Zagrożenia w sieci bezprzewodowej

Nie eksploatuj sieci bezprzewodowej bez zabezpieczeń. Powiemy, czym mogłoby to grozić. Postaramy się też odpowiedzieć na pytanie, czy promieniowanie sieci WLAN i Bluetooth może być niebezpieczne.

Niektórzy użytkownicy sieci traktują swoje dane jak kierowca mercedesa, który stawia swoje auto w biały dzień na ulicy i zostawia kluczyki w stacyjce. Mówiąc inaczej, postępują w wyjątkowo lekkomyślny sposób. Z kolei niektórzy inni użytkownicy są bardzo zaniepokojeni z powodu poziomu promieniowania sieci bezprzewodowych. Omówimy typowe luki zabezpieczeń i odpowiemy na pytanie, czy trzeba się obawiać elektromagnetycznego smogu.

Bankowość internetowa, zakupy w sklepach internetowych, prywatne i służbowe dokumenty tekstowe, sprawozdania finansowe - każdy posiada jakieś poufne dokumenty i dane, do których osoby nieuprawnione nie powinny mieć dostępu. Ostrożność trzeba zachować już w tradycyjnych kontaktach z Internetem i lokalnymi sieciami kablowymi, a cóż dopiero powiedzieć o sieciach bezprzewodowych! Ponieważ bazują one na transmisji radiowej, bez skutecznych zabezpieczeń są wystawione w mniejszym lub większym stopniu na łup złodziei danych lub hakerów.

Ataki - szkody bezpośrednie i pośrednie

Co do zasady, są dwa rodzaje ataku na sieć bezprzewodową, choć każdy z nich wykorzystuje te same słabe punkty. W pierwszym przypadku napastnik szuka określonych poufnych informacji lub danych, względnie chce wyrządzić szkodę, choćby poprzez zainstalowanie wirusa albo trojana.

W drugim przypadku napastnikowi może chodzić o znalezienie niezabezpieczonych sieci WLAN z dostępem do Internetu po to, by wykorzystać ten dostęp na własne potrzeby. W niektórych miastach powstały już całe subkultury tego rodzaju internetowych pasażerów na gapę. Członkowie tych subkultur wypracowali nawet własny język, a war driving, bo taką nazwę nosi wyszukiwanie niezabezpieczonych sieci WLAN, stał się w wielkich miastach poważnym problemem ekonomicznym.

War driving - w poszukiwaniu otwartych sieci

War driving oznacza poszukiwanie niezabezpieczonych sieci radiowych z dostępem do Internetu. Uczestnicy tej nielegalnej sceny podróżują po mieście autobusami, rowerami czy samochodami, preferując przy tym śródmieścia lub tereny przemysłowe i uzbrojeni w notebooka lub palmtopa przeczesują pasmo częstotliwości w poszukiwaniu otwartych prywatnych sieci.

Efekty takich akcji można nieraz znaleźć w Internecie w postaci list z adresami. Niektórzy z "poszukiwaczy", szczególnie w centrach wielkich miast, oznaczają otwarte sieci za pomocą specjalnych znaków malowanych kredą, na przykład na ścianie budynku. Wtajemniczeni natychmiast orientują się, że tu znajduje się sieć bezprzewodowa z otwartym dostępem do Internetu.

Szara strefa

W rzeczywistości uczestnicy procederu war driving stosują w swoich atakach względnie niegroźne narzędzia. W większości przypadków nie zadają sobie trudu wtargnięcia do dobrze zabezpieczonych sieci. W praktyce już podstawowe zabezpieczenia sieci WLAN z reguły wystarczają do tego, by odstraszyć większość potencjalnych agresorów (zob. artykuł "Zabezpieczenia sieci bezprzewodowych" na str. 74).

Z prawnego punktu widzenia war driving jest szarą strefą. Wyszukiwanie niezabezpieczonych sieci WLAN nie jest nielegalne, ponieważ mamy tu do czynienia zaledwie z wyszukiwaniem. Włamanie do cudzej sieci jest już natomiast poważnym przestępstwem i grozi surowymi karami. Z kolei nie są znów

nielegalne dostępne w Internecie narzędzia do przeprowadzania ataków na sieci WLAN, gdyż mogą one równie dobrze służyć administratorom do wykrywania słabych punktów we własnych sieciach.

Rouge Access Point - stacja bazowa pod przykrywką

Kolejny rodzaj ataków na sieci radiowe umożliwia Rouge Access Point. To dodatkowy punkt dostępowy, np. przeszmuglowany i zainstalowany przez pracownika firmy. Punkty dostępowe to te elementy sieci bezprzewodowej, które służą jako stacje bazowe, elementy łączące i pośrednie pomiędzy sieciami kablowymi a bezprzewodowymi.

Rouge Access Point jest podłączany do sieci lokalnej, z którą współpracuje również sieć bezprzewodowa mająca być przedmiotem ataku. Za pomocą takiego dodatkowego punktu dostępowego napastnik może bez przeszkód gromadzić informacje z przekazów w ramach lokalnej sieci po to, by następnie przesłać je dalej. Tego rodzaju punkty dostępowe są trudne do wykrycia, przede wszystkim wówczas, gdy napastnik sam stosuje środki bezpieczeństwa w rodzaju biernego rozsyłania SSID .

Man in the middle - totalne podsłuchiwanie

Ataki typu man in the middle są od dawna znane w technologiach sieciowych, jednak w przypadku sieci radiowych są szczególnie niebezpieczne. Man in the middle jest umieszczany jako serwer/klient pomiędzy regularnym klientem a punktem dostępowym. Jego zadaniem jest przechwycenie i przejęcie komunikacji między uczestnikiem a punktem dostępowym.

Napastnicy korzystający z techniki man in the middle mogą uzyskać dodatkowe informacje przechwytując cały ruch między klientem a punktem dostępowym w taki sposób, że uprawnieni użytkownicy nawet niczego nie zauważają. Z jednej strony man in the middle jest kolejnym punktem dostępowym, w którym loguje się klient. Z drugiej strony działa jako serwer, przekazując logowanie klienta i same dane do właściwego punktu dostępowego po to, by nie zostać wykrytym.

Tak więc wobec klienta man in the middle podszywa się pod właściwy punkt dostępowy. Dysponując danymi uwierzytelniania z klienta, man in the middle, tym razem w roli serwera, może zachowywać się wobec właściwego punktu dostępowego jak normalny klient. To właśnie dzięki temu napastnik może przechwytywać całą komunikację.

Sniffery - młot na szyfrowanie WEP

Istnieją łatwe w zastosowaniu metody znacznego zwiększenia bezpieczeństwa sieci radiowych. Najbardziej znana z nich to szyfrowanie WEP, które jako element składowy standardu IEEE 802.11 jest nieodłączną częścią dzisiejszej technologii WLAN (zob. artykuł "Zabezpieczenia sieci bezprzewodowych" na str. 74). Niestety, szyfrowanie WEP ma swoje słabe punkty.

Cóż z tego, że w początkowej fazie napastnik nie jest w stanie odczytać danych szyfrowanych metodą WEP. Nie oznacza to przecież wcale, że nie jest w stanie odebrać tych danych. Narzędzia do podsłuchiwania, tzw. sniffery, umożliwiają rejestrację całego ruchu radiowego. Dysponując już danymi, mogą teraz spróbować je odszyfrować, łamiąc klucz WEP.

Użytkownicy sieci WLAN powinni zatem zadać sobie trud i sprawdzić za pomocą odpowiedniego programu, jak Web Attack, Airsnort czy WEP Crack, ile wysiłku wymaga złamanie szyfrowania WEP ich własnych sieci.

Dlatego też obecnie dostępne są najróżniejsze uzupełnienia standardu WEP, choćby w postaci dynamicznie generowanych kluczy. Wadą takiego rozwiązania jest ograniczenie polegające na tym, że w takiej sieci mogą być stosowane wyłącznie urządzenia określonego rodzaju. Nie jest to możliwe w wielowarstwowych, złożonych sieciach. W przyszłości WEP musi być zastąpiony innymi algorytmami szyfrowania (zob. artykuł "Zabezpieczenia sieci bezprzewodowych" na str. 74).

Rozgłaszanie (nie prowokuj)

W sieciach bezprzewodowych punkty dostępowe rozsyłają szczególne rodzaje pakietów. Zawartością tych tak zwanych administration frames mogą być dane w rodzaju typu sieci (ad hoc/tryb infrastruktury), SSID (Service Set Identifier, nazwa sieci), kanał roboczy, szyfrowanie WEP, adresy MAC i IP. Tak więc jest to całkiem pokaźny zbiór ważnych informacji o twojej sieci. Tego rodzaju rozsyłanie ułatwia wprawdzie konfigurowanie kolejnych połączeń i jest do zaakceptowania w dużych sieciach firmowych o rozbudowanych mechanizmach zabezpieczeń, jednak w małych sieciach prywatnych jest to zupełnie zbędny element dodatkowego ryzyka. Dlatego lepiej wyłącz rozsyłanie SSID przez punkt dostępowy.

Adres MAC - łatwa zmiana

Jednym z najbardziej skutecznych mechanizmów ochrony przed napastnikami jest stosowanie list kontroli dostępu. Polega to na narzuceniu punktowi dostępowemu listy kart sieciowych, z którymi wolno mu się łączyć. Wykorzystuje się w tym celu adresy MAC (Machine Access Code), które umożliwiają jednoznaczne zidentyfikowanie każdej karty sieciowej. Niestety, i ten mechanizm nie daje stuprocentowej ochrony. Istnieją specjalistyczne narzędzia, które pozwalają zmienić adres MAC karty. W hakerskim żargonie taka manipulacja nosi nazwę spoofing. Jeżeli haker ustali za pomocą sniffera, jakie adresy MAC akceptuje punkt dostępowy, może odpowiednio zmanipulować kartę sieciową swojego notebooka. Wymaga to jedynie zmiany trybu pracy karty ze standardowego na promiscuous (ang. dosłownie przypadkowy). W trybie standardowym karta przyjmuje jedynie te pakiety danych, które są jednoznacznie dla niej przeznaczone, natomiast w trybie promiscuous może przyjmować również ramki przeznaczone dla innych kart.

Nie istnieje zatem naprawdę niezawodny mechanizm ochrony sieci bezprzewodowych. Tym większego znaczenia nabiera optymalne wykorzystanie tych środków, które stoją do dyspozycji.

Zagrożenie zdrowia?

Każdy rodzaj radiowej komunikacji bezprzewodowej wykorzystuje fale radiowe do transmisji danych. Ciało ludzkie pochłania takie fale. Są określone dopuszczalne wartości maksymalne, które mają zapobiegać zagrożeniom zdrowia. Przestrzeganie istniejących przepisów w tym zakresie nadzoruje Urząd Regulacji Telekomunikacji i Poczty (www.urtip.gov.pl).

WLAN - promieniowanie i wartości graniczne

Zgodnie z rozporządzeniem ministra infrastruktury z dnia 6 sierpnia 2002 r. (Dziennik Ustaw nr 138, pozycja 1162), urządzenia stosowane w lokalnych radiowych sieciach komputerowych pracujących na częstotliwościach 2400,00 - 2483,5 MHz mogą dysponować maksymalną mocą 100 mW EIRP (zastępcza izotropowa moc promieniowania). W tej kategorii mieszczą się praktycznie wszystkie dostępne na rynku urządzenia pracujące w standardzie 802.11b (i jego "dopalonej" odmianie 802.11b+ o szybkości transmisji 22, 33 i 44 Mb/s, która jednak nigdy nie została uznana za standard przez IEEE) i/lub 802.11g (zob. artykuł "Najważniejsze standardy WLAN" na str. 24). Urządzenia WLAN korzystające z pasma 5 GHz (5150 - 5350 MHz) mogą pracować z maksymalną mocą 200 mW e.i.r.p., ale wolno ich używać tylko wewnątrz pomieszczeń zamkniętych.

Oprócz tego urządzenia WLAN mogą również pracować na zewnątrz i wewnątrz pomieszczeń w paśmie 5470 - 5725 MHz z mocą 1W EIRP. Equivalent Isotropically Radiated Power - zastępcza izotropowa moc promieniowania jest obliczana dla teoretycznej, w praktyce niestosowanej i na dobrą rzecz nieosiągalnej idealnie kulistej charakterystyki promieniowania anteny.

Urządzenia WLAN nie zawsze pracują z maksymalną mocą. Jeżeli komunikacja przebiega bez zakłóceń, redukują moc. Ponadto natężenie pola spada wraz ze wzrostem odległości. Nawet gdy punkt dostępowy pracuje z pełną mocą, natężenie pola elektromagnetycznego w odległości 50 cm od niego wynosi ok. 0,03 W/m2, a więc znacznie poniżej dopuszczalnej wielkości maksymalnej 10 W/m2.

Warto zauważyć, że punkt dostępowy rzadko pracuje z maksymalną mocą - może się to zdarzyć, gdy na przykład przesyłasz plik z filmem o gigantycznej objętości.

Bluetooth - promieniowanie a wartości graniczne

Urządzenia Bluetooth korzystają wyłącznie z pasma 2,4 GHz. Istnieją trzy klasy mocy tych urządzeń, ustalone przez Bluetooth Special Interest Group (www.bluetooth.org). Urządzenia class 1 pracują z mocą 100 mW i mają zasięg do 100 m.

Maksymalna moc 2,5 mW urządzeń class 2 daje zasięg ok. 20 m. Wreszcie urządzenia class 3 o mocy 1 mW uzyskują zasięg ok. 10 m. Przy dobrej jakości połączenia urządzenia Bluetooth również ograniczają swoją moc do niezbędnego minimum. Zestawy słuchawkowe to najczęściej urządzenia klasy 3 i w praktyce często pracują z mocami od 0,1 do 0,5 mW.

Podsumujmy. Promieniowanie elektromagnetyczne urządzeń WLAN jest bez porównania mniejsze od promieniowania telefonów komórkowych. Te ostatnie pracują z mocami pomiędzy 1 a 2 W, a więc dziesięciokrotnie większymi, niż karta WLAN o mocy 200 mW i nawet 2000 razy większymi od zestawu słuchawkowego class 3 o mocy 1 mW.

Jak na razie wydaje się, że uwagę opinii publicznej bardziej przyciąga promieniowanie masztów telefonii komórkowej, o czym mogą świadczyć histeryczne nieraz protesty przed ich instalacją na dachach czy w pobliżu budynków. Ta histeria jakoś słabo przekłada się na konkretne działania. Wyszukiwarka Google na hasło "ochrona przed promieniowaniem elektromagnetycznym" zwraca aż...18 dokumentów.

Zagrożenia w sieci bezprzewodowej

Komentuje Paweł Latała, inżynier D-Linka: najczęstszym grzechem popełnianym przez użytkowników sieci bezprzewodowej jest pozostawianie urządzeń w konfiguracji domyślnej, czyli bez jakichkolwiek zabezpieczeń. W takiej sytuacji naprawdę trudno spodziewać się, że nikt do naszej sieci nie uzyska dostępu. Należy też pamiętać o tym, że proste zabezpieczenia, jak ukrywanie SSID, czy enkrypcja WEP nie są idealne i zwłaszcza stosowane pojedynczo, mogą być niewystarczające. W celu maksymalnej ochrony sieci, należy łączyć różne mechanizmy zabezpieczeń!

Ustawienia domyślne często też nie są korzystne dla wydajności sieci. Kilka punktów dostępowych pracujących w pobliżu, na tym samym kanale, będzie się nawzajem zakłócać, czasami nawet całkowicie uniemożliwiając transmisję w sieci. W pogoni za uzyskiwaniem jak największej mocy sygnału większość użytkowników niestety zapomina, że najważniejszy jest jednak stosunek mocy sygnału do szumu i zamiast stosować mocniejsze anteny, należy po pierwsze spróbować wyeliminować źródła zakłóceń lub zmienić wykorzystywany kanał komunikacji.

W taki sposób zmniejszysz oddziaływanie promieniowania

1. Punkt dostępowy ustaw w odległości co najmniej pięciu metrów od stanowiska pracy. W stanie bezczynności wysyła on sygnał identyfikacyjny o pełnej mocy co 1/10 s, jednak już w trakcie transmisji danych pracuje z sumaryczną mocą wszystkich klientów, których obsługuje.

2. Podłącz zasilanie punktu dostępowego do listwy z wyłącznikiem, abyś mógł go całkowicie wyłączyć, gdy nie jest potrzebny.

3. Gdy przesyłasz dane z komputera, staraj się być w jak największej odległości od niego.