T: Standardy szyfrowania sieci bezprzewodowej.

Komunikacja bezprzewodowa ze względów bezpieczeństwa wykorzystuje komunikację szyfrowaną. Szyfrowanie w sieciach bezprzewodowych wykorzystuje następujące standardy: WEP, WPA oraz WPA2.

Zadanie2:

> Odszukaj w serwisie internetowym Wikipedii informacje na temat następujących zagadnień: WEP, WPA, WPA2 oraz RADIUS, PSK, TKIP, AES.

WEP (ang. Wired Equivalent Privacy) – standard szyfrowania stosowany w sieciach bezprzewodowych standardu IEEE 802.11.
W standardzie WEP oferowane są współdzielone klucze poufne o długości 40 bitów.
Według przeprowadzonych badań do złamania jednego bajta klucza niezbędne jest rozkodowanie około 60 pakietów. Wraz ze wzrostem ilości rozkodowanych bajtów wzrasta tempo rozkodowywania. Wydłużenie klucza spowoduje jedynie podwojenie czasu, jaki jest potrzebny na rozszyfrowanie klucza.

WPA (ang. Wi-Fi Protected Access) – 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 może korzystać z trybu:

- Enterprise – wtedy używa serwera RADIUS, który przydziela klucze odpowiednim użytkownikom.
- 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 kryptologiczny o ograniczonym zasięgu, dla którego opracowano również zoptymalizowaną wersję.

WPA2 (ang. Wi-Fi Protected Access II) – protokół sieci bezprzewodowych. Implementuje w sobie: 802.1x oraz CCMP.
W porównaniu z WEP:

- wykorzystuje 128-bitowe klucze kryptograficzne,
- ma poprawione wszystkie znalezione luki w zabezpieczeniach WEP,
- wykorzystuje dynamiczne klucze (na poziomie użytkownika, sesji, pakietów),
- automatycznie dystrybuuje klucze,
- posiada podniesiony poziom bezpieczeństwa autoryzacji użytkownika (przy użyciu 802.1x oraz EAP).

Ze względów bezpieczeństwa zaleca się stosowanie w sieciach bezprzewodowych zabezpieczeń WPA2.

RADIUS (ang. Remote Authentication Dial In User Service) – usługa zdalnego uwierzytelniania użytkowników, którzy wdzwaniają się do systemu (poprzez usługę „połączenie wdzwaniane").
Obecnie jest najpopularniejszym protokołem uwierzytelniania i autoryzowania użytkowników sieci telefonicznych i tunelowych. Używany jest także w sieciach bezprzewodowych.
W odpowiedzi na próbę zalogowania się użytkownika do sieci serwer dostępowy (NAS) generuje zapytanie o dane użytkownika, w tym jego identyfikator i hasło. Po wprowadzeniu tych danych z poziomu terminala użytkownika, jego identyfikator wraz z zakodowanym hasłem zostają wysłane do serwera RADIUS-a.

PSK, Pre-shared key – w kryptografii klucz, który jest ustalony między dwoma stronami przed jego użyciem. W praktyce jest to hasło zabezpieczające dostęp do określonych zasobów.

TKIP (ang. Temporal Key Integrity Protocol) – protokół używany w celu zabezpieczenia warstwy łącza danych w sieciach bezprzewodowych zgodnych ze standardem IEEE 802.11. Został stworzony przez grupę

specjalistów, którzy ujawnili słabość szyfrowania algorytmem WEP. TKIP do szyfrowania wykorzystuje algorytm RC4. Szyfrowanie TKIP w WPA jest podatne na atak kryptoanalityczny o ograniczonym zasięgu.

AES, Advanced Encryption Standard – symetryczny szyfr blokowy. AES bazuje na zasadzie, zwanej siecią substytucji-permutacji. Wykazuje się dużą szybkością pracy zarówno w przypadku sprzętu komputerowego, jak i oprogramowania. Jest pierwszym dostępnym publicznie szyfrem, który był zatwierdzony i wykorzystywany przez NSA do ochrony ściśle tajnych informacji.