

Šiandieninis bevielio tinklo saugumas

Turinys

WPA.....	3
WPA Autentifikavimas.....	3
WPA duomenų kodavimas.....	3
Duomenų teisėtumas.....	3
WPA, TKIP, MIC, 802.1x, EAP – akronimai!.....	3
WPA-802.1x ar WPA-PSK?.....	4
Kurį 802.1x protokolą pasirinkti?.....	4
Ar gali tinklas būti segmentuotas?.....	5
Išvados.....	5

WPA

2003 buvo žengtas didžiulis žingsnis sparčiai augančioje bevielų tinklų saugumo srityje, kuomet Wi-Fi Alliance kompanija sukūrė WPA (Wi-Fi Protected Access) standartą. Wi-Fi Alliance pradėjo naujojo WPA kodavimo testavimus 2003 birželio mėn. ir netrukus WPA tapo privalomu saugumo standartu kiekvienam bevielio tinklo įrenginiui.

WPA apibrėžia vartotojų autentifikavimą, paremtą 802.1x standartu, padidintą duomenų kodavimą, naudojant laikino rakto vientisumo protokolą (Temporal Key Integrity Protocol - TKIP) bei duomenų ratifikavimą, naudojant žinutės vientisumo tikrinimą (Message Integrity Check - MIC).

WPA Autentifikavimas

802.1x yra lankstus protokolas bendram saugiam vartotojų bei tinklų autentifikavimui. Jis yra paremtas autentifikavimo protokolu EAP (Extensible Authentication Protocol). Keletas EAP metodų, tokių kaip TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security), PEAP (Protected Extensible Authentication Protocol) bei EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) buvo sukurti specialiai bevieliams tinklams. Saugus bendras autentifikavimas ne tik užkerta kelią nepageidaujamiems vartojam pasiekti tinklą, bet ir apsaugo nuo man-in-the-middle atakų.

802.1x autentifikavimui reikalingi trys tinklo komponentai – besikreipiantis klientas, autentifikatorius bei autentifikavimo serveris. Autentifikatorius veikia kaip tarpininkas, persiųsdamas 802.1x protokolo žinutes iš besikreipiančio kliento į autentifikavimo serverį. 802.11 tinkluose prieigos taškai (Access points) atlieka autentifikatoriaus vaidmenį. Autentifikavimo serveris atsakingas už vartotojų teises naudotis tinklu. 802.1x autentifikavimo serveriai paprastai būna RADIUS serveriai.

WPA taipogi pateikia autentifikavimo alternatyvą – iš anksto padalintų raktų metodą PSK (Pre-Shared Key). PSK yra numatytas naudoti mažuose namų arba ofisų tinkluose, kuriuose saugus autentifikavimas nėra kritiškai svarbus. PSK metodui būtini tik du komponentai – klientas bei autentifikatorius. Šiame modelyje prieigos taškas naudodamas PSK yra atsakingas tikrai už kliento priėmimą į tinklą.

WPA duomenų kodavimas

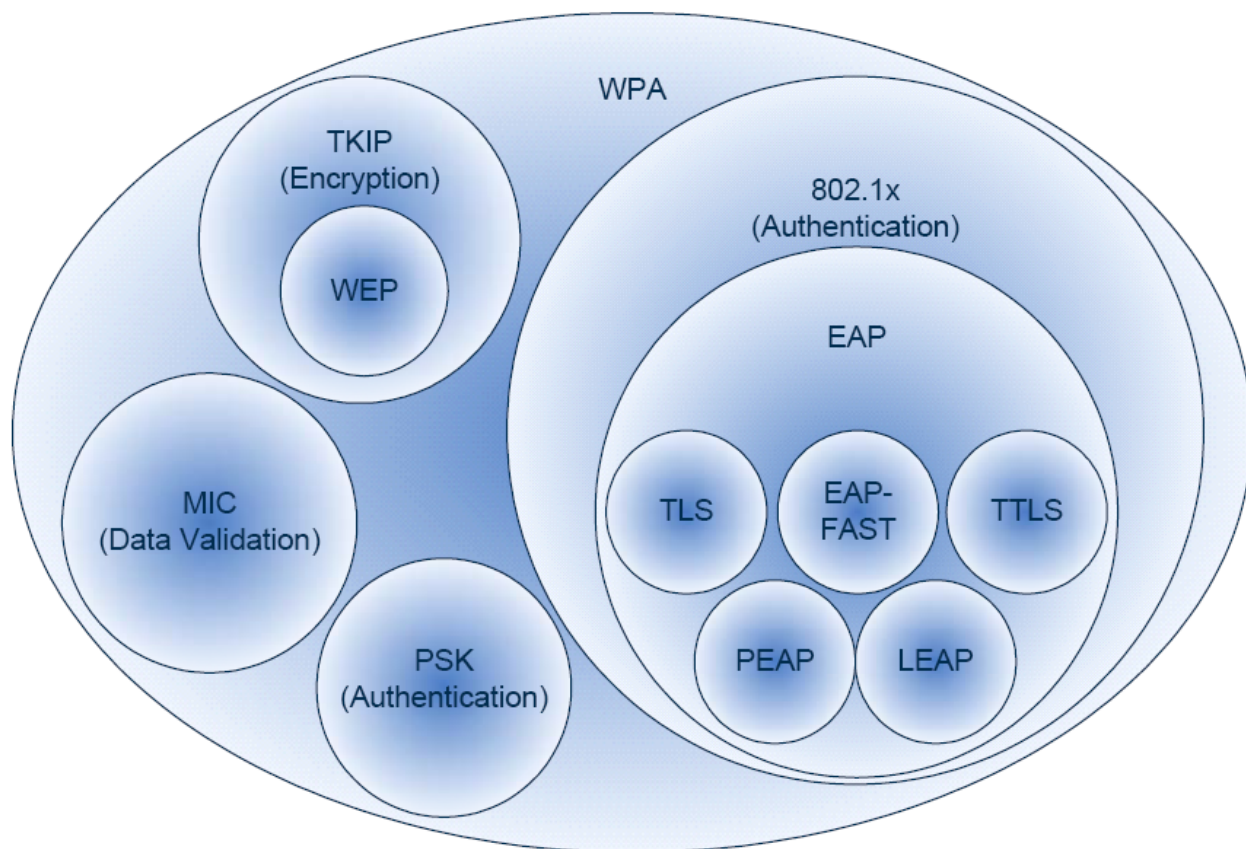
TKIP išplečia 802.11 standarto WEP (Wired Equivalent Privacy) mechanizmą bei saugiai keičia WEP raktą su lig kiekvienu duomenų paketu. Tokiu būdu kodavimas užveria kelią slaptam pasiklausymui. TKIP yra sukurtas apsaugoti nuo WEP rakto atakų, tokių kaip AirSnort bei WEPCrack.

Duomenų teisėtumas

Duomenų teisėtumui tikrinti CRC (Cyclic redundancy check) algoritmą pakeitė MIC algoritmas. CRC algoritmas, naudotas 802.11 protokole yra labai nesunkiai apeinamas. MIC algoritmas šiuo atveju yra žymiai stipresnis. Duomenų teisėtumo procedūros tikrina duomenis nuo žalingų bei atsitiktinių duomenų perdavimo iškraipymų.

WPA, TKIP, MIC, 802.1x, EAP – akronimai!

Diagrama žemiau perteikia šių protokolų susietumą:



1pav. WPA algoritmai

Pastebėkime, kad WPA būtini trys komponentai – kodavimas, autentikavimas bei duomenų teisėtumo tikrinimas. Kaip WPA-802.1x autentikavimo alternatyvą galima rinktis WPA-PSK (Pre-Shared Key).

WPA-802.1x ar WPA-PSK?

- 802.1x yra kur kas saugesnis nei PSK, tačiau tam reikia RADIUS autentikavimo serverio.
- WPA-802.1x paprastesnis klientų konfigūravimas, nes klientams nereikia nurodyti autentikavimo rakto, jį RADIUS serveris pateikia automatiškai

Kurį 802.1x protokolą pasirinkti?

Naudojant 802.1x autentifikavimą, reikia pasirinkti 802.1x protokolą. Yra galimybė vienu metu naudoti keletą iš jų.

- **EAP-TLS:** Ko gero pats saugiausias bendrojo naudojimo 802.1x protokolas. EAP-TLS reikalinga PKI sertifikatai serveryje bei kliento kompiuteryje. Tai šiek tiek komplikuoja tinklo administravimą, nes sertifikatą reikia patalpinti kiekviename bevielio tinklo įrenginyje.
- **PEAP:** PEAP yra panašus į EAP-TLS, tačiau nereikalauja sertifikatų kliento kompiuteryje. PEAP sukuria saugų duomenų perdavimo tunelį kliento duomenim gauti.
- **EAP-TTLS:** EAP-TTLS yra labai panašus į PEAP. EAP-TTLS naudoja vartotojo vardą bei slaptažodį, vartotojų atpažinimui.
- **EAP-FAST:** EAP-FAST skiriasi nuo išvardintųjų tuo, kad nereikalauja PKI. EAP-FAST sukurtas dirbti kuo mažiau apkrautai, bet išliekant autentifikuotiems.

- **LEAP:** LEAP yra Cisco sukurtas 802.1x protokolas. LEAP yra pakankamai paprastas autentifikavimo metodas, nereikalaujantis PKI. LEAP naudoja vartotojo vardo bei slaptažodžio kombinaciją atpažinti vartotojus.

LEAP yra pats seniausias bei buvęs plačiausiai naudojamas 802.1x protokolas. Tačiau neseniai paskelbtas lengvai įveikiamas bei nesaugus. LEAP gali būti naudojamas tik kraštutiniu atveju, jei jokie kiti autentifikavimo metodai įrangos nepalaikomi.

Ar gali tinklas būti segmentuotas?

Yra galimybė naudoti WPA apsaugą ir segmentuotam tinklui, izoliuojant tam tikrus įrenginius atskirame tinklo segmente. Efektyviausiais įgyvendinimo būdas yra VLAN (Virtual Local Area Network).

- Dauguma prieigos taškų (AP) turi galimybę turėti bent 2 VLAN segmentus.
- Dauguma prieigos taškų turi galimybę valdyti srautus tarp skirtingų segmentų.

Išvados

WPA saugumo standartas yra kur kas patikimesnė bei vienintelė plačiai naudojama alternatyva, senajam bei pripažintam nesaugiu, WEP standartui.