RADIUS (cd)

Metody uwierzytelniania w oparciu o serwer RADIUS

PAP – Password Authentication Protocol

Metoda autentykacji za pomocą „czystych haseł”.

CHAP – Chellenge-handshake Authentication Protocol

Serwer wysyła „chellenge” czyli ciąg znaków do klienta, który hashuje go (wraz z hasłem) przy użyciu funkcji skrótu (MD5) i odsyła do serwera. Serwer sprawdza poprawność wygenerowanego hash-a. Wymaga zapisanego hasła zarówno po stronie klienta jak i serwera.

MSCHAP

Wersja CHAP udoskonalona przez Microsoft. Nie wymaga by obie strony komunikacji znały niezaszyfrowane hasło. Funkcja skrótu to MD4. Pozwala na zmianę hasła.

MSCHAPv2

Udoskonalona wersja MSCHAP. Pozwala na autoryzację klienta i serwera – klient wysyła serwerowy challenge w pakiecie RESPONSE, serwer wysyła odpowiedź w pakiecie SUCCESS.

EAP (Extensible Authentication Protocol)

Protokół uwierzytelniania stosowany w sieciach bezprzewodowych, przewodowych, połączeniach P-t-P. Stosowany w sieciach ze względu na wbudowane mechanizmy retransmisji i eliminacji zduplikowanych pakietów. Sam NIE jest mechanizmem autentykacji, tylko bazą dla różnych metod uwierzytelniania.

EAP-MD5

Metoda autentykacji przy użyciu hasha MD5.

Zalety: Wsparcie. W tym w systemie Windows.
Wady: Minimalne zabezpieczenia a wręcz ich brak. Nie wspiera wymiany klucza. (więc nie nadaje się do WPA/WPA2 ani dynamicznego WEP) .

EAP-PSK

EAP zabezpieczony znanym kluczem PSK (Preshared Key)

Wady: Nie znam żadnych zastosowań „real-world”.

EAP-SIM, EAP-AKA

Autoryzacja EAP oparta na karcie SIM, USIM (UMTS).

EAP-GTC – Generic Token Card

EAP zabezpieczony „czystym hasłem”. Hasła są tymczasowe i generowane za pomocą tokenów.

Wady: Trzeba mieć token. Przesyłane są niezaszyfrowane hasła.
Zalety: Można używać w sesji PEAP/TTLS – wtedy daje wysoki poziom bezpieczeństwa.

EAP-LEAP (Lightweight Extensible Authentication Protocol)

Wymyślony przez Cisco, wprowadza dynamiczne klucze WEP i dwustronną autentykację. Obecnie Cisco sugeruje: nie używać.

Wady: Brak wsparcia w systemie Windows. Używa lekko zmodyfikowanego MS-CHAP, który jest prosty do złamania. Metoda ataku ASLEAP (http://asleap.sourceforge.net) .

EAP-FAST – Flexible Authentication via Secure Tunneling

Tunelowany EAP bez certyfikatów ssl. Zamiast tego używa się "wstępnych poświadczeń" (PAC) (Protected Access Credential).

Zalety: Lepszy niż LEAP. Wspierany przez CISCO.
Wady: dystrybucja PAC. Tzw. Faza 0 - automatyczna dystrybucja jest niebezpieczna (oparta o MSCHAPv2). Dystrybucja ręczna jest uciążliwa.

EAP-TLS Extensible Authentication Protocol - Transport Layer Security

Dwustronna autentykacja za pomocą klucza SSL klienta oraz serwera.

Zalety: Bardzo dobre wsparcie.
Wady: Z założenia wymaga certyfikatu klienta.

EAP-TTLS – Tunneled Transport Layer Security

Uwierzytelnienie serwera za pomocą certyfikatu, klient autoryzuje się w tunelu TLS.

Wady: Nie wspierany przez Microsoft Windows.

EAP-PEAP – Protected Extensible Authentication Protocol

Działa prawie jak EAP-TLS, z tą różnicą że do autentykacji używa się hasła zamiast klucza prywatnego. W tunelu można używać MSCHAPv2 (PEAPv0) lub GTC (PEAPv1). PEAPv1 nie jest wspierany przez system Windows.

Wady: Słabe wsparcie wszystkich wersji.
Zalety: PEAPv0 wspierany natywnie przez Microsoft Windows. Może być automatycznie rozprowadzany przez AD.

Tunelowanie EAP:

Faza 1
Zestawienie tunelu.

Faza 2
Użycie metod takich jak MSCHAPv2, GTC, SIM, ...