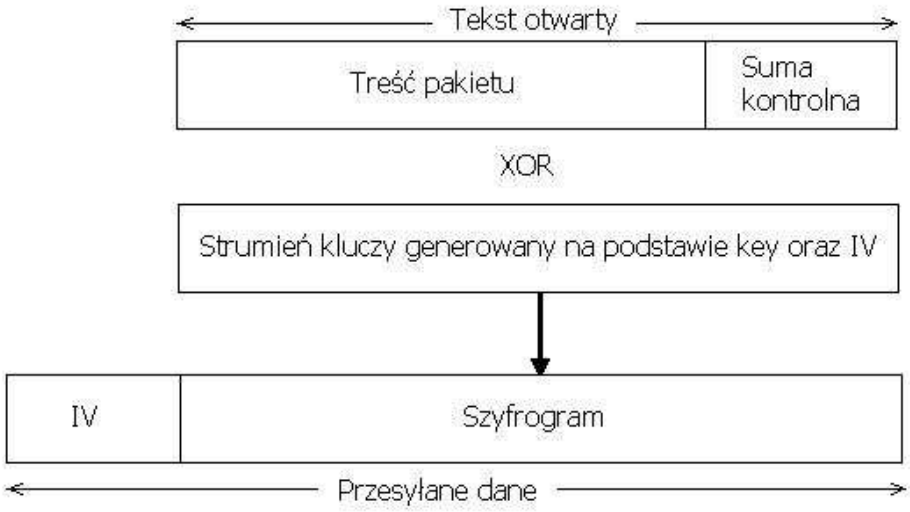
4.3.1 Zasada działania

Szyfrowanie w mechanizmie WEP odbywa się w oparciu o szyfr strumieniowy RC4 znany też jako ARC4 lub ARCFOUR. Algorytm RC4 został opracowany przez Ronalda Rivesta w 1987 roku i pozostawał utrzymany w tajemnicy aż do roku 1994, kiedy to został opublikowany w Internecie na jednej z grup dyskusyjnych. Algorytm generuje strumień kluczy, który jest poddawany operacji XOR z zawartością tekstu wejściowego. Algorytm ten oprócz sieci bezprzewodowych stosowany jest w wielu innych produktach, takich jak Lotus, Oracle a także SSL i SSH. Algorytm RC4 dla

[4] „Sieci komputerowe” – Andrew S. Tanenbaum

szyfrowania WEP wybrany został z tego powodu, że jest stosunkowo prosty i szybki w działaniu i nie spowalnia działania sieci w taki sposób jak inne bardziej skomplikowane algorytmy.

Sposób, w jaki odbywa się szyfrowanie każdego pakietu najlepiej przedstawia ilustracja zawarta w książce Andrew S. Tanenbaum'a.



Rys. 5. Zasada działania mechanizmu WEP,
źródło: „Sieci komputerowe" - Andrew S. Tanenbaum – str 695

Z punktu widzenia użytkownika, działanie mechanizmu WEP jest w miarę proste. Na początku trzeba wygenerować cztery różne klucze szyfrowania. W przypadku standardowego szyfrowania 64-bitowego, które może być zastosowane na wszystkich urządzeniach Wi-Fi, każdy z kluczy to dziesięciocyfrowa liczba szesnastkowa. Klucz można utworzyć wybierając na przykład na chybił trafił dziesięć przypadkowych cyfr szesnastkowych (cyfry od 0 do 9 oraz litery od A do F). Wygenerowany w ten sposób klucz, będzie wyglądał mniej więcej tak: 52A45C914F. W większości nowych punktach dostępu znajduje się program, który umożliwia generowanie tych czterech kluczy na podstawie wprowadzonej frazy będącej pewną sekwencją liter lub wyrazów, takich jak na przykład: „Ala ma kota" lub „sierotka ma rysia". Dla danej karty sieciowej oraz punktu dostępu ta sama fraza zawsze spowoduje

wygenerowanie tych samych czterech kluczy szyfrowania. Można spotkać także urządzenia, które generują z frazy tylko jeden klucz a nie cztery.

Następnie użytkownik musi dystrybuować te cztery klucze (lub jeden klucz, jeśli w danej instalacji sieciowej potrzebny jest tylko jeden klucz) do wszystkich bezprzewodowych kart sieciowych, które będą się łączyć z punktem dostępu. Proces ten, czyli dystrybucja kluczy jest krytyczną operacją dotyczącą bezpieczeństwa sieci Wi-Fi. Trzeba pamiętać, że należy wpisać czterdzieści cyfr szesnastkowych z absolutną dokładnością. Nie może być żadnej pomyłki. Sytuacja wygląda lepiej, gdy proces ten może być zastąpiony wpisaniem tej samej frazy do programu narzędziowego uruchamianego na wszystkich komputerach klienckich. Trudności z dystrybucją kluczy zostały w dużej mierze rozwiązane w protokole WPA, ale o tym później.

Gdy wszystkie punkty dostępu oraz wszystkie bezprzewodowe karty sieciowe znajdujące się w sieci mają już wprowadzone wszystkie cztery klucze, to można włączyć mechanizm szyfrowania WEP. Od tej chwili cały ruch sieciowy między punktem dostępu a bezprzewodowymi kartami sieciowymi będzie szyfrowany. Po uruchomieniu szyfrowania WEP nie trzeba już wykonywać żadnych innych operacji związanych z tym mechanizmem, aż do chwili podjęcia decyzji o zmianie kluczy. Najlepiej zmieniać klucze jak najczęściej, ponieważ jak przedstawię niżej, szyfrowanie WEP jest bardzo słabym zabezpieczeniem, a częsta zmiana kluczy może trochę to bezpieczeństwo podnieść.

4.3.2 Wady protokołu WEP

Słabość mechanizmu WEP opisał bardzo dokładnie Jeff Duntemann w książce „Przewodnik po sieciach Wi-Fi”:

„(…)liczby pseudolosowe, które tworzą strumień klucza, są generowane za pomocą 24-bitowej liczby początkowej używanej przez komputer do generowania liczb losowych. Liczbę tę nazywa się wektorem inicjalizacji (IV) – initializator vector. Wartość wektora inicjalizacji jest przesyłana wraz z każdą zaszyfrowaną ramką w sposób bezpośredni i niezaszyfrowany, w związku z czym haker może przejrzeć dwie zaszyfrowane ramki i zorientować się, czy zostały one zaszyfrowane za pomocą tego samego wektora inicjalizacji czy nie. Standardowo każda przesyłana ramka jest

szyfrowana za pomocą innego wektora inicjalizacji. Problem polega jednak na tym, że istnieje tylko 16777216 różnych możliwych wartości wektora inicjalizacji. Na pierwszy rzut oka mogłoby się wydawać, że jest to duża liczba. Jeśli jednak mamy do czynienia z siecią Wi-Fi, która jest w stanie przesłać dane z szybkością 11Mbps, to w przypadku ciągłego i intensywnego ruchu sieciowego można wykorzystać wszystkie wartości wektora inicjalizacji już po około 6 godzinach. Po wykorzystaniu wszystkich wartości większość obecnie sprzedawanych urządzeń typu Wi-Fi resetuje wartość wektora inicjalizacji do zera i ponownie rozpoczyna przesyłanie danych w eter za pomocą drugiego zestawu 16777216 ramek, dzięki czemu cierpliwy haker ma w tym momencie dostęp do pełnego drugiego zestawu ramek zaszyfrowanego za pomocą tych samych współczynników wektorów inicjalizacji." Po kilku godzinach wysyłany jest trzeci zestaw ramek, i tak w kółko. Tym sposobem złamanie zabezpieczenia WEP zajmuje hakerowi kilka lub kilkanaście godzin.

„Gwoździem do trumny" technologii WEP jest obecność słabych wartości wektora inicjalizacji. „Z powodu pewnych własności matematycznych algorytmu około 2% wszystkich 16777216 wartości wektora inicjalizacji są to wartości, które mogą być „zdrajcami". Powodują one wyciekanie pewnych informacji związanych z szyfrowanymi przez nie danymi. Wartość wektora inicjalizacji każdej ramki dołączona jest do ramki i to w postaci niezaszyfrowanej! Umożliwia to programom służącym do łamania haseł, takim jak na przykład AirSnort, wyszukiwanie słabych wartości wektora inicjalizacji, a następnie zbieranie i gromadzenie pakietów zaszyfrowanych za pomocą tych wartości aż do momentu, gdy zbierze się ich wystarczająca liczba, by można było przeprowadzić łamanie hasła. Wykorzystanie słabych wartości wektorów może skrócić czas potrzebny na złamanie mechanizmu WEP w sposób dramatyczny." Czas ten mierzony już jest nie w godzinach, ale w minutach.

Istnieją także inne słabe punkty, które powodują, że złamanie zabezpieczenia WEP staje się szybsze i łatwiejsze. W przypadku niektórych kart bezprzewodowych ponowna ich inicjalizacja powoduje zresetowanie sekwencji wektora IV do zera. Jeżeli karta sieciowa będzie regularnie inicjalizowana, to o wiele częściej będą występować wektory IV o niskich wartościach niż o wartościach wysokich. Wzrasta przez to szansa, że haker zbierze więcej pakietów zaszyfrowanych za pomocą tych samych wektorów inicjalizacji.

Drugim sposobem atakowania mechanizmu WEP jest brutalny atak siłowy. Napastnik może za pomocą programów „zgadywać" hasło lub skorzystać z ataku

słownikowego. Na szczęście przed takim atakiem można się łatwo zabezpieczyć, wystarczy stosować mocne hasła, o których pisałem już na początku rozdziału IV.

4.3.3 Firmowe rozszerzenia protokołu

Po wykryciu niedoskonałości mechanizmu WEP firmy produkujące sprzęt Wi-Fi zaczęły rozszerzać standardowy protokół. Pierwszą reakcją wielu producentów było zwiększenie długości klucza do 128 i więcej bitów (tak zwany WEP2), jednak rozwiązanie to nie zwiększało przestrzeni wektorów inicjalizacyjnych IV i jedynie utrudniło przeprowadzenie ataków siłowych. Pierwszym skutecznym rozwiązaniem tego problemu była najprawdopodobniej propozycja firmy RSA, indywidualnego kodowania każdego pakietu oraz wyeliminowania pierwszych bajtów strumienia klucza. Mechanizm ten nazwano WEPPlus i został on zastosowany przez firmę Proxim w niektórych punktach dostępowych i kartach bezprzewodowych Orinoco. Firma Cisco wprowadziła rozwiązanie o nazwie SAFE, które polega na cyklicznej wymianie kluczy i jest konfigurowane za pomocą centralnego serwera kontroli dostępu. Wymiana kluczy następuje w sposób niewidoczny dla użytkownika dzięki mechanizmowi CCKM.

Oferowane od sierpnia 2005 roku oprogramowanie McAfee Wireless Home Network Security zmieniało automatycznie klucze WEP co 3 godziny. Program ustawiał nowe klucze szyfrowania zarówno w komputerze jak i w punkcie dostępu, i współpracował z większością dostępnych na rynku routerów Wi-Fi.[5]

Firmowe rozszerzenia protokołu WEP miały jedną wielką wadę, urządzenia jednej firmy nie działały ze sprzętem sieciowym innych firm. Aby zabezpieczenia takie mogły zadziałać, cała sieć musiała być stworzona z urządzeń tylko jednej firmy.

[5] Networld nr 9/2005 str 19

4.3.4. Dlaczego stosuje się WEP

Pomimo, iż szyfrowanie WEP może zostać łatwo i szybko złamane to może się okazać, że jest to jedyne zabezpieczenie, jakie można zastosować. Dotyczy to starszego sprzętu sieciowego, który nie obsługuje niczego innego poza WEP. Poza tym zawsze lepiej ze słabym zabezpieczeniem niż z żadnym, gdy ktoś będzie chciał skorzystać z czyjegoś łącza a mając do dyspozycji wiele sieci w okolicy, wybierze sieć, która nie posiada żadnych zabezpieczeń.

Istnieje wiele powodów, dla których zabezpieczenie WEP będzie jeszcze długo stosowane niezależnie od tego jak bezpieczne będą rozwiązania w przyszłości.

- Mechanizm WEP jest obsługiwany przez każde urządzenie standardu 802.11.
- Jest łatwy w konfiguracji.
- Nowe urządzenia będą wybierały taki poziom zabezpieczeń, który umożliwi ich współpracę ze starszym sprzętem.
- Wiele osób nadal twierdzi, że WEP stanowi wystarczające zabezpieczenie.

4.4. WPA

Po złamaniu mechanizmu szyfrowania WEP w sierpniu 2001 roku, stowarzyszenie Wi-Fi Alliance zmuszone zostało do szybkiego stworzenia innego protokołu szyfrującego pozwalającego na lepsze zabezpieczenie sieci bezprzewodowych. W tym czasie opracowywany był już standard 802.11i ale był on dopiero w trakcie projektowania i trzeba było znaleźć szybsze rozwiązanie. Nowy mechanizm miał być pozbawiony wszystkich błędów z WEP oraz musiał współpracować z urządzeniami już wyprodukowanymi. Przy projektowaniu nowego mechanizmu zabezpieczeń, skorzystano z niektórych rozwiązań technicznych wykorzystanych we wcześniejszym WEP, a także z nowych pomysłów standardu 802.11i. Po kilku miesiącach pracy narodził się nowy standard nazwany WPA (Wi-Fi Protected Access)

4.4.1 Zasada działania mechanizmu WPA

Mechanizm WPA rozwiązuje prawie wszystkie problemy występujące w WEP:

- Została wydłużona długość kluczy szyfrowania w stosunku do WEP z 40 do 128 bitów. Dzięki czemu brutalny atak siłowy na klucze stał się praktycznie nie możliwy.
- Standard WPA także korzysta z algorytmu RC4, jednak klucze szyfrowania w standardzie WPA zmieniane są regularnie i w sposób automatyczny. Dla większego bezpieczeństwa, wymiana ta przebiega w zaszyfrowany sposób.
- Klucze zmieniane są bardzo często, dzięki czemu napastnik nie będzie w stanie przechwycić wystarczającej liczby pakietów, tak jak miało to miejsce w WEP, by odszyfrować wartość klucza.
- Zwiększono długość wektora IV z 24 do 48 bitów. Dostępnych jest teraz 281 trylionów różnych wartości inicjalizacji. Jak pisałem w poprzednim rozdziale, w mechanizmie WEP możliwych było niecałe 17 milionów wartości, jest to więc różnica kolosalna.
- W WPA zastosowany został mechanizm uwierzytelniania wzajemnego, dzięki czemu jest on odporny na ataki typu „człowiek w środku".
- Zastosowano technologię MIC (Michael), która ma na celu uniemożliwienie napastnikowi przechwycenia pakietów z danymi. MIC posługuje się ściśle określoną funkcją matematyczną, przy pomocy której zarówno nadajnik jak i odbiornik liczą, a następnie porównują wyniki. Przy braku zgodności przyjmuje się, że miała miejsce próba przejęcia danych i pakiet taki zostaje odrzucony.

Mechanizm WPA został zaprojektowany tak, by spełniać wymagania zarówno dużych jak i małych sieci. Projektanci wzięli pod uwagę fakt, że nie wszystkie sieci są podobne do siebie – wielkie i rozległe sieci mają inne wymagania niż sieci składające się z kilku użytkowników. W obu tych przypadkach mechanizm ten działa zupełnie inaczej. W dużych, centralnie zarządzanych sieciach WPA obsługuje uwierzytelnianie oraz wymianę kluczy za pomocą serwera RADIUS. Jest to serwer, który zarządza centralnie uwierzytelnianiem w sieci oraz dystrybucją kluczy szyfrowania.

Z tego powodu mechanizm WPA można podzielić na dwa rodzaje:

1. Personal, który opiera się na kluczu PSK, stąd nazwa WPA-PSK, do zastosowań domowych
2. Enterprise, korzystający z serwera RADIUS, do zastosowań profesjonalnych

Uwierzytelnianie w sieciach Wi-Fi może się odbywać na wiele różnych sposobów ujętych w standardzie 802.1x. W wielkich sieciach firmowych rozproszonych w wielu miejscach system 802.1x może być bardzo skomplikowany, a jego wdrożenie może zająć nawet kilkanaście dni. Dokładniej temat uwierzytelniania opiszę w dalszej części pracy.

W małych sieciach składających się z jednego punktu dostępu protokół uwierzytelniania 802.1x jest również wykorzystywany, jednak nie ma w nich serwera RADIUS, dzięki temu cały system jest mniej skomplikowany. Brak serwera odpowiedzialnego za dystrybucję kluczy może okazać się problemem dla administratora lub właściciela sieci. Musi on bowiem ręcznie wprowadzić klucz szyfrowania do wszystkich urządzeń Wi-Fi korzystających z sieci. Wprowadzony klucz pozostaje zapisany w pamięci urządzenia i jest on nazywany kluczem wstępnie przydzielonym PSK (ang. pre-shared key). Czynność ta wykonywana jest w taki sam sposób jak w mechanizmie WEP, trzeba wpisać 32 cyfry szesnastkowe lub frazę, na podstawie której generator utworzy odpowiedni klucz.

Wielką wadą szyfrowania WEP był fakt, że ludzie zmieniali klucze bardzo rzadko, a niekiedy nawet wprowadzone klucze nie były zmieniane nigdy. Było to spowodowane problemem związanym z wpisywaniem do każdego urządzenia nowych kluczy, wszystkie trzeba wpisać ręcznie, co w przypadku większej sieci stanowiło spory problem. Przy stałej wartości klucza osoba nieuprawniona do korzystania z sieci mogła w dość krótkim czasie zebrać odpowiednią ilość pakietów by złamać zabezpieczenie WEP. Pomysł leżący u podstaw mechanizmu WPA, polegał na regularnej automatycznej zmianie kluczy wykonywanej, co pewien stały, określony przez administratora czas. Za zmianę kluczy odpowiedzialny jest protokół TKIP (ang. Temporal Key Integrity Protocol).

TKIP powiększa rozmiar klucza z 40 do 120 bitów oraz podmienia pojedynczy klucz statyczny WEP kluczami generowanymi dynamicznie i rozprowadzanymi przez serwer identyfikacyjny. TKIP stosuje metodologię hierarchii i zarządzania kluczami,

pozbawiającą intruzów możliwości przewidywania, który klucz WEP nadaje się do wykorzystania. Hierarchia kluczy TKIP pozwala na wymianę pojedynczego klucza WEP na około 500 miliardów możliwych kluczy dających się użyć do danego pakietu danych.[6]

Jeżeli przedział czasu odnawiania klucza zostanie wyznaczony zgodnie z intensywnością ruchu w sieci to napastnik nie będzie w stanie zebrać tylu pakietów, by wystarczyły do złamania klucza. Przedział czasu zmiany klucza może być ustawiony w punkcie dostępu lub w bramie bezprzewodowej. Domyślna wartość tego przedziału wynosi 60 minut, co w zupełności wystarcza dla małych sieci domowych lub biurowych. Jeżeli mamy do czynienia z większymi sieciami o dużej przepustowości zaleca się skrócić ten czas do 10-15 minut. Przy takich ustawieniach, na dzień dzisiejszy żaden haker nie jest w stanie zebrać wystarczającej ilości pakietów w tak krótkim czasie. Odnawianie kluczy zajmuje kilka sekund, dlatego nie zaleca się skracania czasu do mniej niż 10 minut, ponieważ może to spowolnić działanie sieci.

Jak już napisałem wcześniej w mechanizmie WPA zastosowano ten sam algorytm szyfrowania RC4, co w WEP. Został on użyty dlatego, że jest prosty i łatwy do zaimplementowania a ponadto nie obciąża zbytnio procesora i pomimo faktu, iż WEP można bardzo łatwo złamać to przez zastosowanie wyżej wymienionych udoskonaleń mechanizm WPA stał się bardzo mocnym zabezpieczeniem.

4.4.2. Wady i problemy protokołu

Pomimo, że WPA jest bardzo silnym zabezpieczeniem ma on też słabe punkty, wynikające z samej koncepcji tego mechanizmu. Nie dotyczy to wykorzystywanym w nim algorytmie RC4. Może się zdarzyć, że mechanizm WPA wyłączy punkt dostępu na jakiś czas. Dzieje się tak, jeżeli w ciągu 60 sekund test MIC (Michael) da wynik negatywny w przypadku więcej niż dwóch pakietów. Z jednej strony jest to dobre rozwiązanie, ponieważ w takim przypadku można przypuszczać, że ktoś próbuje dostać się do sieci. Z drugiej strony pozwala to włamywaczowi na zaatakowanie sieci atakiem typu odmowa usługi (DoS), za pomocą celowo uszkadzanych pakietów, co może doprowadzić do wyłączenia punktu dostępu.

[6] http://www.tomshardware.pl/network/20030710/nktwpa-02.html

Stowarzyszenie Wi-Fi Alliance zaprojektowało standard WPA, by mógł być zastosowany na sprzęcie wyprodukowanym już wcześniej, za pomocą aktualizacji oprogramowania. Niestety jak się okazało później, było to czasami kłopotliwe. Można wymienić kilka podstawowych problemów związanych z aktualizacjami starszego sprzętu.

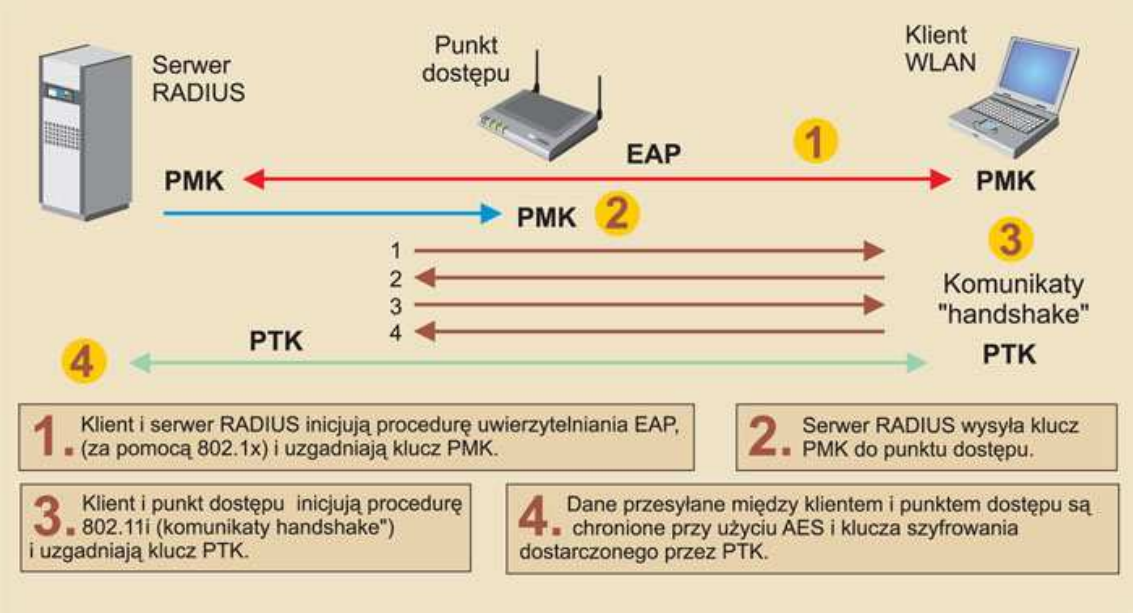
- Wystarczy, że jedno urządzenie w sieci nie będzie w stanie zaktualizować się do działania z WPA to automatycznie ucierpi bezpieczeństwo całej sieci.
- Zdarzało się, że w starszym sprzęcie mimo prób aktualizacji, mechanizm WPA nie działał. Było to spowodowane faktem, iż WPA wymaga większej mocy obliczeniowej niż WEP. W takim przypadku trzeba było zainwestować w nowe urządzenia lub korzystać dalej z szyfrowania WEP z nadzieją, że nic się nie wydarzy.
- Niektórzy producenci sprzętu nie udostępniali aktualizacji oprogramowania, w związku z czy trzeba było korzystać z oprogramowania typu Open Source.
- Mechanizm WPA nie działa ze starszymi systemami operacyjnymi. Microsoft wprowadził obsługę tego standardu w Windows XP, jednak nie udostępnił aktualizacji dla starszych systemów typu Windows 98. Użytkownikom korzystającym z wcześniejszych systemów pozostaje jedynie szukanie alternatywnego oprogramowania, co często wiąże się ze sporym wydatkiem.

Niektóre z wymienionych przeze mnie problemów związanych z WPA wynikały stąd, że mechanizm ten był przygotowywany w dużym pośpiechu. Omówiony przeze mnie mechanizm WPA jest częścią technologii wziętych z przyszłego standardu 802.11i, który później został nazwany przez organizację Wi-Fi Alliance mianem: WPA2.

4.5. WPA2 (802.11i)

Standard IEEE 802.11i został wprowadzony w czerwcu 2004 roku. Prace nad tym standardem trwały na tyle długo, że w międzyczasie wprowadzono inne rozwiązania mające na celu podniesienie słabego poziomu bezpieczeństwa sieci bezprzewodowych. Rozwiązaniem takim było stworzenie WPA, który wykorzystuje

wiele funkcji nowego standardu 802.11i. Zasadnicza zmiana w stosunku do specyfikacji WPA to rezygnacja z algorytmu RC4 na rzecz szyfrowania AES (Advanced Encryption Standard). Za zarządzanie kluczami i integralność komunikatów odpowiada pojedynczy składnik używający protokołu CCMP (Counter mode Cipher Block Chaining (CBC) - Message Authentication Code (MAC) Protocol). Można powiedzieć, że WPA2 to poprawiony i zaakceptowany przez IEEE WPA.



Rys.6. Działanie mechanizmu 802.11i, źródło: http://www.networld.pl/artykuly/48492.html

Wydawać by się mogło, że zsumowanie owoców dotychczasowych prac prowadzonych nad bezpieczeństwem sieci bezprzewodowych powinno dać w sumie silne zabezpieczenie. Jednak już w lipcu 2004 roku firma Aruba Wireless Networks poinformowała o złamaniu standardu 802.11i. Dokładny opis ataku został przedstawiony na stronach portalu www.idg.pl:

„Aruba Wireless Networks zajmuje się zabezpieczeniami sieci bezprzewodowych. Specjalistom z tej firmy udało się złamać zabezpieczenia nowo wprowadzonego standardu - 802.11i. Aby móc złamać zabezpieczenia, włamywacz musi uzyskać - oprócz bezpośredniego dostępu do zaatakowanej sieci - również dostęp do klucza, który służy do szyfrowania transmisji przechodzącej przez punkt dostępu. Jeżeli włamywaczowi uda się dostać do takiego punktu dostępu, bez problemu może

odłączyć z sieci dowolnego i - co najważniejsze - zalogowanego użytkownika, który po takim rozłączeniu automatycznie ponawia nawiązanie połączenia. Jest to o tyle istotne, że podczas ponownego nawiązania próby połączenia przez użytkownika można ją podsłuchać i zdobyć potrzebne dane do uzyskania dostępu do sieci. Tak zdobyte dane analizowane są później używając metody "brute force". Oczywiście problem ten, według Joshua Wright z SANS Institute, można rozwiązać stosując scentralizowane zarządzanie kluczami." [7]

W poprzednim standardzie - WPA, wystarczyła aktualizacja softu by zadziałał w większości starszych sieciowych kartach bezprzewodowych. W WPA2 natomiast to nie wystarcza, urządzenia muszą być specjalnie zaprojektowane do obsługiwania mechanizmu 802.11i. Poza tym początkowo systemy operacyjne nie obsługiwały nowego standardu zabezpieczeń. Microsoft opublikował darmową poprawkę przeznaczoną do uaktualnienia komponentów sieci bezprzewodowych w systemie Windows XP Service Pack 2. Dzięki temu system będzie w stanie obsłużyć WPA2.[8]

Podsumowując, mechanizmy zawarte w metodzie 802.11i gwarantują najwyższy poziom bezpieczeństwa przez uwierzytelnianie użytkowników, dobre szyfrowanie dynamicznie generowanym kluczem oraz kontrolę integralności przesyłanych danych. Mimo tego, że WPA2 został złamany jest w tej chwili najmocniejszym zabezpieczeniem. Atak zaprezentowany przez firmę Aruba Wireless Networks jest na tyle skomplikowany, że tylko wykwalifikowani specjaliści będą w stanie go wykonać. Od tamtej pory nie pojawiły się żadne informacje o złamaniu mechanizmu WPA2 innym sposobem. Nie było też informacji o wykorzystaniu wyżej wymienionego ataku przez hakerów. Od marca 2006 roku wszystkie urządzenia korzystające z sieci standardu 802.11 certyfikowane przez Wi-Fi Alliance muszą być kompatybilne z WPA2.

[7] http://wireless.idg.pl/artykuly/45535_1.html
[8] Poprawka jest dostępna pod adresm: http://support.microsoft.com/default.aspx?scid=kb;en-us;893357

4.6. Uwierzytelnianie i szyfrowanie (w sieciach bezprzewodowych)

4.6.1. Standard IEEE 802.1x

802.1x jest standardem IEEE uwierzytelnionego dostępu do przewodowych sieci Ethernet i bezprzewodowych sieci standardu 802.11. Standard IEEE 802.1x podwyższa poziom zabezpieczeń i ułatwia ich wdrażanie, ponieważ oferuje obsługę scentralizowanej identyfikacji użytkowników, uwierzytelniania, dynamicznego zarządzania kluczami i ewidencjonowania aktywności.[9]

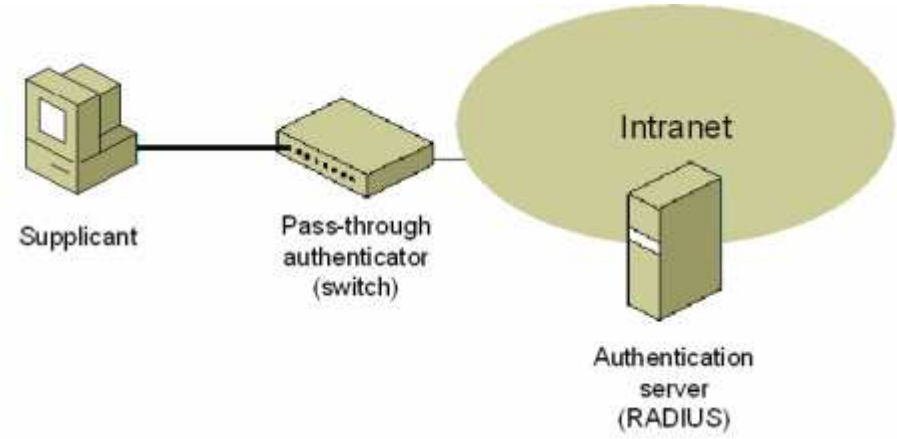
Kariera standardu 802.1x w sieciach bezprzewodowych rozpoczęła się, gdy na jaw wyszły wszystkie słabości WEP. Wtedy to wielu dostawców zaimplementowało 802.1x w bezprzewodowych punktach dostępu, by zapewnić bezpieczeństwo sieci przynajmniej na poziomie autoryzacji. Zastosowanie uwierzytelniania 802.1x eliminuje niebezpieczeństwo nieautoryzowanego dostępu do sieci już na poziomie warstwy dostępu. Zazwyczaj uwierzytelnienie jest przeprowadzane przez serwer RADIUS. Standard IEEE 802.1x jest oparty na protokole EAP.

Alternatywnie IEEE 802.1x może zostać tak skonfigurowany, aby umożliwiać nieautoryzowanym klientom dostęp do specjalnie wydzielonej podsieci wirtualnej zwanej VLAN. Podsieć taka może zostać przystosowana specjalnie na potrzeby gości.

Środowisko standardu 802.1x składa się z trzech elementów:

- Klient – w sieciach Wi-Fi jest to komputer zaopatrzony w bezprzewodową kartę sieciową, który próbuje uzyskać dostęp do sieci przez punkt dostępu. W sieciach LAN jest to komputer łączący się ze switch'em.
- Switch lub Access Point – wymusza uwierzytelnienie klienta przed udostępnieniem portu LAN do użytku.
- Serwer uwierzytelniający – dokonuje uwierzytelnienia i autoryzacji klienta. W chwili połączenia sprawdza uprawnienia użytkownika i przesyła informację do punktu dostępu, który udziela, bądź nie udziela dostępu. W sieciach bezprzewodowych najczęściej do tego celu wykorzystuje się RADIUS.

[9] http://technet2.microsoft.com/WindowsServer/pl/Library/908d13e8-c4aa-4d62-8401-86d7da0eab481045.mspx?mfr=true



Rys. 7. Schemat działania standardu 802.1x, źródło: http://wss.pl/Articles/6880.aspx

4.6.2. EAP

Działanie protokołu EAP bardzo szczegółowo opisał Microsoft na swoich witrynach internetowych: http://www.microsoft.com/poland/technet. Poniżej przedstawiam krótki opis protokołu znajdujący się pod dokładnym adresem:[10]

„W standardzie 802.1X protokół EAP jest używany do wymiany komunikatów podczas procesu uwierzytelniania. Protokół EAP umożliwia korzystanie z dowolnej metody uwierzytelniania, na przykład certyfikatów, kart inteligentnych lub poświadczeń. Pozwala on również na nieograniczoną konwersację między klientem EAP (np. komputerem bezprzewodowym) a serwerem EAP, takim jak serwer usługi uwierzytelniania internetowego (IAS, Internet Authentication Service). Na konwersację składają się żądania wysyłane przez serwer, które dotyczą podania informacji uwierzytelniających, oraz odpowiedzi wysyłane przez klienta. Aby uwierzytelnienie powiodło się, klient i serwer muszą korzystać z tej samej metody uwierzytelniania.

- **EAP-TLS** - Protokół EAP-TLS (Transport Layer Security) to typ protokołu EAP, który jest używany w środowiskach zabezpieczeń korzystających z certyfikatów i stanowi najsilniejszą metodę uwierzytelniania i ustalania klucza.

[10] http://technet2.microsoft.com/WindowsServer/pl/Library/908d13e8-c4aa-4d62-8401-86d7da0eab481045.mspx?mfr=true

- **EAP-MS-CHAP v2** - EAP-Microsoft Challenge Handshake Authentication Protocol version 2 stanowi metodę uwierzytelniania wzajemnego, która obsługuje uwierzytelnianie użytkowników i komputerów w oparciu o hasła. Aby proces uwierzytelniania przy użyciu protokołu EAP-MS-CHAP v2 zakończył się powodzeniem, zarówno serwer, jak i klient, muszą udowodnić, że znają hasło użytkownika.
- **PEAP** - Protokół PEAP z protokołem EAP-TLS, który używa certyfikatów do uwierzytelniania serwerów oraz kart inteligentnych lub certyfikatów do uwierzytelniania użytkowników i komputerów klienckich."

4.6.3. PPPoE (Point-to-Point Protocol over Ethernet)

Protokół ten został stworzony do autoryzacji w sieciach LAN. Często służy on także do łączenia z Internetem poprzez zastosowanie odpowiedniego modemu, przykładem może być usługa Neostrada świadczona przez Telekomunikację Polską.

Okazało się jednak, że protokół PPPoE może być zastosowany również w przypadku sieci bezprzewodowych. Może on stanowić alternatywę dla protokołu 802.1x. Zaletą PPPoE jest jednorazowa konfiguracja sieci (za pomocą wbudowanych kreatorów systemów Windows 2003/XP/2000), niezwykle podobna do konfiguracji Neostrady. Tak samo jak 802.1x, może wykorzystywać serwer RADIUS.

Niestety PPPoE jest wpierane tylko przez profesjonalne i drogie punkty dostępu. Rozwiązaniem jest konfiguracja odpowiedniego komputera oparta na Linux, MikroTik lub BSD, ale czynność ta jest dosyć skomplikowana.

4.6.4. VPN (Virtual Private Network)

Wirtualne Sieci Prywatne, w skrócie VPN, to dobry sposób na zabezpieczenie transmisji, gdy nie mamy dostępu do Access Pointa lub z innych względów nie chcemy wprowadzać szyfrowania ruchu w całej sieci Wi-Fi.

VPN umożliwia tworzenie wirtualnych sieci korzystających z technologii tunelowania (protokół PPTP). Przez tunel taki płynie ruch w ramach sieci prywatnej, pomiędzy klientami końcowymi, za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Dane przesyłane takim tunelem mogą być szyfrowane i kompresowane, co zapewnia wysoką wydajność i bezpieczeństwo takiego rozwiązania.

W sieci Wi-Fi zastosowanie VPN jest uzasadnione w dwóch przypadkach:

1) Chcemy uchronić nasze dane przed wścibskim administratorem.

2) Zależy nam na bezpieczeństwie transmisji w nieszyfrowanej sieci.

4.7. WPS (Wi-Fi Protected Setup)

W 2003 roku stowarzyszenie Wi-Fi Alliance przeprowadziło badania, które miały określić, dlaczego tak mało osób włącza szyfrowanie WPA, WPA2 bądź WEP. Okazało się, że konfiguracja tych zabezpieczeń dla 44 procent ludzi stanowiła poważny problem, była po prostu za trudna.[11] Moim zdaniem wartość ta została trochę zawyżona, ponieważ jak pokażę później włączenie WPA lub WEP jest bardzo proste i osoby, które chociaż w minimalnym stopniu umieją korzystać z komputera powinny sobie z tym poradzić. Jedynym problemem może być konfiguracja WPA lub WPA2 w sieci, w której korzysta się z serwera RADIUS. Według mnie przyczyną faktu, że ludzie nie zabezpieczają swoich sieci jest po prostu lenistwo. Przeważnie każde dostępne urządzenie posiada dokumentację oraz instrukcję, z których można dowiedzieć się, w jaki sposób je skonfigurować. Z innego punktu widzenia to wynik 44 % nie powinien dziwić, biorąc pod uwagę to, że badania były przeprowadzane w Stanach Zjednoczonych a jak wiadomo Amerykanie wymyślą wszystko byle by się nie napracować i ułatwić sobie życie.

Wi-Fi Protected Setup będzie stosowany w sieciach infrastrukturalnych gdzie do uzyskania połączenia korzysta się z punktów dostępu. W sieciach „ad hoc” system ten nie będzie działał. Zaleca się go do zastosowania w małych sieciach domowych i biurowych. W większych sieciach gdzie zastosowano serwery uwierzytelniania WPS

[11] http://www.wi-fi.org

nie zda egzaminu. System ten został zaprojektowany w taki sposób, by użytkownik nie musiał praktycznie niczego znać ani wiedzieć. Do połączenia się z punktem dostępu nie trzeba znać nazwy SSID ani klucza szyfrowania WPA2, dane te zostaną same przesłane z nadajnika do komputera. Działanie WPS w praktyce podzielono na dwa różne rozwiązania. W pierwszym przypadku, aby zabezpieczyć sieć Wi-Fi użytkownik musi podać składający się z cyfr kod PIN (Personal Information Number). W drugim rozwiązaniu wystarczy tylko nacisnąć jeden przycisk, sposób ten określa się skrótem PBC (Push Button Configuration).

System WPS wykorzystuje opisany już przeze mnie mechanizm zabezpieczeń WPA2 i jest kompatybilny z wszystkimi urządzeniami certyfikowanymi przez Wi-Fi Aliiance do korzystania z 802.11i, jednak w większości wypadków potrzebna będzie aktualizacja oprogramowania. Od stycznia 2007 organizacja wystawia certyfikaty zgodności z WPS wszystkim urządzeniom, które pomyślnie przejdą testy zarówno z PIN jak i PBC. Obecnie na rynku jest jedynie kilka punktów dostępu, które mogą wykorzystywać nowy standard.

Rys. 8. Znak certyfikacji WPS
źródło: www.wi-fi.org

Na dzień dzisiejszy nie można jeszcze w pełni ocenić działania tego standardu, ponieważ urządzenia korzystające z WPS dopiero zaczynają pojawiać się na rynku. Po kilku miesiącach działania będzie można ocenić system w praktyce, a z czasem będą wychodzić wady i zalety tego rozwiązania. Jedyne co można stwierdzić, to że będzie zapewniał taki sam poziom bezpieczeństwa jak WPA2. Jednak moim zdaniem system WPS szybko zostanie złamany. Pomimo zastosowania standardu 802.11i, nowy standard jest zbyt prosty i na pewno zostaną odkryte pewne luki, które pozwolą na nieautoryzowany dostęp lub podsłuch.

4.8. Dekalog administratora sieci

Chciałbym przedstawić tutaj „dekalog administratora sieci”, który znalazłem na stronie internetowej portalu www.idg.pl.[12] Myślę, że każdy administrator powinien nauczyć się go na pamięć. W 10 punktach zostały przedstawione czynności, jakie powinno się wykonać, aby dobrze zabezpieczyć sieć Wi-Fi. Poniżej cała treść „dekalogu”:

1. Zmień nazwę i hasło - zaraz po uruchomieniu routera zmodyfikuj przynajmniej hasło użytkownika "admin", który zwykle ma nielimitowany dostęp do sprzętu.
2. Włącz zabezpieczenia - nie przesyłaj siecią żadnych ważnych danych, zanim nie uruchomisz przynajmniej szyfrowania WEP; a najlepiej WPA-PSK lub WPA2. Nie myśl, że skoro w pobliżu nie było żadnych WLAN, nikt nie może cię podsłuchiwać.
3. Uruchom firewall w stacjach roboczych - niezależnie od włączenia firewalla w routerze powinieneś zabezpieczyć również desktopy. Nawet jeśli ktoś dostanie się do twojej sieci, będzie miał olbrzymie trudności z wniknięciem na pulpity maszyn.
4. Filtruj adresy MAC - niech z routerem mogą się połączyć jedynie te urządzenia, które należą do ciebie.
5. Oddziel sieć bez- i przewodową - jeżeli komputery podłączone kablem dostają adresy IP z zakresu 192.168.2.1-100, zmodyfikuj tak opcje routera, aby Wi-Fi działało w zakresie 192.168.3.1-100 lub innym.
6. Nie zarządzaj przez WLAN – nawet, jeśli włączyłeś dostęp do panelu administracyjnego routera przez SSL (czyli w przeglądarce wpisujesz adres https://...), wyłącz możliwość zmieniania opcji przez Wi-Fi albo od strony Internetu. Zabezpieczysz się w ten sposób nie tylko przed intruzami, lecz także przed nagłym odcięciem sobie dostępu do sieci.
7. Rezygnuj z domyślnych kanałów - tuż po uruchomieniu routera zmień domyślny kanał transmisji na inny (patrz numer 09/2006 PC World Komputera).

[12] http://wireless.idg.pl/artykuly/52702.html

8. Właściwie ustaw punkt dostępowy/router - jeśli sprzęt będzie stał na środku mieszkania, zmniejszysz "przeciekanie" sygnału przez ściany.
9. Obniż moc urządzeń - jeśli to możliwe, postaraj się zmniejszyć moc nadawania w routerze i karcie sieciowej. Transfer spadnie minimalnie, natomiast zabezpieczysz się przed wardriverami buszującymi pod twoim blokiem.
10. Teraz najważniejsze: sprawdź się. Spróbuj się włamać do własnego WLAN z pracy albo z klatki schodowej. Skorzystaj też ze skanera portów w witrynie Sygate.

4.9. Fizyczne zabezpieczenia sieci

4.9.1 Zabezpieczenia przed kradzieżą

Zablokowanie sieci Wi-Fi przed nieautoryzowanym dostępem to nie wszystkie czynności, jakie powinniśmy zrobić by uczynić naszą sieć bezpieczną. Oprócz prób połączenia i włamania się do naszej sieci, musimy wziąć pod uwagę także takie osoby, których nie interesują przesyłane dane ani dostęp do Internetu. Obiektem zainteresowania tych osób jest sprzęt zastosowany przy budowie sieci bezprzewodowej i często ma dla nich wartość tylko materialną. Krótko mówiąc, musimy zabezpieczyć się przed kradzieżą. Ktoś może powiedzieć, że jak się złodziej uprze to ukradnie wszystko i to jest prawda, nigdy nie zabezpieczymy się w 100% przed kradzieżą, nawet zamykając rzeczy w sejfie jesteśmy narażeni na to, że znajdą się osoby chcące go otworzyć. W takim wypadku musimy postarać się o to, by nasz sprzęt sieciowy zainstalowany z dala od naszych domów na masztach lub wieżach, nie rzucał się zbytnio w oczy, jak złodziej go nie zobaczy to nie ukradnie. W przypadku, gdy posiadamy punkt dostępu i antenę na dachu swojego domu to prawdopodobieństwo tego, że ktoś tam wejdzie i ukradnie sprzęt jest porównywalne do wytypowania 6 w lotku. Nikt bowiem o zdrowym umyśle nie będzie ryzykował więzieniem wkradając się do domu po to by zarobić parę złotych. Trochę inaczej sprawa wygląda, gdy nasz punkt dostępu i anteny są ulokowane na wieży lub maszcie w niezamieszkałej okolicy. Wtedy złodziej niezauważony przez nikogo może wejść na górę i zabrać sprzęt. W takim przypadku ciężko jest obronić się przed napastnikiem, jedynie co możemy zrobić to

utrudnić złodziejowi zadanie. Gdy na wieży mamy zainstalowany punkt dostępu to dobrze żeby był on w skrzynce zamykanej na zamek lub kłódkę, dobrze byłoby go też umiejscowić w takim miejscu, by z dołu nie był widoczny. Jeżeli chodzi o anteny to wystarczy dobrze umocować je do masztu, pozwoli to także na zabezpieczenie ich przed silnym wiatrem

Oprócz takich mało wartościowych rzeczy jak punkty dostępu, kable i anteny powinniśmy martwić się o bezpieczeństwo naszego laptopa lub palmtopa. Taki komputer jest znacznie lepszą zdobyczą dla złodzieja. Jeżeli wykorzysta go w celach zarobkowych i sprzeda pierwszemu chętnemu za pół ceny to jeszcze pół biedy, gorzej sprawa wygląda, gdy napastnik zechce za pomocą tego laptopa połączyć się z naszą siecią bezprzewodową. Nie musi on wtedy znać żadnego hasła i nie obchodzi go czy sieć jest zabezpieczona jakimś mechanizmem czy nie. System operacyjny sam połączy się z siecią bez większych problemów.

Aby zapobiec takim wydarzeniom, musimy mieć komputer zawsze na oku, nie zostawiać go nawet na chwilę w niepewnych miejscach. Najlepiej zawsze mieć go w torbie lub trzymać w ręce. Nie zaleca się też zostawiania laptopa na noc lub dłużej nawet w czasie urlopu. Było już kilka przypadków wyniesienia przez złodziei komputerów z firm pomimo zatrudnionych tam firm ochroniarskich.

W sieciach standardu 802.11 zastosowanych w firmach, odpowiedzialność za zabezpieczenie przed kradzieżą przechodzi na dział ochrony lub firmę ochroniarską. Jedyne, co musimy zrobić jako administrator a nawet jako użytkownik sieci to poinformowanie ochrony gdzie znajdują się urządzenia sieciowe i ewentualnie okablowanie, tak by żadna obca osoba nie kręciła się w okolicy sprzętu.

4.9.2 Zabezpieczenia przed działaniem czynników atmosferycznych.

Ta część pracy dotyczy sprzętu stosowanego w sieciach 802.11 wystawionego na działanie czynników atmosferycznych. Można wymienić cztery czynniki, które mogą nas pozbawić dostępu do sieci, a nawet mogą powodować uszkodzenie anten lub punktów dostępowych: wiatr, opady, pioruny i temperatura.

Większość anten i niektóre punkty dostępowe mocowane są na zewnątrz budynków na dachach, w celu zapewnienia dobrej widoczności. Często to nie wystarcza

i stawia się specjalne maszty tak by antena znalazła się jeszcze wyżej. Maszt taki musi być bardzo stabilny, mocno przytwierdzony do dachu lub innego podłoża, jeśli przekracza wysokość kilku metrów powinien być także przypięty linami najlepiej z czterech stron. Jeśli zaniedbamy tą czynność to przy mocniejszym podmuchu wiatru maszt może się przewrócić, co najczęściej kończy się uszkodzeniem anteny lub punktu dostępu, jeśli był tam także zamontowany.

Drugim uciążliwym czynnikiem zagrażającym naszej sieci są opady atmosferyczne. Padający deszcz lub śnieg może okazać się sporym problemem, jeśli mamy źle uszczelnioną tubę od anteny lub skrzynkę z punktem dostępu. Musimy zadbać o to by tak zamontować urządzenie by nie dostała się do niego woda, ponieważ w przypadku punktu dostępu wystarczy tylko kilka kropel by uległ zniszczeniu. Wystawiając access point na zewnątrz musimy umieścić go w bardzo szczelnej skrzynce, albo w inny sposób ochronić go przed działaniem wody. Można umieścić go pod dachem lub skonstruować samemu małe zadaszenie. Jeżeli chodzi o anteny to zagrożenie opadami dotyczy tylko tych anten, które są zamknięte szczelnie w tubie bądź skrzynce np. yagi, anteny panelowe. Problem polega na tym, że w przypadku nieszczelności woda łatwo się może dostać do środka i w momencie, gdy będzie jej dużo to może spowodować znaczny spadek mocy odbieranego lub nadawanego sygnału.

Jeżeli chodzi o temperaturę to najczęstszym problemem może być przegrzanie się punktu dostępowego a w konsekwencji jego zawieszenie. Montując routery bezprzewodowe w szczelnych puszkach trzeba zapewnić swobodny przepływ powietrza. Najprościej jest wywiercić kilka otworów, najlepiej od dołu by przy opadach deszczu woda nie dostawała się do środka.

Warto też zastosować urządzenie zwane odgromnikiem, które zabezpiecza urządzenia radiowe przed piorunami lub wyładowaniami atmosferycznymi. Odgromnik podłącza się do kabla między punktem dostępu a anteną i uziemia poprzez połączony przewód uziemiający. Odgromniki posiadają w środku element przypominający bezpiecznik, który podczas skoku napięcia zrywa połączenie, chroniąc sprzęt.

Rozdział V. Utworzenie dobrze zabezpieczonej sieci Wi-Fi w praktyce.

W rozdziale tym przedstawię w praktyce opisane przeze mnie zabezpieczenia. Do tego celu stworzyłem testową sieć, która składa się z punktu dostępowego Linksys WRT54GC, laptopa Asus oraz z komputera stacjonarnego. Notebook HP wykorzystam do przeprowadzania ataków i sprawdzania konfiguracji sieci. Komputer stacjonarny podłączony jest do routera kablem, natomiast laptop Asus oraz HP korzystają z połączenia bezprzewodowego w standardzie 802.11g.

Rys. 9. Schemat sieci testowej wykorzystanej do przeprowadzenia badań

Na wszystkich komputerach w sieci zainstalowane zostały systemy Microsoft Windows XP Home. Ponieważ wszystkie komputery należące do tej sieci znajdowały się w jednym pomieszczeniu, wykorzystałem karty sieciowe, jakie były zamontowane wewnątrz laptopów. Połączenia były dobre i stabilne, dlatego nie musiałem korzystać z anten zewnętrznych.

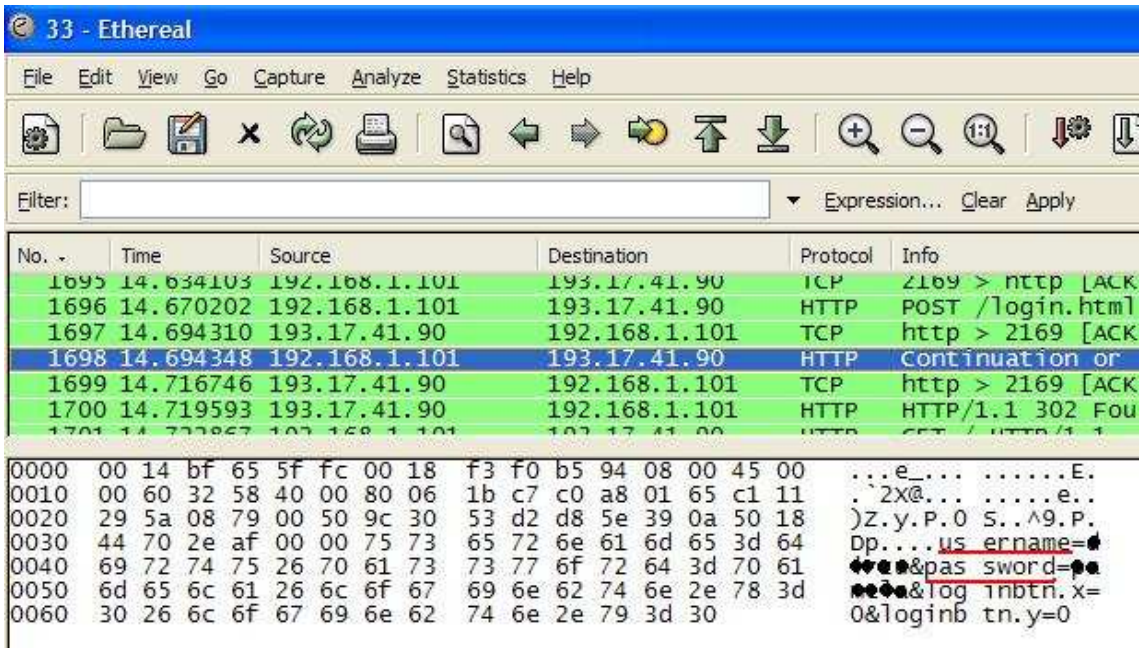
5.1 Sieć niezabezpieczona

Na początku chciałbym pokazać jak łatwo można połączyć się z siecią bezprzewodową, która nie posiada żadnych zabezpieczeń. Zademonstruję też, z jaką łatwością można przechwycić informacje przesyłane w tej sieci. Oprócz mało ważnych informacji o tym, jakie strony internetowe otwiera użytkownik można dowiedzieć się jaki ma login i hasło do poczty e-mail lub do banku internetowego.

Mając działającą już sieć składającą się z routera WRT54GC, komputera stacjonarnego oraz laptopa Asus, przeprowadzę próbę połączenia się do tej sieci za pomocą notebooka HP. Po włączeniu komputera, system Windows od razu wykrył dostępną sieć i wystarczyło tylko kliknąć w przycisk „Połącz" by połączył się z tą niezabezpieczoną siecią. Jeżeli we właściwościach karty sieciowej będzie włączona opcja automatycznego łączenia z siecią będącą w zasięgu, wtedy laptop sam nawiąże połączenie.

Rys. 10. Kolejne etapy łączenia się z niezabezpieczoną siecią.

Po podłączeniu się do testowej sieci mogę teraz zacząć podsłuchiwać cały ruch sieciowy. Wystarczy, że skorzystam z programu przechwytującego pakiety, który zbierze odpowiednie dane. Do tego celu wykorzystałem program Ethereal, który pokazał mi, co użytkownicy laptopa Asus oraz komputera stacjonarnego robili w Internecie. Oprócz wyświetlenia stron, jakie przeglądali, program wychwycił też hasło i login do konta pocztowego.



Rys. 11. Ethereal – widoczne przechwycone login i hasło

Oprócz podsłuchiwania ruchu sieciowego, w niezabezpieczonej sieci można zrobić wiele złego. Jak już pisałem we wcześniejszych rozdziałach poważnym zagrożeniem jest podszywanie się pod adres IP innego użytkownika. Aby tego dokonać trzeba zmienić adres MAC swojej karty sieciowej na adres wybranego użytkownika. W podrozdziale 5.3 opisuję dokładnie jak to zrobić.

Kolejnym niebezpieczeństwem związanym z pojawieniem się intruza w sieci jest możliwość zmiany przez niego ustawień sieciowych. Jeżeli punkt dostępowy posiada standardowe ustawienia to można w łatwy sposób dostać się do jego panelu konfiguracyjnego. Wystarczy poszukać w Internecie informacji o domyślnych ustawieniach dla danego routera bezprzewodowego. W przypadku Linksysa WRT54GC jego panel administracyjny jest dostępny pod adresem 192.168.1.1 a login i hasło jest

takie same: „admin”. W ten sposób za pomocą laptopa HP, z którego skorzystałem do wpięcia się do sieci, mogę teraz pozmieniać ustawienia punktu dostępowego. Jeżeli zmienię jego adres IP, hasło administratora oraz odłączę inne komputery od sieci za pomocą filtracji MAC to właścicielowi sieci pozostanie tylko i wyłącznie zresetowanie routera.

Jak pokazałem wyżej, nie ma nic trudnego w połączeniu z siecią bezprzewodową nie posiadającą zabezpieczeń a także z przechwytywaniem przesyłanych danych. Dlatego też nigdy nie powinno się korzystać z niezabezpieczonych sieci Wi-Fi.

5.2 Wyłączenie rozgłaszania nazwy SSID sieci

Przy wyłączonym rozgłaszaniu nazwy SSID sieci, intruz (laptop HP) nie będzie mógł się połączyć z punktem dostępu, ponieważ nie będzie znał jego nazwy. Sieć stanie się dla niego niewidoczna. Nie będzie jej widać ani w Windowsie ani też w programie Netstumbler.

Rys. 12. Niewidoczna sieć zarówno dla Netstumblera jak i dla Windows

Istnieje jednak bardzo łatwy sposób na obejście tego zabezpieczenia. Wystarczy uruchomić program Netstumbler lub Kismet w systemie Linux i poczekać aż jeden z klientów nawiąże połączenie z siecią, wtedy bowiem wysyła on czystym tekstem SSID ukrytej sieci, a wymienione programy wychwycą tą nazwę. Jeżeli w sieci znajduje się tylko jedna osoba to może minąć trochę czasu zanim pozna się SSID. Jednak im więcej użytkowników jest w danej sieci, tym szybciej powinna zostać przechwycona nazwa SSID. Aby zademonstrować powyższe działania, na laptopie intruza – HP uruchamiam

program Netstumbler a potem na komputerze Asus najpierw wyłączam połączenie sieciowe by po chwili je ponownie włączyć. Po tej operacji na laptopie intruza otrzymałem zadowalający wynik, Netstumbler wychwycił nazwę sieci SSID, której szukałem: „sieci_testowa”. Znając już nazwę mogę już bez przeszkód nawiązać połączenie. Zabezpieczenie to chroni jedynie przed wardriverami i osobami, które nie wiedzą o istnieniu takiej sieci, ale warto je włączyć jako uzupełnienie WPA lub WPA2.

5.3 Filtracja MAC

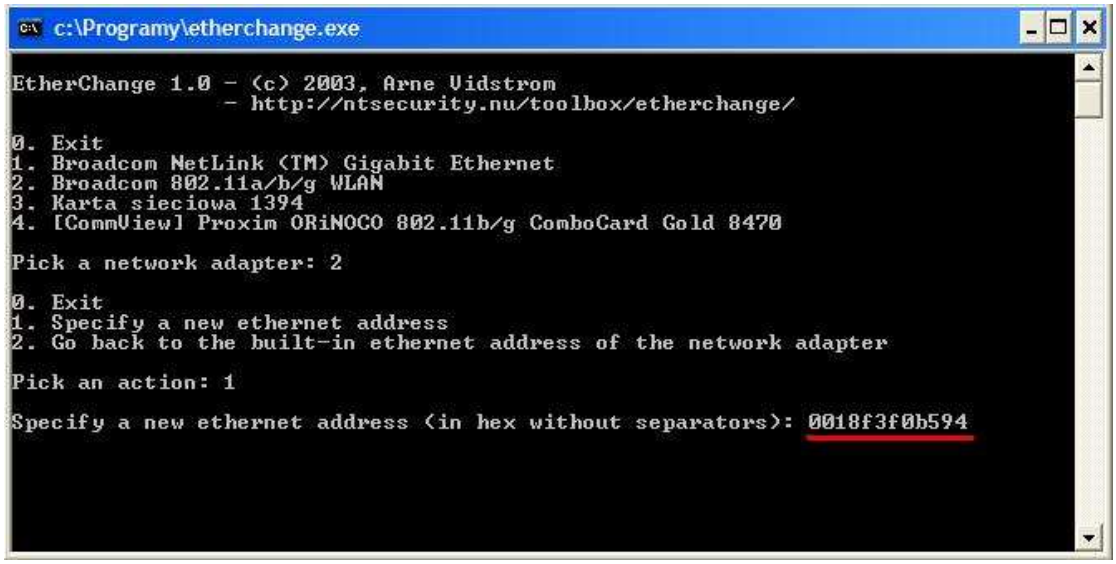
Aby zademonstrować działanie tego zabezpieczenia, w ustawieniach punktu dostępowego włączam filtrację MAC i tylko laptopowi Asus pozwolę na połączenie z siecią. W tym celu wpisuję jego adres MAC do tablicy i od tej pory tylko i wyłącznie on może poprawnie komunikować się z punktem dostępu. Inne komputery nie będą mogły połączyć się z siecią mimo tego, że ani Windows ani Netstumbler nie pokazuje, że ta sieć jest zabezpieczona. Na laptopie HP widać „siec_testową” jako niezabezpieczoną jednak przy próbie połączenia okazuje się dopiero, że dostęp do niej jest zabezpieczony.

Rys. 13. Przy filtracji MAC siec_testowa wykrywana jest jako niezabezpieczona

Jedynym sposobem na obejście tego zabezpieczenia jest podmiana adresu MAC karty sieciowej na adres, który może łączyć się z tą siecią. W moim przypadku tylko laptop Asus ma dostęp do sieci, dlatego na laptopie HP muszę zmienić adres MAC karty sieciowej na taki, jaki jest w Asusie. Żeby poznać adresy MAC innych komputerów w sieci trzeba skorzystać ze sniffera. Do tego celu wykorzystałem darmowy program CommView for Wifi, który pomimo tego, że laptop HP nie był połączony z siecią wyświetlił interesujące dla mnie dane – adres MAC laptopa Asus.

Rys. 14. CommView for WiFi - adresy MAC punktu dostępowego i laptopa Asus

Znając już adres MAC karty sieciowej laptopa Asus wystarczy teraz podmienić swój adres na ten, który wyświetlił się w programie CommView for WiFi. Istnieje wiele programów do podmiany adresu MAC, ja skorzystałem z darmowego narzędzia etherchange. Zmieniłem adres MAC karty sieciowej w laptopie HP i po ponownym uruchomieniu komputera mogłem już uzyskać połączenie z zabezpieczoną siecią. W tym momencie obydwa laptopy mają ten sam adres MAC jednak nie przeszkadza to we wspólnym działaniu.



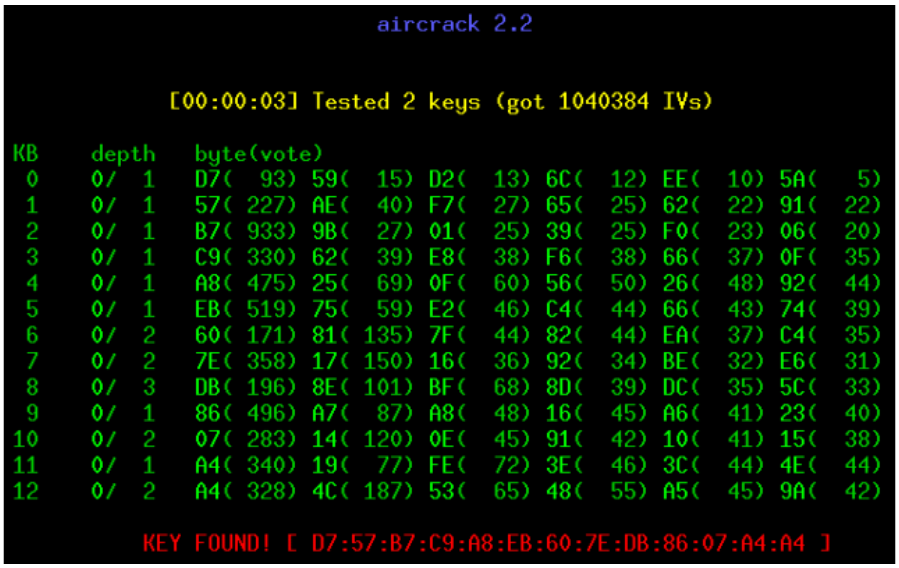
Rys. 15. Etherchange – szybki sposób na zmianę MAC

Jak widać filtrację adresów MAC da się w bardzo łatwy sposób ominąć, dlatego zabezpieczenie to nie powinno być nigdy stosowane samodzielnie. Warto jednak je zastosować razem z metodami szyfrowania WPA lub WPA2

5.4 Szyfrowanie WEP

Po włączeniu mechanizmu WEP w punkcie dostępu i w laptopie Asus dane przesyłane siecią bezprzewodową są teraz szyfrowane. Osoba z zewnątrz nieznająca klucza nie będzie mogła się podłączyć. Na laptopie HP przy próbie połączenia pojawi się jedynie informacja o zabezpieczonej sieci. Nie znając klucza szyfrowania WEP nie tylko nie można połączyć się z siecią, ale także nie można przechwycić żadnych danych za pomocą wykorzystywanych wcześniej przeze mnie programów (Ethereal, CommView for WiFi). Pomimo tego szyfrowanie WEP da się w krótkim czasie złamać i uzyskać potrzebny klucz. W tym celu najlepiej skorzystać z oprogramowania dostępnego pod systemem Linux. Powstały odpowiedniki tych programów także dla systemu Windows jednak są mniej funkcjonalne i nie współpracują ze wszystkimi kartami sieciowymi.

Do złamania zabezpieczenia WEP wykorzystam specjalną dystrybucję Linux'a – Backtrack, która została stworzona z myślą o sieciach bezprzewodowych. Pierwszą rzeczą, jaką muszę zrobić jest przestawienie bezprzewodowej karty sieciowej w tryb monitorowania, tak by przechwytywała wszystkie pakiety przesyłane w sieci. Następnym krokiem jest włączenie airodump – programu, który zacznie przechwytywać słabe wartości wektora IV. Szybkość zbierania tych informacji zależy od ruchu, jaki aktualnie panuje w sieci. Proces ten można przyspieszyć za pomocą programu aireplay, który wstrzykuje pakiety sztucznie stwarzając większy ruch, po to by wychwycić więcej pakietów. Po przechwyceniu około miliona wartości wektora IV można spróbować złamać klucz. W tym celu uruchamiam program aircrack i po kilku lub kilkudziesięciu minutach, otrzymam wartość klucza WEP.



Rys.16. Wynik działania programu aircrack

Proces łamania klucza WEP w programie aircrack może zająć nawet do godziny czasu, zależy to m.in. od złożoności klucza oraz od ilości znalezionych wartości IV. Proces ten można znacznie przyspieszyć korzystając z nowej wersji oprogramowania aircrack-ptw. Jego twórcy zapewniają, że odszyfrowanie klucza WEP zajmuje tylko 1 minutę. Jak widać szyfrowanie WEP w miarę prosty sposób da się złamać, dlatego też nie powinno się go używać się dla żadnych sieci bezprzewodowych. Aktualnie mechanizm ten zapewnia tylko minimalny stopień bezpieczeństwa.

5.5 Szyfrowanie WPA

W momencie włączenia szyfrowania WPA w sieci testowej, jako użytkownik laptopa HP nie mam prawie żadnych szans na połączenie ani chociaż podsłuchanie, co się dzieje w tej sieci. Jedyną możliwością złamania szyfrowania WPA jest próba odgadnięcia wartości klucza. Można tego dokonać za pomocą wspomnianego już wcześniej programu aircrack, który metodą brute-force lub słownikową próbuje znaleźć klucz. Może się to udać jedynie wtedy, gdy klucz PSK będzie bardzo łatwy do odgadnięcia (np. 123, osa, auto itp.). W przypadku bardziej złożonego klucza złamanie

WPA nie będzie możliwe. Jeżeli administrator sieci zdecyduje się zabezpieczyć sieć tym właśnie mechanizmem warto dla większej pewności włączyć także filtrację adresów MAC oraz wyłączyć rozgłaszanie nazwy SSID sieci.

5.6 802.11i – najlepsze zabezpieczenie

Obecnie szyfrowanie WPA2 (802.11i) jest najlepszym zabezpieczeniem jakie można zastosować w sieciach Wi-Fi. Na dzień dzisiejszy nie stworzono oprogramowania, które byłoby w stanie w jakikolwiek sposób wykryć wartość klucza szyfrowania. Po włączeniu w punkcie dostępu szyfrowania 802.11i, podobnie jak to miało miejsce z WPA, na laptopie intruza w żaden sposób nie da się połączyć z siecią. Nie da się także przechwycić żadnych przesyłanych danych. Szyfrowanie WPA2 w pełni zabezpiecza dostęp do sieci nieuprawnionym użytkownikom. Myślę jednak, że w przyszłości także i to zabezpieczenie zostanie złamane, dlatego też można razem z WPA2 włączyć filtrację MAC.

Rozdział VI: Inne sieci bezprzewodowe

Oprócz bardzo popularnych sieci 802.11 istnieje jeszcze kilka typów sieci bezprzewodowych, z którymi mamy styczność na co dzień. Mówię tu o sieciach opartych na podczerwieni oraz Bluetooth. Poniżej przedstawię w skrócie ich działanie oraz bezpieczeństwo.

6.1. Podczerwień (IrDA)

Sieci oparte na podczerwieni nie zdobyły popularności z 2 ważnych powodów: po pierwsze mają bardzo mały zasięg, dochodzący maksymalnie do kilku metrów a po drugie, nadajnik i odbiornik muszą się nawzajem widzieć. Z tego typu sieci możemy skorzystać na przykład do połączenia ze sobą dwóch laptopów lub komputera z telefonem komórkowym. Pomimo, że w sieciach standardu IrDA nie zastosowano żadnego mechanizmu zabezpieczającego przesyłane dane, osoba chcąca podpiąć się do tej sieci ma bardzo utrudnione zadanie. Żeby znaleźć się w zasięgu fal podczerwonych musiałaby podejść bardzo blisko atakowanego urządzenia, co z pewnością zauważyłby użytkownik sieci. Jedynie w przypadku, gdy nie będzie nikogo w pobliżu działania sieci to napastnik ma szansę na połączenie się. Systemy Windows 2000, XP i wyższe automatycznie kojarzą się z innymi komputerami działającymi w sieci IrDA. Istnieje zatem jeden sposób na zabezpieczenie sieci opartej na podczerwieni: wystarczy być przy niej i nie odchodzić daleko w czasie jej działania.

6.2. Bluetooth

Najczęściej sieci bluetooth wykorzystywane są tak jak IrDA w telefonach komórkowych, ale istnieje także możliwość połączenia w ten sposób komputerów. Jednak zyskują one większą popularność niż sieci na podczerwień głownie dlatego, że działają nawet do 100 metrów i nadajnik z odbiornikiem nie muszą mieć zapewnionej widoczności. Można powiedzieć, taka sieć to mała sieć WLAN. Ostatnimi czasy

pojawiło się dużo doniesień o udanych atakach na bluetooth ale większość związana jest bardziej z telefonami komórkowymi niż z komputerami. Sieci bluetooth cały czas zyskują na popularności tak więc przypuszczalnie z czasem będzie coraz więcej prób włamań oraz zostaną wykryte słabe punkty tej sieci. Aby zabezpieczyć się przez nieautoryzowaną próbą połączenia do naszej sieci bluetooth, powinniśmy mieć je wszystkie na oku i nie dopuszczać w pobliże nieznajomych osób. Gorzej sprawa wygląda w ruchliwych miejscach, gdzie ktoś może skopiować dane z telefonu komórkowego bez naszej wiedzy i jedyne, co możemy zrobić by poczuć się bezpieczniej to nie trzymać poufnych i ważnych danych w swojej komórce.

6.3. Wimax

WiMax (WiMaxWorld Interoperability for Microwave Access) jest technologią bezprzewodową opracowaną przez IEEE po to by zapewnić dostęp do szerokopasmowych usług na dużym obszarze. WiMax został oparty na standardach IEEE 802.16 i ETSI HiperMAN. Technologia ta oferuje teoretyczny zasięg do 40-50 km oraz maksymalne przepustowości rzędu 70 Mb/s. Działa w zakresie 2-66 GHz zarówno w paśmie licencjonowanym jak i nielicencjonowanym.

Standard sieci WiMax dopiero jest w fazie tworzenia a koniec prac zaplanowano na 2008 rok. Mimo to firmy produkują już urządzenia zgodne z tą technologią opierając się na dotychczasowych wynikach badań. Przykładem na to, że WiMax się szybko rozwija może być fakt powstawania coraz więcej sieci obejmujących swoim zasięgiem duże obszary. W Polsce działa już kilka takich sieci, pierwsza powstała w Bielsku-Białej w 2004 roku[13] i jak dotąd nie można powiedzieć o nich złego słowa. Jednym z czynników hamujących szybszy rozwój WiMax jest wysoka cena urządzeń sieciowych korzystających z tego standardu, jednak z czasem powinno się to zmienić.

Ponieważ technologia 802.16 nie jest skończona i nie jest zatwierdzona przez IEEE na razie mało mówi się o bezpieczeństwie przesyłanych nią danych. Poniżej przedstawiam informacje, jakie udało mi się znaleźć w Internecie na stronie www.wimax.biz.pl odnośnie bezpieczeństwa nowego standardu.

„Grupa IEEE 802.16 zaproponowała następujące mechanizmy zabezpieczania transmisji:

[13] Networld nr 9/2005 str. 10

- Autentyfikacja terminala (wymiana certyfikatów w celu uniemożliwienia wejścia do systemu podejrzanym urządzeniom),
- Autentyfikacja użytkownika (realizowana za pomocą protokołu EAP – Extensible Authentication Protocol),
- Szyfrowanie danych (realizowane za pomocą protokołu DES –Data Encryption Standard lub AES –Advanced Encryption Standard),
- Szyfrowanie każdej usługi unikalnym kluczem prywatnym, asocjacja odmiennym systemem zabezpieczeń."[14]

W miarę upływu czasu jak WiMax będzie coraz częściej wykorzystywany myślę, że pojawią się informacje o wykrytych lukach w zabezpieczeniach. Podobnie jak w Wi-Fi do czasu odkrycia słabości WEP użytkownicy sieci standardu 802.11 żyli w złudnym poczuciu bezpieczeństwa tak samo wróżę technologii WiMax. Wszystko będzie działało idealnie aż do dnia, w którym jakaś mądra osoba odkryje słabości zabezpieczenia tego standardu.

6.4. VectraStar

System VectraStar do przesyłu danych wykorzystuje częstotliwości w przedziale 3,6 – 3,8 GHz i odległość między nadajnikiem i odbiornikiem może wynosić nawet kilkadziesiąt kilometrów. W Polsce z tego systemu korzysta na razie tylko NASK. Pierwszy nadajnik takiej sieć zainstalowano w 2005 roku w Warszawie na wieżowcu Warsaw Trade Center. Promień zasięgu sieci VectraStar wyniósł 30 km a deklarowana prędkość przez NASK wynosiła 100 Mb/s. O bezpieczeństwie przesyłanych danych tą siecią wiadomo bardzo niewiele, mimo to można stwierdzić, że system VectraStar bardzo bezpieczny. Dzieje się tak, ponieważ urządzenia działające w tej sieci są trudno osiągalne a kart sieciowych korzystających z takiego standardu dla laptopów czy palmtopów w ogóle nie ma.

[14] http://www.wimax.biz.pl/index.php/content/view/11/4/

6.5. LMDS i MMDS

Local Multipoint Distribution System (LMDS) jest bezprzewodową technologią pozwalającą na transmisję danych z dużą przepustowością przy użyciu mikrofalowych urządzeń radiowych. MMDS działa podobnie jak LMDS jednak na innych częstotliwościach. Rozwiązania te są w stanie uzyskać przepustowość łącza nawet rzędu 600 Mb/s a maksymalne odległości dochodzą do 40 km. Technologia ta zapewnia wysoki poziom bezpieczeństwa przesyłanych danych, ponieważ sprzęt korzystający z LMDS jest bardzo drogi oraz z sieci takich korzystają przeważnie większe firmy i aby uzyskać dostęp do sieci trzeba byłoby się najpierw fizycznie włamać do budynku firmy.

6.7. FSO

System FSO (Free Space Optics) został nazwany przez miesięcznik Networld „bezprzewodowym kablem”. Określenie to w bardzo dobry sposób przedstawia działanie tego standardu. FSO używa techniki laserowej do wysyłania danych w formie wiązki widocznej lub podczerwieni. Pierwsze systemy pojawiły się na rynku w 1990 roku i zapewniały prędkość od 10 do 100 Mb/s, obecnie prędkości dochodzą nawet do 2,5 Gb/s, a prace nad 10 Gb/s już trwają. FSO może działać do odległości kilku kilometrów jednak system jest bardzo wrażliwy na zmiany pogody. Deszcz, mgła, śnieg, błyski i zanieczyszczenia powietrza skutecznie osłabiają sygnał. W warunkach klimatycznych panujących w Polsce w celu uzyskania stabilnego połączenia FSO nie powinno przekroczyć odległości 1 km. Rozwiązanie to można uznać za bardzo bezpieczne, ponieważ prawie nie ma możliwości przechwycenia sygnału przez inne urządzenie a wysoka cena urządzeń powoduje, że stać na nie może być tylko wielkie firmy.

6.8. Porównanie technologii bezprzewodowych

Technologia	Popularność	Zasięg	Max. przepustowość	Poziom zabezpieczeń	Cena
802.11x	bardzo duża	kilka kilometrów	540 Mb/s	średni	niska
Irda	średnia ale spada	kilka metrów	16 Mb/s	żaden	średnia
Bluetooth	średnia	kilkadziesiąt metrów	1 Mb/s	średni	średnia
WiMax	średnia ale wzrasta	kilkadziesiąt kilometrów	70 Mb/s	duży (do czasu)	wysoka
VectraStar	niska	kilkadziesiąt kilometrów	100-200 Mb/s	duży	bardzo wysoka
LMDS/ MMDS	niska	kilkadziesiąt kilometrów	600 Mb/s	duży	bardzo wysoka
FSO	niska	kilkadziesiąt kilometrów	2,5 Gb/s	duży	bardzo wysoka

Wnioski

Sieci bezprzewodowe standardu 802.11 są dzisiaj jedną z najszybciej rozwijających się dziedzin informatyki. Z dnia na dzień przybywa coraz więcej sieci Wi-Fi, jednak jak pokazałem w moich badaniach, szybki rozwój sieci nie idzie w parze z polepszeniem bezpieczeństwa. Dzieje się tak, ponieważ ludzie nie umieją ustawić dostępnych standardów zabezpieczeń lub po prostu im się nie chce tego zrobić. Organizacja Wi-Fi Alliance myśli, że nowo wprowadzony system WPS rozwiąże ten problem, ale dopiero czas pokaże czy tak się stanie.

Bezpieczeństwo sieci bezprzewodowych jest złożonym procesem, który rozpoczyna się od sformułowania dobrej polityki bezpieczeństwa i który w zasadzie nigdy się nie kończy. Prędzej czy później każdy mechanizm zabezpieczeń zostanie złamany lub zostaną wykryte luki pozwalające na dostęp lub wyciek informacji z sieci. Na dzień dzisiejszy najlepszym rozwiązaniem jest stosowanie kilku mechanizmów zabezpieczeń. Na przykład, stosując WPA lub WPA2 warto włączyć też filtrację adresów MAC oraz nie rozgłaszanie nazwy SSID sieci a dla pewności można zmieniać co jakiś czas klucz. Przedstawione rozwiązanie jest obecnie najlepszym sposobem zabezpieczenia małych i średnich sieci domowych lub firmowych. W większych sieciach wykorzystuje się serwery uwierzytelniania takie jak RADIUS, które sprawdzają użytkowników i jedynie bardzo zdolni hakerzy są w stanie zagrozić takiej sieci.

Prace nad polepszeniem zabezpieczeń w sieciach standardu 802.11 trwają cały czas a równolegle pracuje się też nad złamaniem tych już istniejących. Myślę, że za kilka lat mechanizm WPA spotka ten sam los, co WEP i trzeba będzie na szybko wymyślić nowy standard. Można się także spodziewać, że zainteresowanie sieciami Wi-Fi zmaleje w najbliższych latach. Jeżeli technologia WiMax stanieje i będzie dostępna dla urządzeń mobilnych to na pewno wyprze starszą technologię Wi-Fi, jednak problem zabezpieczenia danych przesyłanych drogą radiową nie zostanie chyba nigdy rozwiązany do końca.

Bibliografia

Książki:

„100 sposobów na bezpieczeństwo sieci” – Andrew Lockhart

„100 sposobów na sieci bezprzewodowe” – Rob Flickenger, Roger Weeks

„802.11. Bezpieczeństwo” – Bruce Porter, Bob Fleck

„802.11. Sieci bezprzewodowe. Poradnik encyklopedyczny” – Matthew S. Gast

„Bezpieczeństwo sieci. Biblia” – Eric Cole, Rolad L. Krutz, James Conley

„Bezprzewodowe sieci komputerowe” – Bartłomiej Zieliński

„Cyberprzestępczość Jak walczyć z łamaniem prawa w Sieci” – Debra Littlejohn Shinder, Ed Tittel

„Domowe sieci bezprzewodowe” – Paul Heltzel

„Fale i anteny” – Jarosław Szóstka

„Przewodnik po sieciach Wi-Fi “ – Jeff Duntemann

„Sieci bezprzewodowe. Praktyczny przewodnik” – Adam Engst, Glenn Fleishman

„Sieci komputerowe” – Andrew S. Tanenbaum

„Sieci standardu Wi-Fi” - - John Ross

„Sieć bezprzewodowa Wi-Fi. Ćwiczenia” – Ireneusz Skop

„Wi-Foo. Sekrety bezprzewodowych sieci komputerowych” – Andrew Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky

„Wireless Hacking. Edycja polska” – Lee Barken i inni

Czasopisma:

„Szerokopasmowe sieci bezprzewodowe” – Suplement Promocyjny nr 44 – Networld

Hackin9 nr 3/2005, 1/2006

Komputer Świat Ekspert Plus nr 1/2006

Networld nr 9/2005, 12/2005, 2/2007

PC World Komputer Special nr 1 - Cyfrowy Dom

Strony internetowe:

http://hack.pl/

http://pl.wikipedia.org

www.elibre.pl – portal o e-publikacjach i technoologii e-papieru

http://warchalking.pl

http://warxing.pl

http://wifi-live.pl

http://wss.pl

http://www.cyberbajt.pl

http://www.dailywireless.org

http://www.dlink.com

http://www.idg.pl

http://www.linksys.com

http://www.microsoft.com/poland/technet

http://www.networld.pl

http://www.pcworld.pl

http://www.wardriving.pl

http://www.wi-fi.org

http://www.wififorum.pl

http://www.wifinetnews.com

http://zielonaszkolka.pl

Wykaz rysunków

Rys.1. Sieć typu ad hoc. Str. 10

Rys.2. Sieć typu infrastrukturalnego. Str. 11

Rys.3. Program NetStumbler w działaniu. Str. 14

Rys.4. Znaki warchalking'owe. Str. 15

Rys.5. Zasada działania mechanizmu WEP. Str. 27

Rys.6. Działanie mechanizmu 802.11i. Str. 36

Rys.7. Schemat działania standardu 802.1x. Str. 39

Rys.8. Znak certyfikacji WPS. Str. 42

Rys.9. Schemat sieci testowej wykorzystanej do przeprowadzenia badań. Str. 47

Rys.10. Kolejne etapy łączenia się z niezabezpieczoną siecią. Str. 48

Rys.11. Ethereal – widoczne przechwycone login i hasło. Str. 49

Rys.12. Niewidoczna sieć zarówno dla Netstumblera jak i dla Windows. Str. 50

Rys.13. Przy filtracji MAC siec_testowa wykrywana jest jako niezabezpieczona. Str. 51

Rys.14. CommView for WiFi - adresy MAC punktu dostępowego i laptopa Asus. Str. 52

Rys.15. Etherchange – szybki sposób na zmianę MAC. Str. 52

Rys.16. Wynik działania programu aircrack. Str. 54