Ingyenes adatvédelem az új lapkákkal

Az egyre növekvő biztonsági igények és zuhanó lapkaárak mellett a Linux-rendszereknek is fel kell készülniük a jövő kihívásaira.

Mindenki szereti biztonságban tudni a titkait, de vajon mennyit hajlandó ezért anyagilag áldozni? Mostanra az Interneten a magánszféra védelme meglehetősen kicsire zsugorodott, a piacon megjelenő új lapkák azonban lehetővé teszik a felhasználók számára, hogy adataikat költségkímélő módon vagy éppenséggel pluszkiadások nélkül védjék meg.
Két szabvány uralkodik döntő többséggel a Hálón: az SSL és az IPsec. Az előbbit a legtöbb böngészőprogramba beépítik, ily módon biztosítva a biztonságos internet-tranzakciók megvalósulását. Az IPsec pedig virtuális magánhálózatokat (VPN) hoz létre, amelyeken keresztül a távoli adatbázisok is biztonságosan érhetők el.
Mindkét szabvány használ titkosítást, hogy a kódfeltörők, hallgatózók és betolakodók elől elrejtse a kényes adatokat. A tavalyi évig az Egyesült Államok kormánya megtiltotta a nagy biztonságú titkosítási módszerek más országokba történő exportját, de azóta a kormány szigora enyhült e tekintetben. A titkosítás általános elterjedésének legnagyobb akadályát jelenleg az a mérhetetlen nagy számítógépes kapacitásszükséglet képezi, amely az üzenetek titkosításához, illetve megfejtéséhez kell. Ha a titkosítás informatikai szempontból nem volna nehéz feladat, a kódokat egyszerű lenne feltörni. Szerencsére a legtöbb korszerű számítógép központi egysége bővelkedik annyi „lóerőben”, hogy lassabb ethernetkapcsolaton vagy akár széles sávú internetkapcsolaton is képes legyen titkosítani az üzeneteket. A gondot a kiszolgáló számítógép jelenti, amelynek egyidejűleg kell tudnia nagyszámú, sok felhasználótól érkező üzenetet kezelni. A kiszolgálógépek jellemzően 100 Mbites úgynevezett Fast ethernet- vagy ennél is gyorsabb hálózaton küldik az adatokat.
A szűk keresztmetszet megszüntetése érdekében a cégek olyan önálló titkosítóberendezések mellett döntöttek, mint például a VPN-gépek vagy az SSL-kártyák. Ezek a gépek sajátos, a célnak megfelelően kialakított lapkákat használnak, amelyek a titkosítási számításokat a szokványos processzoroknál sokkalta gyorsabban végre tudják hajtani.
A megfelelően nagy sebesség eléréséhez a jelenlegi biztonsági lapkák még nem eléggé gyorsak, ezért előfordulhat, hogy a nagyobb VPN- és SSL-hálózatokban több ilyen drága berendezést is össze kell kapcsolni – további járulékos berendezésekkel együtt. A végeredmény egy olyan VPN-csúcsgép, amelynek ára több százezer dollárra rúghat.
A segítség azonban máris úton van! A biztonság iránti fokozott érdeklődés újabb cégeket ösztönzött arra, hogy képviseltessék magukat a biztonsági lapkák piacán, ahol ez idő tájt tíz cég van jelen, de továbbiak is várhatók.
A lapkák többségét tavaly a Hifn állította elő, amely a programalapú tömörítéssel foglalkozó Stac cég melléküzletága. Olyan lapkagyártó óriások, mint az Intel, a Motorola és a Philips szintén betörni készülnek a piacra.
A kereskedelmi verseny tehát igen kedvező a műszaki újítások számára. Nem meglepő, hogy legjavuk olyan kis cégektől származik, mint a Chrysalis-ITS, a SafeNet és a Securealink; valamint az újonnan indulóktól, mint a Corrent, a NetOctave és a BlueSteel (ez utóbbi a Broadcom biztonságtechnikával foglalkozó leányvállalata). A piaci versenynek köszönhetően a jövő év közepére olyan 10 Gbit/s sebességgel működő lapkák jelennek meg, amelyek hálózati környezetben akár a legszélesebb keresztmetszeteken is képesek lesznek kiszolgálni.
Ez a sebesség százszorta nagyobb, mint a tavalyi év kezdete óta kapható legnagyobb teljesítményű lapka sebessége, ami valóban látványos fejlődés. A Moore-törvény átlagos fejlődési ütemével összemérve ez azt jelenti, hogy tízévnyi fejlődést két évnél egy kicsivel hosszabb időre sűrítettünk össze. Már csak egy rövidebb időszakra van szükség, amíg az új, gyorsabb lapkák a rendszerekben általánossá válnak, és jövőre a mostani VPN-csúcsgépek is csupán néhány ezer dollárba fognak kerülni.
Ha a titkosítás ilyen olcsóvá válik, valójában nem is különálló gépeken fog működni: ezek a nagy sebességű lapkák minden hálózati kártyán, illetve minden számítógépes hálózatban fel fognak tűnni. Az internetszolgáltatók csekély költséggel (körülbelül 1 dolláros havidíjért) kínálnak majd védelmi szolgáltatásokat a felhasználók számára. Ezért az árért a legtöbb ember biztonságosan fog tudni elektronikus levelet küldeni és fogadni, böngészni, illetve további elektronikus tevékenységet folytatni a Világhálón.
Néhány elemző azt jósolja, hogy 2004-re az internetes adatforgalomnak nagyjából a fele titkosított lesz.
Számos esetben ez csak kis vagy éppenséggel semmilyen hatást sem fog az alkalmazásokra kifejteni. Az IPsec az IP-szabvány részeként a hálózati verem 3-as rétegén dolgozik, vagyis nem egyszerűen az alkalmazási réteg alatt, hanem még a TCP-nél is lejjebb. Azt követően, hogy az operációs rendszer két számítógép között biztonságos kapcsolatot létesített, a két gép közti teljes adatforgalom titkosításra, illetve feloldásra kerül anélkül, hogy az az alkalmazásokra bármilyen hatást is gyakorolna.
Az SSL magasabb szintű protokoll, amit az alkalmazásnak közvetlenül kell kezelnie. Minthogy azonban már be van építve a böngészőprogramba, az azon keresztül elért bármilyen szolgáltatás felhasználhatja. A felelősség a webes rendszergazdákat terheli annyiban, hogy webfelületük minél nagyobb részét nagymérvű biztonságot szavatoló kiszolgálókra kell telepíteniük. Amint a biztonsági költségek csökkennek, a webhelyek teljes biztonsága ugyancsak megoldható.
Az IPsec használata akkor nagy fogás, ha az operációs rendszerben adunk neki helyet. A Linux-felhasználók már használhatják a FreeS/WAN-környezetet, amely az IPsec nyílt forrású, elismert megvalósítása. Ezzel szemben a legtöbb Linux-változat még nem tartalmazza ezt a programot, jóllehet a helyzet könnyen megváltozhat, amint a titkosítás egyre nagyobb népszerűségre tesz szert.
Összehasonlításképpen megemlíteném, hogy az IPsec szerepel a Windows 2000 szokásos szolgáltatásai között. A titkosításért felelős lapkák árának zuhanásával együtt a Linux-közösségnek is készenlétben kell állnia.
A fejlesztőknek, terjesztőknek és végfelhasználóknak egyaránt fel kell készülniük arra, hogy rendszerük képes legyen az olcsó titkosítási berendezések által nyújtott előnyök kihasználására.

Linley Gwenapp
(linley@linleygroup.com)
a The Linley Group szakmai elemző cég alapítója és vezetője.
A cég honlapja elérhető a ➲ http://www.linleygroup.com címen.