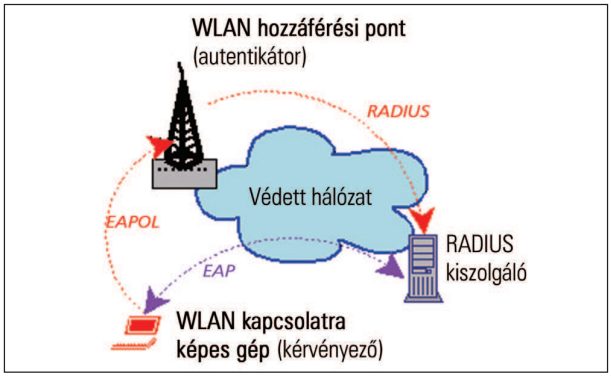
WLAN-ok védelme WPA és FreeRADIUS alkalmazásával (1. rész)

Vezeték nélküli hálózatunkat a kiöregedett, biztonságot nem nyújtó WEP helyett védjük az új szabvány szerint, s egyben építsük össze a hitelesítést linuxos hálózatunkkal.

Aggódunk ***802.11b vezeték nélküli helyi hálózatunk (wireless local area network, WLAN)*** biztonsága miatt, mert még a jó öreg ***WEP***-et (wired equivalent privacy, vezetékes egyenértékű adatvédelem) használjuk? Aki kizárólag a ***WEP***-re bízza magát, bizony ***jól teszi, ha fél***: komoly és jól ismert sebezhetőségek vannak benne, amelyek révén a kalózok néhány órányi hallgatózás után, nyers erőből végzett töréssel könnyedén visszafejthetik ***WEP***-kulcsainkat. De van remény! A ***WPA (Wi-Fi protected access, Wi-Fi védett elérés)*** új hitelesítési eljárásokkal és továbbfejlesztett kulcselőállítási képességgel ruházza fel a ***802.11b*** hálózatokat, és a ***WPA*** támogatására képes ***WLAN***-készülékek szinte pillanatok alatt megjelentek az üzletekben. További örömre ad okot, hogy a ***WPA-kérvényezők (ügyfélrendszerek)***, a ***hitelesítők (hozzáférési pontok)*** és a ***kiszolgálók (RADIUS hitelesítő kiszolgálók)*** számára linuxos eszközök is rendelkezésre állnak. Következő két cikkemben a ***WPA***-t és alkotó protokolljait, illetve ezek együttműködését fogom ismertetni, valamint szólok arról is, hogy a ***FreeRADIUS*** csomag segítségével hogyan helyezhetünk üzembe egy ***Linux***-alapú ***WLAN*** hitelesítő kiszolgálót.

Áttekintés

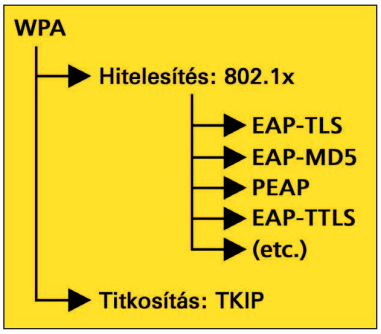
Mi is alapvetően a baj a ***802.11b*** hálózatok biztonságával? Röviden, a ***802.11b*** szabvány ***WEP*** protokolljában van két súlyos hiba. Az első, a titkosítási-megvalósítási hiba lehetetlenné teszi, hogy a gyakorlatban 40 bitnél erősebb kulcsot használjunk, még ha rendszerünk elvileg képes is lenne a hosszabb kulcsok kezelésére. A második a ***WEP*** titkosítási kulcs származtatási eljárásában keresendő, miatta a támadó megfelelő számú csomag elfogása után meg tudja határozni a hálózat titkos ***WEP***-kulcsát – azt a titkosítási kulcsot, amelyet a hálózat minden egyes állomása használ.
A jelenleg fejlesztés alatt álló ***802.11i*** protokoll teljes értékű, erőteljes biztonsági keretrendszert fog biztosítani a ***WLAN***-okhoz. Természetesen véglegesítése után is kell némi idő ahhoz, hogy a protokoll széles körben elérhetővé váljon a kereskedelmi termékekben és a szabad programokban. Térjünk rá a ***WPA***-ra. A ***WPA*** a ***802.11i*** két kulcsfontosságú összetevőjét emeli át a ***802.11b***-be. Az első a rugalmas és nagyteljesítményű hitelesítési szolgáltatásokat biztosító ***802.1x*** hitelesítő protokoll. A második a ***TKIP*** protokoll, melynek segítségével egyedi ***WEP***-kulcsokat tudunk hozzárendelni az egyes ***WLAN***-ügyfelekhez, majd dinamikusan tudjuk elvégezni ezek újraegyeztetését, így a ***WEP***-nél látott kulcsszármaztatási sebezhetőség megszűnik.



1. ábra A WPA felépítése

Az *1. ábrán* a ***WPA*** alapú rendszerek összetevői közötti kapcsolatokat szemléltettem. Először is, van egy ***WLAN***-képes ügyfélrendszerünk, ennek ***WPA*** ügyfélprogramját kérvényezőnek nevezzük. Az ügyfél/kérvényező csatlakozik egy ***vezeték nélküli hozzáférési ponthoz (access point, AP)***, amely hitelesítő szerepet játszik, miközben gyakorlatilag proxyzza a hitelesítési párbeszédet a kérvényező és a háttérben üzemelő hitelesítő kiszolgáló között. Az 1. ábrán ez a hitelesítő kiszolgáló egy ***RADIUS*** kiszolgáló, de ***TACACS***-t is használhatunk.
A kérvényező és a kiszolgáló közötti hitelesítésproxyzás mellett az ***AP/hitelesítő*** a ***TKIP (Temporal Key Integrity Protocol, ideiglenes kulcsintegritás protokoll)*** alkalmazásával adatokat közöl a hitelesítő kiszolgálóról, ezzel segítve a ***WEP*** munkamenetkulcs beszerzését. Ezután átadja a kulcsot a kérvényezőnek. A kérvényezőnek rendszeres időközönként újra kell hitelesítenie magát, ilyenkor új ***WEP*** kulcsot kap.
A hitelesítő (***RADIUS***) kiszolgáló elhagyható. Egy másik lehetőség az ***előre megosztott kulcs (pre-shared key, PSK)*** mód használata, ennél az egyes ***WPA*** kérvényező rendszerek egyedi kulcsát kézzel adjuk meg az ***AP***-nek, majd ***RADIUS***

helyett ezt használjuk fel a hitelesítésre. Ez az eljárás is jobb, mint a ***WEP***, mert magát a megosztott kulcsot nem használjuk titkosító kulcsként. Feladata csupán a dinamikus *WEP* kulcsokat szállító *TKIP* tranzakciók védelmének megalapozása.
A *WPA*-t jelenleg az újabb *WLAN* csatolók és hozzáférési pontok széles köre támogatja, sőt, a belső programok frissítésével néhány régebbi, *802.11b*-s terméken is elérhetővé vált. A linuxos világban támogatását az ügyfél oldalon a *wpa_supplicant (hostap.epitest.fi/wpa_supplicant)*, a linuxos hozzáférési pontokon a *hostapd (hostap.epitest.fi/hostapd)*, míg a hitelesítő kiszolgálók oldalán a *FreeRADIUS (www.freeradius.org)* biztosítja.
Mielőtt rátérnénk szűkebb témánkra, s egyben következő cikkem tárgyára, a *WPA*-képes *FreeRADIUS* kiszolgálók építésére, vizsgáljuk meg részletesebben is a *WPA* hitelesítési és titkosítási megoldásait.



2. ábra A WPA protokolljai0

WPA hitelesítés: 802.1x, EAP és RADIUS

Mindenki tud követni? Csak azért, mert a *WPA* valójában egy kicsit bonyolultabb annál, amit az 1. ábra tartalma sugall. Tehát: a *WPA* használatakor az ügyfélrendszernek (a kérvényezőnek) még az előtt kell hitelesítenie magát, hogy engedélyt kapna a csatlakozásra, amikor is hozzájut egy rendszeresen lecserélésre kerülő titkosítási munkamenetkulcshoz.
A dolog attól kezd bonyolódni, hogy a *WPA* hitelesítésre használt *802.1x* protokoll számos különböző módszer használatát teszi lehetővé a kérvényezők hitelesítésére – ami persze jó dolog. Moduláris, bővíthető hitelesítő megoldást alkalmazva nem kell attól tartanunk, hogy a *WPA*, a *802.1x* vagy a *802.11i* egy csapásra elavulttá válik, ahogy a különféle hitelesítő protokollok divatba jönnek és elfelejtődnek.
A *802.1x* modularitása és bővíthetősége a számos változatban létező *Extensible Authentication Protocol (bővíthető hitelesítő protokoll, EAP)* hozománya. Ejtsünk néhány szót a legnépszerűbb változatokról.

Az a számtalan protokoll!

Nem véletlen, hogy egy egész cikket szentelek a *WPA* működésének boncolgatására, és nem vetem bele magam a *FreeRADIUS WPA* használatára való beállításának témájába – annyi a *WPA* felépítésében részt vevő protokollal és alprotokollal találkozhatunk ugyanis, hogy megfelelő alapismeretek hiányában pillanatok alatt összezavarodunk. Aki már most elveszítette a fonalat az talán a *WPA* protokolljait hierarchikus formában szemléltető *2. ábra* alapján rendet tud teremteni gondolatai között.
Az *EAP-MD5* egyszerű, *MD5* kivonat alapú azonosítóadatcserét végez. A kérvényező közöl egy felhasználónevet és egy *MD5* kivonatolt jelszót a kiszolgálóval, amely összehasonlítja ezeket az adatbázisában tárolt adatokkal. Sajnos hallgatózással meg lehet szerezni a *WPA* kérvényező által elküldött kivonatot, és offline, szótár alapú támadással meg lehet határozni az előállításához használt jelszót. Gondot jelent az is, hogy bár az *EAP-MD5* hitelesíti a kérvényezőt a kiszolgáló felé, ám semmit nem tesz annak érdekében, hogy a kiszolgálót is hitelesítse a felhasználó számára, például tanúsítvánnyal, ahogy azt az *SSL* esetében is láthatjuk. Az *EAP-MD5* tehát *WPA* környezetben meglehetősen gyenge választás *802.1x* hitelesítésre.
Az *EAP-TLS* alapvető hitelesítésre a *TLS* titkosító protokollt, az *SSL* leszármazottját használja. Ez egy erőteljesnek mondható hitelesítési mód, hiszen használatakor a kiszolgáló és az ügyfél egyaránt saját digitális tanúsítványával – ezek adják a hitelesítési transzakciók alapját – igazolja magát. Nagyobb számú felhasználónak digitális tanúsítványt adni, illetve ezeket a tanúsítványokat kezelni ugyanakkor összetett és időrabló teendő lehet. Elég, ha arra gondolunk, hogy a szervezetünket elhagyó személyek tanúsítványát vissza kell vonni. Az *EAP-TLS* használatához általában teljes értékű *nyilvános kulcs infrastruktúrát (Public Key Infrastructure, PKI)* kell fenntartani, ami viszont egy kisebb vagy akár közepes méretű szervezet számára megterhelő lehet. Ne feledjük el azt sem, hogy a hitelesítések kezdeményezésekor a felhasználónevek nyílt szövegként továbbítódnak, ami apró kis hiányosság ugyan, de nem árt megjegyezni.
A *PEAP (Protected, védett EAP)* eredetileg a *Microsoft* fejlesztése, célja a gyengébb, de egyszerűbb hitelesítési eljárások, például az *MD5* és az *MS-CHAP TLS* titkosítással való védelme. A *PEAP* használatakor az azonosító adatok továbbítása előtt egy titkosított csatorna jön létre a kérvényező és a kiszolgáló között. Általában a webes alkalmazások is hasonló módon használják a *TLS*-t: segítségével felépítenek egy titkosított alagutat, ezen keresztül biztonságosan le lehet bonyolítani az egyszerű, felhasználónév és jelszó alapján végzett hitelesítéseket, és nincs szükség a TLS biztonságosabb, ám jóval bonyolultabb, ügyféltanúsítványra épülő eljárásainak alkalmazására. A *PEAP* fő hátránya *Microsoft*-központúsága. Bár a szabad programok között is találni a *PEAP* támogatására képest, a legtöbben nem látják a *Microsoft* szándékát arra, hogy biztosítsa az együttműködés lehetőségét más gyártók *WPA* termékeivel vagy megoldásaival.
Az *EAP-TTLS* lényegében egy nem microsoftos *PEAP*-alternatíva. Esetében is létrejön egy titkosított *TLS* alagút, ezen keresztül *TLS* alapú vagy egyéb, gyengébb hitelesítési eljárást lehet folytatni. Fő előnye a *PEAP*-pal szemben, hogy nincs kitéve egy nagyvállalat szeszélyeinek. Jelenleg hitelesítési módszerből is többet támogat – igaz, a *PEAP*-ot is úgy tervezték, hogy a jelenleg megvalósítottaknál jóval több módszer támogatására legyen képes. Néhányan úgy látják, a *Microsoft* támogatása nélkül az *EAP-TTLS* nem lesz olyan sikeres, mint a PEAP.
További *EAP*-variánsok az *EAP-SIM*, a *Microsoft EAP-MSCHAPv2*-je és a *Cisco Lightweight EAP*-ja (*LEAP*).
Álljunk csak meg, bizonyára ezt kérik néhányan; hát a *RADIUS* nem hitelesítő protokoll? Hogyan illeszkedik a képbe? A *RADIUS* az a protokoll, amely felett a hitelesítő, vagyis az *AP* a hitelesítő kiszolgálóval tartja a kapcsolatot.
A *802.1x* és a *WPA* témakörében a *RADIUS*-ra mint szállítóeszközre gondolhatunk, amely felett a hitelesítő továbbítja az *EAP*-üzeneteket a kiszolgálónak. Tehát a végfelhasználó, mint kérvényező *EAP* nyelven beszél a hitelesítővel, a hite-

lesítő pedig *RADIUS*-csomagokba ágyazva továbbítja a kérvényt a kiszolgáló felé. Van egy további protokoll is, mely hasonló szerepet játszik, vagyis a kérvényező és a hitelesítő között közvetít, és ez az *EAPOL*, azaz az *EAP Over LAN*. Ez egy tökéletesen átlátszó protokoll, ugyanis a kérvényező és a hitelesítő oldali programba van beépítve, és mint ilyennek, beállításokat sem kell megadnunk neki. Mondhatnám úgy is, amíg nem *WPA* alapú programot akarunk írni, addig semmi érdemlegeset nem kell tudnunk az *EAPOL*-ról. Attól kezdve, hogy egy kérvényező csatlakozást kezdeményez az *AP* felé, az *AP kizárólag EAP* alapú forgalmat engedélyez. Csak a hitelesítés – a kiszolgáló válaszán alapuló – teljes befejezése után kap a kérvényező *DHCP* bérletet, illetve engedélyt a *WLAN*-hoz való teljes értékű csatlakozásra. A sikeres hitelesítés másik folyománya egy *WEP*-kulcs kiosztása a kérvényezőnek.

A TKIP és a WEP kulcsozás

Ha egy kérvényezőt *EAP-TLS* vagy más titkosított *EAP*-változat segítségével hitelesítünk, akkor a hitelesítési forgalom titkosított. Maguk a vezeték nélküli hálózat keretei viszont nem, hiszen ennek előfeltétele a *WEP* engedélyezése a kérvényező rendszer és a hozzáférési pont közötti kapcsolaton. A megvalósítást végző szempontjából érdekes módon ez a *WPA* használatának legegyszerűbb mozzanata. A sikeres hitelesítés után a kiszolgáló, a hitelesítő és a kérvényező a *TKIP*-t alkalmazzák a hitelesítő és a kérvényező rendszer közötti kapcsolaton érvényes *WEP*-kulcsok egyeztetésére és biztonságos továbbítására. A folyamat nagyrészt átlátszó, a feladat elvégzéséhez sem a kiszolgálón, sem a kérvényezőn nem kell megadnunk semmilyen beállítást. A legtöbb hozzáférési ponton ugyanakkor, ide értve a linuxos *hostapd*-t is, meg lehet adni egyedi beállításokat, például a *WEP* kulcsfrissítési időközt.
A *TKIP* kapcsán érdemes még megjegyezni, hogy, mint említettem is, esetében a kiszolgáló elhagyható. Ha a kérvényezőket és a hitelesítőt előre megosztott kulcsos üzemmódra állítottuk be, a *TKIP*-t akkor is használhatjuk a *WEP*-titkosítás kulcsozására és a kulcsok frissítésére a kérvényező és a hozzáférési pont között.

Összefoglalás – egyelőre

Dióhéjban ennyit a *WPA*-ról. A következő alkalommal a most megismert fogalmakat a *FreeRADIUS* használata kapcsán fogjuk alkalmazni, és összeállítunk egy *Linux* alapú, *WPA*-s hitelesítő kiszolgálót. Aki nem tud addig várni, tanulmányozza az internetes forrásokat. Első a biztonság!

Linux Journal 2005. április, 132. szám

A cikk forrásai: ➲ *www.linuxjournal.com/article/8017*

Mick Bauer (mick@visi.com)
Biztonsági szakember, a Linux Journal biztonsági témákkal foglalkozó szerkesztője, biztonsági tanácsadó a Minnesota állambeli Minneapolisban található Upstream Solutions LLC Inc.-nél.