D-Link
Building Networks for People

Hálózati eszközök (4. rész)
Vezeték nélküli hálózatok biztonsága

Tovább folytatjuk az otthoni hálózatunk építését: az előttünk álló legsürgetőbb feladat a vezeték nélküli adatkapcsolatunk biztonsági problémáinak megoldása.

A vezeték nélküli hálózatok meglehetősen védtelenek, fokozottan ki vannak téve a támadás veszélyének. Ennek oka az adatok továbbításában keresendő: mivel az információ vezeték helyett az éterben közlekedik, nem szükséges a 'fizikai' hozzáférés a hálózathoz. Elegendő csupán a rádiójelek terjedési hatósugarában lennünk, és elfoghatjuk a hálózat egyes gépei között gazdát cserélő információt. A dolog veszélyességét fokozza, hogy mi felhasználók egyébként is elég félvállról (gyakorlatilag semmibe) vesszük a biztonsági előírásokat, javaslatokat. Úgy gondoljuk, az emlegetett kockázat egyáltalán nem nyugszik valós alapokon – vagy szimplán csak nem érdekel bennünket. Ez a bizonyos kockázat a bekövetkezési valószínűség és az okozott kár szorzata. Azt tudjuk, hogy az adatforgalomhoz történő hozzáférés miatt a betörés bekövetkezési valószínűség jelentősen megnő, növelve ezáltal a kockázatot. Ez azonban még nem minden: idegen felhasználók hálózatunk használatához történő vonzalma abból ered, hogy mindennapi céljukra tudják használni azt. Ebből következően az okozott kár is jelentős lehet.

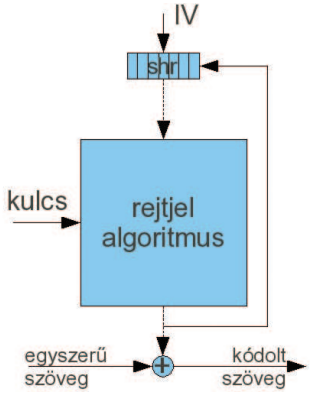
Hálózatunk illetéktelen használata a támadó fél számára az alábbi előnyökkel kecsegtet:

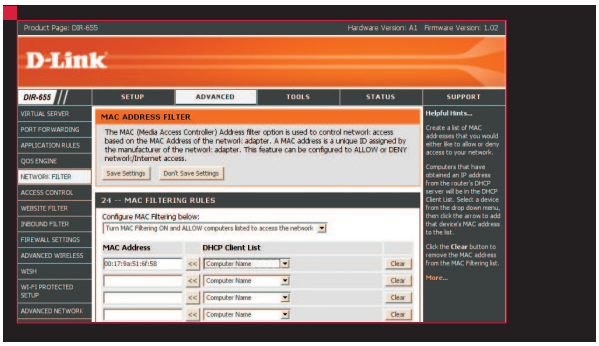
- Sikeres belépés után a mi előfizetésünket használva tud mindenféle illegális tevékenységet végezni: kéretlen reklámlevelet küldhet, másokat zaklathat, betörhet különböző kiszolgálókra, így a betörés nyomai hozzánk vezetnek, a betörő névtelen maradhat.
- A belső, otthoni hálózatunkon gyakran mindenféle korlátozás nélkül tesszük lehetővé a gépeken található dokumentumokhoz történő hozzáférést, ezáltal a hálózatunkba jutott ügyfélgépek egyszerűen lemásolhatnak fájlokat anélkül, hogy észrevennénk.
- Jelszavaink eltulajdonítása csak annyi munkába kerül, hogy el kell indítani egy programot, amely rögzíti a hálózaton küldött adatokat. Innen már gyerekjáték kiolvasni azokat. Leszámítva persze a titkos csatornákon történő adatátvitelt, de ez nem túl gyakori a mindennapokban.
- Sokan egyszerűen csak használják mások internet előfizetését a társasház szomszéd lakásából. Azon túl, hogy igazságtalan, és persze hogy benn van a hálózatunkban, letöltéseivel elhasználhatja a szolgáltató által rendelkezésre bocsátott letöltési kvótát, mi pedig hoppon maradunk.

Mondanom sem kell, hogy az utóbbi két eset igen kecsegtető és a bekövetkezése igen valószínű a mindennapokban is. Ennek megoldására két dolgot tehetünk. Az egyik, hogy lezárjuk a hálózatot akár jelszóval, akár egyéb technikával. Természetesen a forgalom figyelésével ez a védelem pillanatok alatt feltörhető, ezért el kell érni, hogy a forgalom a támadó számára értelmezhetetlen legyen, azaz kódolnunk kell az adatforgalmat. Az adatforgalom kódolása gyakran együtt jár a hálózat lezárásával, ugyanis a hálózatba történő belépéshez is kódolt adatokat kell kapnunk a hozzáférési ponttól.

A bukott szamár: WEP

A fentiekre természetesen a ***802.11***-es szabványcsalád kidolgozói is gondoltak, megalkották a ***WEP*** (***Wired Equivalent Protection;*** a vezetékessel egyenrangú védelem) titkosítást, ám a folyamat során valahol szőr került a hurkába, a protokoll ugyanis több durva hiányosságot is tartalmaz: nyíltan továbbítja a kulcs bizonyos részét (az úgynevezett inicializációs vektort), amelyek ráadásul 50%-os valószínűséggel már 5000 adatcsomag után ismétlődnek, ezen kívül az eredeti





A *WPA* és a *WPA2* kétféle autentikációs módot támogat: az egyik az otthoni használatra szánt ***PSK*** (***Pre-Shared Key***, előre kiosztott kulcs), a másik a főleg vállalati környezetbe illő ***Radius*** hitelesítő kiszolgálón keresztüli kulcskiosztó módszer, amely lehetővé teszi különböző hozzáférési szintek meghatározását is. Mi a beállításainkhoz a ***WPA-PSK*** protokollt fogjuk használni. Ennek lényege, hogy az autentikációt az induló kapcsolatkulcs, mint jelszó megadásával végezzük.

szabványban mindössze 40+24 bit volt a kulcs mérete. Ennek eredményeképp egy ilyen titkosítás feltörése az adatforgalom mennyiségétől függően kettő és tíz perc közé tehető. A probléma gyors orvoslása a kapcsolatkulcs méretének növelése 256bit-re, de ez csupán arra elég, hogy nem 10 perc, hanem 2-3 nap alatt tudja a támadó feltörni a hálózatot. *WEP* használata esetén a kapcsolatkulcs megadásával csatlakozhatunk a hozzáférési ponthoz.

Hatékony megoldás: WPA

A fenti hibák gyors megoldásért kiáltottak, megszületett a *WPA* (***Wi-Fi Protected Acces***, ***Wi-Fi*** védett hozzáférés), amely a *WEP*-hez hasonlóan ***RC4*** folyamkódolót használ 128 bites kulccsal és 48 bites inicializációs vektorral, ám lényeges különbség a ***TKIP*** (***Temporal Key Integrity Protocol***, ideiglenes biztonságos kulcs protokoll) bevezetése, amely folyamatosan cserélgeti a kapcsolat során használt kulcsot, így a támadó hiába fejtené meg a kulcsot, rövid időn belül semmire sem megy vele, pláne, ha egy kulcsot rövidebb ideig használ a rendszer, mint a feltöréséhez szükséges idő. A *WPA* előnye, hogy kompatibilis az összes korábbi eszközzel, hátránya, hogy ugyanazt az ***RC4*** folyamkódolót használja, mint a gyenge *WEP* protokoll, így még mindig nem nyújt tökéletes védelmet.

Biztos megoldás: WPA2

A ***WPA2*** gyakorlatilag egy időben készült a *WPA*-val, ezért is van, hogy a legtöbb implementáció egyesítve tartalmazza a ***WPA/WPA2*** protokollok kezelését. Legfőbb különbség a *WPA*-hoz képest az új ***AES*** (***Advanced Encryption Standard***, fejlett kódolási szabvány) kódoló használata a régi ***RC4*** helyett. Ezen kívül bevezették a négy lépéses azonosítási protokollt, ami nagyobb biztonságot nyújt a kapcsolódáskor történő támadások ellen. A ***WPA2*** „hátránya", hogy nem kompatibilis a régebbi (***820.11a,b***) eszközökkel illetve számos olcsóbb ***no-name g*** eszköz sem támogatja. A ***D-Link*** ilyen szempontból is jó választás, hiszen már a legolcsóbb, 10000 Ft alatti eszközök is tartalmazzák ezt a biztonsági módot.

Otthoni vezeték nélküli hálózatunk biztonságos beállítása

Otthoni hálózatunk feje még mindig a ***D-Link DIR-655***-ös szélessávú útválasztója, amelyet a ***D-Link Magyarországtól*** kaptunk a hálózatunk megépítéséhez. Ehhez kapcsolódunk a hasonló körülmények között birtokunkba került ***D-Link DWA-645***-ös *PC*-kártyával. Az útválasztó a fent ismertetett összes titkosítási módszert ismeri a visszamenőleges kompatibilitás miatt. A sorozat előző részében beállítottuk a második legerősebb biztonsági szintet, amely a *WPA* titkosítást alkalmazza. Azért ezt választottuk, hogy a közben eltelt időben is biztonságosan használjuk a hálózatot (említettük a *WEP* gyengeségeit), ugyanakkor a régi ügyfél oldali eszközökkel is hozzáférjünk.
Attól függően, hogy milyen ügyfél oldali eszközzel rendelkezünk, igyekezzünk az általa is támogatott legmagasabb biztonsági szintű kapcsolatot használni. Jelen esetben szerencsénk van, mivel a *PC*-kártyánk is a legújabb

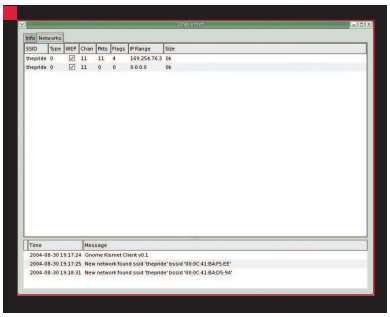
WPS: Biztonsági beállítások egyszerűen

A beállítási nehézségek kiküszöbölésére a ***Wi-Fi Alliance*** kitalált egy ajánlást, amelyet ***Wi-Fi Protected Setup***-nak (***Wi-Fi Védett Beállítások***) keresztelt. Az ajánlás lényege egy olyan egyszerű, egyetlen kattintással elvégezhető hálózatbeállítási, kapcsolatfelépítési folyamat, amely végén a felhasználó biztonságos hálózati kapcsolattal rendelkezik: nem kell jelszót és kapcsolatfelépítési információkat megjegyezni, a csatlakozáshoz elég megadnunk egy ***PIN*** kódot, és készen is vagyunk. A ***D-Link DIR-655*** útválasztó támogatja ezt az beállítási módszert, bár erről sem felhasználói kézikönyvben, sem a ***Wi-Fi*** kártya leírásában nem esik szó. Ez valószínűleg azért van, mert a vezeték nélküli hálózati kártyák vezérlőprogramjainak is támogatnia kell majd ezt a funkciót, s mivel a szabvány 2007 elején jelent meg, a hardvergyártóknak még nem volt idejük beépíteni. Mindenesetre a routerben a ***Wi-Fi Protected Setup*** menüpontra kattintva elvégezhetjük a beállításokat a hozzáférési pont oldaláról, a többi már a hálózati kártyák gyártóin múlik.

szériából való, így próbálkozhatunk a legerősebb, *WPA2* titkosítással. Ehhez nyissuk meg az eszközünk webes felületét, írjuk be a böngészőbe az *IP* címét: http://192.168.0.1 A bejelentkezés után válasszuk a bal oldali menüből a *WIRELESS SETTING* menüpontot, majd kattintsunk a *Wireless Network Setup Wizard* gombra, kövessük a varázsló utasításait, mindent változatlanul hagyva, és amikor a biztonsági szint képernyőhöz érünk, válasszuk a *BEST*, vagyis a legjobb lehetőséget, ezt követően adjuk meg a kapcsolódáshoz szükséges jelszót, és végül mentsük a beállításokat, és a megjelenő képernyőn válasszuk az eszköz újraindítását.
Ezek után máris csatlakozhatunk a *NetworkManager Applet* ikonjára kattintva. Az átállítás után az *Applet* még a régi titkosítási adatokat tárolja, ezért válasszuk a *Csatlakozás másik vezeték nélküli hálózathoz* menüpontot az elérhető vezeték nélküli eszközök listája alatt, adjuk meg a hálózatunk nevét, majd válasszuk a *WPA2* biztonsági szintet, adjuk meg a jelszót, ami egyben az induló kapcsolatkulcs (*Pre-Shared Key*). A típust hagyhatjuk *Automatikus* módban.

MAC korlátozás

Tovább fokozhatjuk a biztonságot, ha beállítjuk az útválasztón, hogy csak a meghatározott fizikai azonosítóval rendelkező hálózati eszközöket engedje csatlakozni. Minden hálózati eszköznek van egy egyedi FF:FF:FF:FF:FF:FF hexadecimális formátumú *MAC* címe, amelyet általában az eszköz hátoldaláról tudunk leolvasni, illetve az `ifconfig` parancs kiadásával kérhetünk le a számítógépen. Ehhez az útválasztó webfelületének *ADVANCED* lapján válasszuk a *NETWORK FILTER* menüpontot. A megjelenő képernyőn a legördülőmenüben válasszuk a második menüpontot, amely csak az itt listázott azonosítójú eszközöket engedi működni. Írjuk be az alább található beviteli mezőkbe a hálózatunkban használt vezetékes és vezeték nélküli eszközök *MAC* címeit, és mentsük a beállításokat.
A *MAC* cím persze egyszerűen hamisítható, ezért nem tökéletes védelem, de mégis eggyel több információ, amit a támadónak ismernie kell, ennélfogva növeli a hálózatunk biztonságát. Általában a *WPA* titkosítás is elegendő védelmet nyújt a támadások ellen, ezért optimális megoldás, ha így használjuk, ugyanakkor megengedjük az újabb eszközöknek, hogy használják az erősebb protokollt. Ehhez az útválasztó vezeték nélküli beállításainak lapján kattintsunk a *Manual Wireless Network Setup* (kézi beállítás) gombra, s a megjelenő képernyő *WPA Mode* feliratú lenyíló menüjében válasszuk az *Auto* módot, amely megengedi mind a *WPA*, mind a *WPA2* protokoll használatát.



Fix eszközeink beállítása WPA2 titkosításhoz

Az előző részben megnéztük, hogyan tudjuk a *NetworkManager Applet* hiányában, a gép indulásakor felélesztení a vezeték nélküli hálózatot az akkori beállításoknak, azaz a *WPA*-nak megfelelően. Ahhoz, hogy ez is *WPA2* protokollon kapcsolódjon, át kell írni a */etc/wpa_supplicant/wpa_supplicant.conf* fájl tartalmát az alábbira:

```
ctrl_interface=/var/run/
➥wpa_supplicant

network={
        ssid="a_hozzaferesi
➥_pont_neve"
        key_mgmt=WPA-PSK
        proto=WPA2
        pairwise=CCMP
        group=CCMP

psk="titkos_jelszo_ami_maga_a
➥_kapcsolatkulcs"
}
```

Az itt leírt megoldások persze nem bombabiztosak, idővel minden rendszer feltörhető, a kulcs itt az idő. Rohanó világunkban csak a gyors információ és a gyors cselekvési lehetőség ér valamit, ha csak lassan lehet megszerezni, az már nem is információ... A *WPA2* titkosítás *MAC* szűréssel ötvözve, rendszeresen változtatott jelszó (kulcs) használata esetén több, mint szükséges a számunkra, a hálózatunk biztonságosnak mondható.
A cikksorozat következő részében tovább csiszolgatjuk az otthoni hálózatunkat, kihasználva a DIR-655 útválasztó finombeállítási lehetőségeit: megnézzük, hogyan biztosíthatunk egyes gépeknek garantált válaszidőt, illetve beállítunk egy-két hozzáférési korlátozást, amivel például száműzhetjük az erőforrás-igényes és idegesítő reklámokat az otthoni hálózatunkból.

Feltöréshez szükséges szoftverek

A gyenge titkosítás feltöréséhez elegendő néhány ingyenesen elérhető szoftver, ami figyeli a hálózati forgalmat, és ezek alapján megszerzi a kapcsolatkulcsot. A szükséges szoftverek együtt, előre feltelepítve megtalálhatók az *Security Live CD* korongon, amelyet bárki letölthet a ➲ *http://www.knoppix.net/wiki/Security_Live_CD* címről. A dolgunk csupán annyi, hogy betöltjük a rendszert a *CD*-ről a gép indításakor, aztán használjuk az alábbi szoftvereket:

- *kismet*: azonosítja vezeték nélküli hálózatok adatait és résztvevőit rögzíti az adatforgalmat, segítségével összegyűjthető a támadáshoz szükséges adatmennyiség. Az adatforgalom rögzítéséhez az *Airodump* nevű szoftver is használható.
- *void11*: kijelentkezteti a hozzáférési pontra csatlakozott gépeket, így azok újracsatlakoznak, mi meg eltesszük ezeket az *ARP* kéréseket
- *arieplay*: a megszerzett *ARP* kéréseket tudjuk vele visszajátszani a hozzáférési pontnak, ezekkel növelve az adatforgalmat, és vele az inicializációs vektorok (*IV*) számát
- *aircrack*: az összegyűjtött forgalmi adatokból (az *IV*-k segítségével) megfejti a kapcsolatkulcsot