T: Protokoły komunikacji bezprzewodowej. Stos protokołów TCP/IP.

Zadanie1:

Odszukaj w zasobach sieci Internet informacje na temat sieci Wi-Fi i protokołów stosowanych w sieciach bezprzewodowych.

Technologie WLAN (Wireless Local Area Network) stanowią połączenia bezprzewodowe tworzone na bazie fal radiowych wysokiej częstotliwości. Specyfikacje sieci bezprzewodowych ustanawiane są przez komitet IEEE (Institute of Electrical and Electronics).

Specyfikacja 802.11 pozwala na transmisję danych z szybkością 1 lub 2 Mb/s w zakresie częstotliwości 2400 do 2483 MHz. Sieci bezprzewodowe pracują w trybie tzw. half-duplex (w jednym momencie urządzenie nie może nadawać i przyjmować danych). Do komunikacji wykorzystuje się protokoły:
- LLC (Logical Link Control),
- CSMA/CA (Carrier Sense Multiple Access with Collision Avidance),
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection),
- RTS/CTS (Request to Send/Clear to Send),

Wi-Fi bazuje na takich protokołach warstwy fizycznej, jak:
- DSSS (ang. Direct Sequence Spread Spectrum),
- FHSS (ang. Frequency Hopping Spread Spectrum),
- OFDM (ang. Orthogonal Frequency Division Modulation).

W sieciach bezprzewodowych (Wi-Fi) zabezpieczenia można podzielić na dwa typy: autoryzacji i transmisji. Autoryzacja ma na celu potwierdzić tożsamość użytkownika, natomiast typ transmisji ma nas zabezpieczyć przed podsłuchiwaniem.

Za bezpieczeństwo transmisji danych odpowiedzialne są protokoły uwierzytelniające i szyfrujące:
- WEP (Wired Equivalent Privacy),
- WPA (TKIP),
- WPA2 (AES).

Stosowane metody zabezpieczeń zgodne ze standardem 802.11:
- uwierzytelniania – identyfikacja i weryfikacja autentyczności informacji przesyłanych przez użytkownika,
- protokół WEP (ang. Wired Equivalent Privacy) – działa na zasadzie współdzielonego klucza szyfrującego o długości 40 do 104 bitów i 24 bitowym wektorze inicjującym,
- protokoły WPA/WPA2 – nowe, dużo bardziej bezpieczne mechanizmy szyfrowania przesyłanych danych,
- autoryzacja – zgoda lub brak zgody na żądaną usługę przez uwierzytelnionego użytkownika,
- rejestracja raportów – rejestr akcji użytkownika związanych z dostępem do sieci.

Główne standardy w sieciach bezprzewodowych:
- 802.11a - 54 Mb/s, częstotliwość 5 GHz,
- 802.11b - 11 Mb/s, częstotliwość 2,4 GHz posiada zasięg ok. 30 m w pomieszczeniu i 120 m w otwartej przestrzeni; w praktyce można osiągnąć transfery rzędu 5,5 Mb/s. Materiały takie jak woda, metal, czy beton obniżają znacznie jakość sygnału; standard 802.11b podzielony jest na 14 niezależnych kanałów o szerokości 22 MHz, Polska wykorzystuje tylko pasma od 2400 do 2483,5 MHz - kanał od 1 do 13,
- 802.11g - 54 Mb/s, częstotliwość 2,4 GHz, obecnie najpopularniejszy standard Wi-Fi, który powstał w czerwcu 2003 roku, wykorzystanie starszych urządzeń w tym standardzie powoduje zmniejszenie prędkości do 11 Mb/s,
- 802.11i (w tym systemie wprowadzono nowe zabezpieczenia za pomocą szyfrowania),
- 802.11n – 540 Mb/s, częstotliwość 2,4 GHz.

Zadanie2:

Zastanów się nad czynnikami powodującymi szybki rozwój sieci bezprzewodowych.

Źródło http://pl.wikipedia.org

WEP (ang. Wired Equivalent Privacy) to standard szyfrowania stosowany w sieciach bezprzewodowych standardu IEEE 802.11. Standard ten powstał w 1997 roku.

Standard specyfikuje klucze 40- i 104-bitowe, do których w procesie wysyłania ramki dołączany jest wektor inicjujący (IV) o długości 24 bitów. Stąd popularnie mówi się o 64- i 128-bitowych kluczach WEP, ale nie jest to stwierdzenie poprawne technicznie. W rozszerzeniach firmowych tego standardu znaleźć można również klucze o długości 232 bitów (z IV daje to 256 bitów), które jednak z uwagi na znane słabości w doborze IV nie zwiększają w istotny sposób siły kryptograficznej całości rozwiązania.

Z uwagi na słabości standardu WEP, IEEE stworzyło najpierw szkielet protokołów uwierzytelniających 802.1x, który umożliwia dobór mechanizmów uwierzytelniania i szyfrowania, a następnie 802.11i, w którym określono m.in. szyfrowanie pakietów algorytmem AES (CCMP) i dodanie mechanizmów MIC i TKIP.

W tym samym czasie organizacja Wi-Fi Alliance zaproponowała zabezpieczenia oparte o projekt 802.11i pod nazwą WPA, które istotnie rozszerza podstawowy mechanizm zabezpieczeń dla sieci bezprzewodowych standardu 802.11.

4 kwietnia 2007 r. naukowcom z Politechniki w Darmstadt udało się pobić rekord w szybkości łamania zabezpieczenia WEP. Andrei Pychkine, Erik Tews oraz Ralf-Philipp Weinmann (atak 'PTW' - nazwany od pierwszych liter ich nazwisk) zredukowali liczbę przechwyconych pakietów wymaganych do skutecznego przeprowadzenia ataku do około 40 tysięcy (wcześniej trzeba było przechwycić od 500 tysięcy do dwóch milionów pakietów). Jak zapewniają odkrywcy, sieć bezprzewodowa szyfrowana 104-bitowym kluczem może zostać rozszyfrowana w czasie nie przekraczającym minuty. W nowej metodzie po przechwyceniu 40 tysięcy pakietów istnieje 50-procentowe prawdopodobieństwo odkrycia klucza. Po przechwyceniu 85 tysięcy pakietów prawdopodobieństwo to wzrasta już do 95 procent.

WPA (ang. WiFi Protected Access) to standard szyfrowania stosowany w sieciach bezprzewodowych standardu IEEE 802.11.

WPA jest następcą mniej bezpiecznego standardu WEP. Standard WPA został wprowadzony przez organizację WiFi. Pierwsza wersja profilu WPA została wprowadzona w kwietniu 2003 roku. WPA wykorzystuje protokoły TKIP (Temporal Key Integrity Protocol), 802.1x oraz uwierzytelnienie EAP.

WPA=802.1x+EAP+TKIP+MIC

WPA został wprowadzony jako standard przejściowy pomiędzy WEP a zabezpieczeniem 802.11i czyli WPA2 w celu zwiększenia bezpieczeństwa użytkowników sprzętu mającego na stałe zaimplementowany WEP bez konieczności ich wymiany. Osiągnięto to przez cykliczną zmianę klucza szyfrującego WEP, co przy odpowiedniej częstotliwości zmian uniemożliwia jego złamanie pomimo istniejących podatności.

Także dzięki temu zabiegowi wyposażenie systemu lub urządzenia w WPA jest możliwe bez zmiany sprzętu - wystarczy zmienić oprogramowanie (sterownik w przypadku kart sieciowych, a w przypadku punktów dostępowych - firmware).

WPA dzieli się na:

- Enterprise – korzysta z serwera RADIUS, który przydziela różne klucze do każdego użytkownika.
- Personal - nie dzieli kluczy na poszczególnych użytkowników, wszystkie podłączone stacje wykorzystują jeden klucz dzielony (PSK - *Pre-Shared Key*).

Najważniejszą różnicą pomiędzy WPA a WPA2 jest używana metoda szyfrowania. Podczas, gdy WPA wersji pierwszej korzysta z TKIP/RC4 oraz Michael (MIC), WPA2 wykorzystuje CCMP/AES.

Uwierzytelnienie w protokole WPA-PSK jest podatne na ataki słownikowe. Szyfrowanie TKIP w WPA jest podatne na atak kryptoanalityczny o ograniczonym zasięgu, dla którego opracowano również zoptymalizowaną wersję.

802.11i (oznaczane również jako **WPA2**, ang. WiFi Protected Access) – protokół sieci bezprzewodowych. Implementuje w sobie: 802.1x oraz CCMP.

W porównaniu z WEP:

- wykorzystuje 128-bitowe klucze
- ma poprawione wszystkie złamane zabezpieczenia WEP
- wykorzystuje dynamiczne klucze (na poziomie użytkownika, sesji, klucza pakietów)
- automatycznie dystrybuuje klucze
- posiada wzmocnione bezpieczeństwo autoryzacji użytkownika (przy użyciu 802.1x oraz EAP)

Źródło http://www.cyberbajt.pl/raport/377/0/385/
Po ujawnieniu słabości algorytmu WEP, przejściową metodą opracowaną w celu zapewnienia bezpieczeństwa w sieciach 802.11 został protokół **TKIP**. Przed protokołem TKIP postawiono dwa cele. Miał on nie tylko usuwać problemy związane z WEP, ale także współpracować z obecnym na rynku sprzętem. Ponieważ wiele algorytmów szyfrowania WEP zostało zaimplementowanych sprzętowo, toteż protokół TKIP miał za zadanie współpracę z podstawowymi mechanizmami algorytmu WEP. Choć istniały już wydajne schematy szyfrowania, projektanci musieli opracować metodę, która nie powodowałaby, że miliony starszych bezprzewodowych kart sieciowych i punktów dostępowych, nie wspierających nowych schematów, okazałoby się przestarzałych.
Protokół **TKIP** (wymagany do uzyskania certyfikatu WPA) składa się z trzech protokołów: kryptograficznego algorytmu integralności komunikatów, algorytmu mieszania kluczy oraz rozszerzenia wektora początkowego. Podobnie jak protokół WEP wykorzystuje algorytm RC4 ale otrzymał nowe mechanizmy, które chronią go przed atakami, na jakie narażony był WEP. Najlepszym rozwiązaniem w zakresie szyfrowania okazało się modyfikowanie podstawowego klucza WEP dla każdego pakietu danych. Protokół TKIP zabezpiecza klucz WEP przed przechwyceniem, generując inny klucz dla każdego pakietu. CRC-32 został tu zastąpiony przez nowy kod integralności MIC (Message Integrity Check - kontrola integralności komunikatów) o nazwie Michael który ma za zadanie poprawę omówionej wcześniej nieefektywnej funkcji sumy kontrolnej ICV ze standardu 802.11. Algorytm ten wykorzystuje unikatowy klucz, który jest mieszany ze źródłowym i docelowym adresem MAC, a także całym fragmentem pakietu zawierającym niezaszyfrowane dane. Zapewnia to integralność pakietu danych i rozwiązuje problemy podrabiania ramek. Ponadto opracowano dokładne reguły generacji wektora IV, co zapobiega jego powtórzeniom i uodparnia cały standard przed atakami z wykorzystaniem kolizji wektora inicjalizacji. Wprowadzono także mieszanie klucza dla pojedynczych pakietów oraz nowy mechanizm zarządzania kluczami i ich wymianą. Mimo, że algorytm WEP jest podstawą protokołu TKIP, wszystkie te funkcje znacznie zmniejszyły wrażliwość algorytmu WEP na ataki.
Jak dotąd algorytm TKIP jest uznawany za bezpieczny, jednak eksperci w dziedzinie bezpieczeństwa WLAN są zdania, że złamanie tego algorytmu to kwestia niedalekiej przyszłości.

Kolejnym zbiorem protokołów wprowadzonym w standardzie 802.11i jest **CCMP**. Protokół CCMP jest podstawą specyfikacji 802.11i. Podobnie jak protokół TKIP zapewnia integralność i poufność danych ale stosuje silniejsze algorytmy. Protokół CCMP oparto na symetrycznym algorytmie blokowym AES (Advanced Encryption Standard) i na jego specjalnym trybie wiązania bloków CCM, w którym jest realizowana poufność i integralność. Algorytm AES został poddany szerokiej analizie na skalę międzynarodową, przeprowadzoną przez ekspertów w dziedzinie kryptografii i jest obecnie uznawany za bezpieczny.
Algorytm AES na potrzeby protokołu CCMP wykorzystuje 128 bitowe klucze. Podobnie jak w TKIP w CCMP zastosowano 48 bitowy wektor IV (nazywany numerem pakietu PN) oraz odmianę kodu MIC. Zastosowanie silnego szyfru AES powoduje, że nie ma potrzeby tworzenia oddzielnego unikatowego klucza dla każdego pakietu, zatem w CCMP nie przewidziano takiej funkcji. CCMP wykorzystuje ten sam klucz zarówno dla szyfrowania danych jak i tworzenia sumy kontrolnej. Wykorzystywana w CCMP suma kontrolna integralności komunikatu jest uważana za znacznie silniejszą niż kod Michael, zastosowany w TKIP. Ponieważ w celu uniknięcia wpływu szyfrowania na prędkość i przepustowość sieci 802.11i jest ono realizowane najczęściej przez oddzielny układ elektroniczny, implementacja algorytmu CCMP wymagała wymiany starszych urządzeń sieciowych.
Algorytm CCMP jest najlepszym rozwiązaniem przy projektowaniu zabezpieczeń w sieciach WLAN, i powinien jak najszerzej zastępować algorytmy TKIP i WEP.

Klient sieci bezprzewodowej pełni funkcję urządzenia oczekującego na uwierzytelnienie (suplikanta), a punkt dostępowy – funkcję urządzenia uwierzytelniającego (autentykatora). W standardzie 802.1x funkcję przełącznika przedstawionego na rysunku przejmuje punkt dostępowy. Serwer uwierzytelniający, pozwalający na efektywne zarządzania kontami użytkowników, ich uprawnieniami i certyfikatami, powinien być dołączony do segmentu sieci kablowej, do której dołączony jest punkt dostępowy. Funkcję tego serwera najczęściej pełni serwer RADIUS.
Uwierzytelnianie użytkownika w standardzie 802.1x realizuje się za pomocą protokołu EAP (Extensible Authentication Protocol). Wymianę komunikatów EAP zachodzącą między urządzeniami 802.1x przedstawia rysunek 3.

Protokół EAP sam w sobie nie specyfikuje żadnej metody uwierzytelnienia, jest nośnikiem specyficznej metody EAP. Istnieje wiele metod uwierzytelniania EAP powstałych najczęściej przy współudziale producentów urządzeń i oprogramowania. Najczęściej spotykane to :

- EAP-TLS jest pierwotnym protokołem EAP dla środowiska 802.11. Jest powszechnie implementowany przez większość wytwórców sprzętu i oprogramowania. W metodzie tej jest wymagane uwierzytelnienie klienta oparte na certyfikatach klucza publicznego. Tego typu certyfikaty są przechowywane najczęściej na kartach inteligentnych. Wymaganie dotyczące użycia certyfikatów daje EAP-TLS duża przewagę nad innym rozwiązaniami, jednak znacznie podnosi koszt zarządzania systemami bezpieczeństwa. Wszystkie urządzenia zgodne z WPA i WPA2 wspierają te metodę. EAP-TLS jest standardowo dostępny w systemie operacyjnym MAC OS 10.3 i wyższych, Windows 2000 SP4, Windows XP, Windows Mobile 2003 i wyższych.
- EAP-TTLS został stworzony przez firmę Funk i Certicom. Jego podstawowa wada to brak wsparcia w środowisku Windows (2000/XP/Mobile 2003/CE) w standardowej instalacji. Wsparcie pojawia się dopiero w Windows 2003. Mimo to EAP-TTLS jest najpopularniejszym protokołem EAP.
- PEAPv0/EAP-MSCHAPv2 jest niekiedy nazywany po prostu PEAP, mimo, że posiada kilka odmian (v0, v1 i v2). Został opracowany przez Microsoft we współpracy z RSA Data Security i Cisco Systems. Jest drugim po EAP-TTLS najczęściej używanym protokołem. Jest wspierany przez cała rodzinę produktów firmy Microsoft oraz MAC OS 10.3 lub wyższy. PEAPv0 sam w sobie nie jest uznawany za bezpieczny, stad prace nad PEAPv1 i PEAPv2.
- PEAPv1/EAP-GTC został zaproponowany przez Cisco Systems jako alternatywa dla PEAPv0. Nie posiada wsparcia w standardowej instalacji w środowisku Windows i nie zyskał na razie dużej popularności. Jest faworyzowany w sprzęcie i oprogramowaniu Cisco Systems. Pozwala na zastosowanie dowolnego protokołu uwierzytelnienia, sam w sobie nie jest uznawany za do końca bezpieczny, dlatego wymaga wsparcia np. od EAP-GTC. Warto tu wspomnieć, że inny protokół faworyzowany przez Cisco tj. LEAP również został uznany za niebezpieczny przez brak odporności na atak słownikowy. LEAP jest zastępowany w przez protokół EAP-FAST.

W przypadku sieci bezprzewodowych mechanizm 802.1x wykorzystywany jest ponadto do dystrybucji kluczy. Realizuje się to przez wygenerowanie dwóch zestawów kluczy. Pierwszy zestaw tworzą klucze nazwane kluczami sesji lub kluczami sparowanymi. Klucze te są unikalne dla każdego połączenia klienta z punktem dostępowym. Klucze sesji zapewniają prywatność połączenia oraz usuwają problem „jednego klucza WEP dla wszystkich". Drugi zestaw tworzą klucze grupowe lub zgrupowane, które są współdzielone przez wszystkie komputery pracujące w jednej komórce sieci 802.11, a wykorzystywane są do szyfrowania ruchu typu multicast. Oba rodzaje kluczy mają wielkość 128 bitów. Klucze sparowane tworzy się na podstawie sparowanego klucza głównego PMK (Pairwise Master Key) o wielkości 256 bitów. Klucz PMK każde urządzenie otrzymuje z serwera RADIUS. W podobny sposób na podstawie głównego klucza GMK (Group Master Key) tworzone są klucze zgrupowane.

W środowisku małych sieci biurowych lub sieci domowych serwery RADIUS z bazą danych użytkowników należą do rzadkości. W takim przypadku klucze sesji generuje się na podstawie wstępnie uzgodnionych kluczy PMK, które wprowadza się ręcznie, tak samo jak w przypadku WEP.

Zadanie3:

Odszukaj w zasobach sieci Internet informacje na temat oprogramowania kismet.