SCHÜLLER ATTILA

AZ IPV6 ÉS A HÁLÓZATI BIZTONSÁG

IPV6 AND NETWORK SECURITY

Az Internetre kapcsolódó eszközök számának rohamos emelkedése miatt az IPv4 címzési rendszert hatékonyabb alternatívával kell kiváltani. Napjainkban az IPv6, más néven IPnG (IP next generation – új generációs IP) tűnik a legalkalmasabb utódnak, egyre több szervezet tér át az új technológiára. Bár a korábbi biztonsági kockázatok közül többre megoldást ígér, az IPv6 is rejt magában veszélyeket. Kulcsszavak: IPv6, IPnG, Internet, biztonság

Because of the quickly increasing number of the Internet capable equipments it is necessary to change the IPv4 address system to a more efficient alternative. In our days the IPv6 (alias IPnG: IP next generation) seems to be adapted for the issue of IPv4. More and more organisations switch to the new technology. Although it promises solutions to several previous security issues, the IPv6 also has security threats. Keywords: IPv6, IPnG, Internet, safety, security

Bevezetés

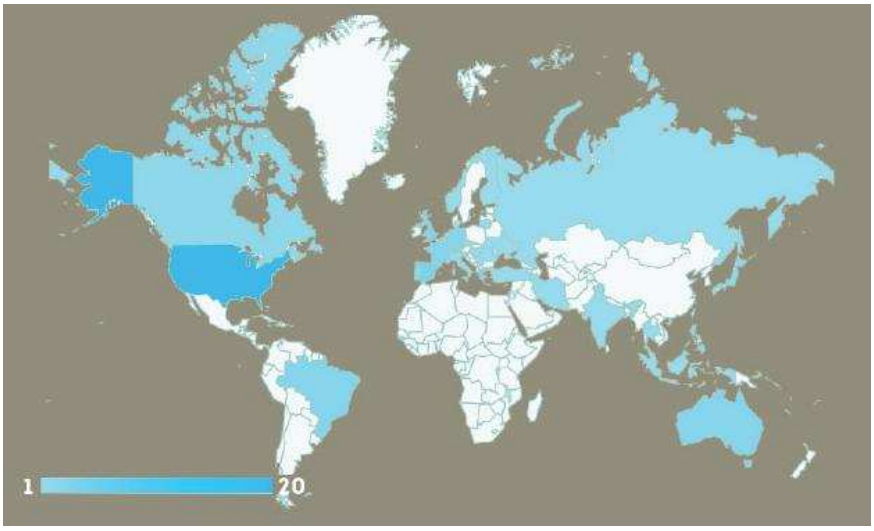
Az Internet Society 2012. június 6-án tartotta meg a World IPv6 Launch elnevezésű eseményt, amely során több nagy Internet szolgáltató, hálózati eszközgyártó és honlap-üzemeltető cég[1] éles üzemben bevezette az IPv6 protokoll használatát[2]. [1]

Ezzel hivatalosan is elkezdődött az új generációs IP-re való áttérés, mert voltak ugyan szolgáltatók, akik már eddig is biztosították ezt a lehetőséget, de ilyen mértékű összefogás még nem volt az elterjesztése érdekében. A

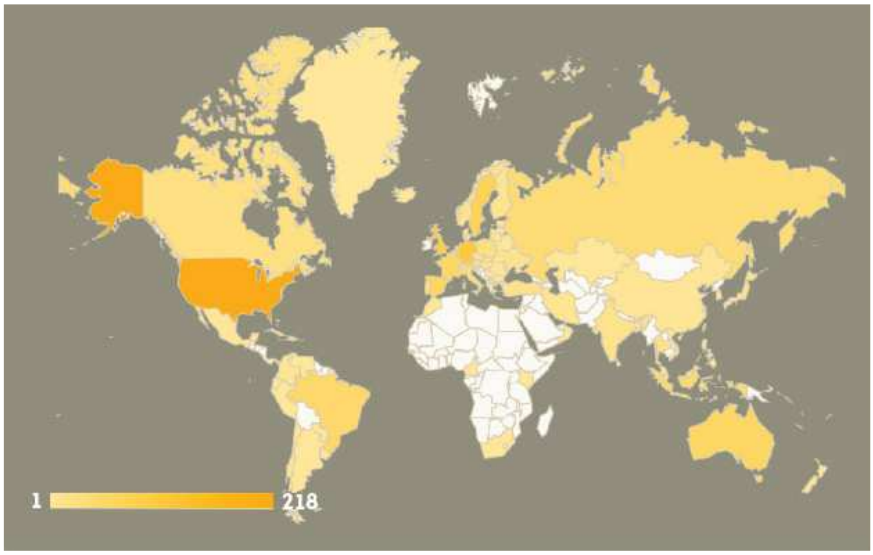
[1] A résztvevők között szerepeltek többek közt: AT&T, Cisco, D-Link, Facebook, Google, Microsoft Bing, Yahoo!.

[2] A bevezetést a tavalyi World IPv6 Day rendezvény előzte meg, amikor is 24 órás teszttel készültek fel a végleges bevezetésre.

jelenleg IPv6 technológiát alkalmazó szolgáltatók és honlap-üzemeltetők megoszlása az 1. és 2. ábrán látható.



1. ábra: Az IPv6-ot biztosító Internet szolgáltatók megoszlása [1]



1. ábra: Az IPv6-ot alkalmazó honlapüzemeltetők megoszlása [1]

A cikk az áttérés szükségességével foglalkozik, valamint azzal, hogy az IPv6 bevezetésével hogyan nő a korábbi rendszerhez képest a hálózati biztonság, illetve milyen új veszélyekre kell felkészülni.

Az áttérés szükségessége

Az Internet kritikus információs infrastruktúrává vált mind az egyének, mind a gazdasági társaságok, mind a kormányzatok, sőt egyenesen más kritikus infrastruktúrák számára.

Az emberek és szervezetek függősége az Internettől egyre növekvő mértékben növekszik, és ezzel egy időben jelentősen változik az a mód, ahogy az Internet szolgáltatásait felhasz-náljuk, ily módon az Internet kritikus infrastruktúra jellege nyilvánvalóan csak erősödni fog. [2]

Ezért kiemelten fontos, hogy olyan technológia álljon rendelkezésünkre, amely mind teljesítményében, mind biztonság tekintetében kielégíti a korunkban elvárt igényeket.

Az új generációs címzési rendszer kialakításánál elődje hiányosságait és hibáit is ki kellett javítani, emellett azonban az új technológiák támogatására is fel kellett készíteni az IPv6-ot.

A jelenleg elterjedt IPv4 címzési rendszernek a következő hátrányai vannak [3]:

— kicsi a címtér, pontosabban fogalmazva kevés a hálózati szám,
— a routing táblák túl nagy méretűek,
— kevés lehetőség van egy IP csomag tartalmának vagy feladójának hitelesítésére,
— nem nyújt minőségi szolgáltatást,
— nem vesz figyelembe olyan szempontokat, mint: mobilitás vagy autokonfiguráció.

Ezek közül a legnagyobb nyomást az IPv4 címek kihasználtsága jelentette. A hálózati technológia fejlődése, a sávszélesség növekedése lehetővé teszi, hogy gyakorlatilag minden számítógép mindig kapcsolatban lehessen a világhálóval, azaz a világ összes többi számítógépével. [4]

A teljes összekapcsoltság eléréséhez nagyobb címzési lehetőségre van szükség. A 32 bit címhosszúsággal rendelkező IPv4 esetén elvileg 2^{32},

azaz kb. 4,3 milliárd, míg a 128 bites IPv6 címzési rendszerrel 3,4 x 10^{38} egyedi IP címet lehet kiosztani.[3]

Teljesítménybeli előnyként jelentkezik, hogy az IPv6 esetében lehetőség van a hierarchikus címzési architektúra kialakítására, szemben az IPv4 címzési rendszerével. Ennek eredményeként az útvonalválasztás gyorsabbá válik, mivel lehetővé teszi az útvonalak csoportosítását (aggregáció). [3]

Az IP csomagok kiértékelése is rövidebb idő alatt feldolgozhatóakká váltak fejléc szerkezetének leegyszerűsítésével, valamint azzal, hogy több opcionális részt is tartalmaz.

Az IPv6 esetén csak a végponton történhet fragmentáció, ez a megoldás a routerek tehermentesítésével járul hozzá a teljesítményjavuláshoz.

A szintén új funkcióként megjelenő mobilitás a rohamos gyorsasággal terjedő mobil eszközök különböző hálózatokban való használatát támogatja, az autokonfiguráció pedig a rendszeradminisztrációt könnyíti meg.

Az IPv4-hez hasonlóan az IPv6-ban is hálózati interfészekhez rendelünk IP-címeket, nem gépekhez, vagy csomópontokhoz.

Az IPv6 es-etén azonban egy interfésznek több IP címe is lehet, ez nemcsak általános, de bizonyos funkciók ellátásának alapvető feltétele. [3]

Ezáltal könnyen megvalósíthatók például a peer to peer kapcsolatok. Természetesen a fej-lesztés a biztonság területén is megmutatkozott. Lássuk, milyen újdon-ságokkal találkozhatunk az új generációs IP-ben!

Biztonságtechnikai fejlődés az IPv4-hez képest

Az IPv6 tervezésénél nemcsak a rendelkezésre álló címek száma volt szempont, hanem a korábbi tapasztalatok figyelembevételével kijavították az IPv4 hibáit, valamint megoldották a technológiai fejlődés során jelentkező hiányosságokat.

[3] Ezek a számok az elméletileg elérhető maximumok, az osztályozások, fenntartások miatt a kioszthatóak címek száma lényegesen kevesebb. Azonban a címzési módokban rejlő lehetőségek így is könnyen felismerhetőek.

Így a biztonság területén is jelentős előrelépés várható, mert az IPv4 elleni többfajta támadástípus az IPv6-on már nem jelent potenciális veszélyt.

A IPv6 legfőbb biztonsági megoldása az IPSec, mely jelenleg az egyik legjobb biztonsági szolgáltatást nyújtó protokoll. [5]

Az IPSec-et kifejezetten az új generációs IP részére fejlesztették ki, annak szerves részét képezi, azonban használata az IPv4-ben is megoldható.

Az IPv6 három alap biztonsági eljárással rendelkezik:

— Authentication Header (hitelesítő fejléc): titkosítást nem tartalmaz, csak hitelesítést végez[4], a hitelesség és a sértetlenség ellenőrzésére, valamint a replay támadások kivédésére használható.
— Encapsulating Security Payload (elzárt biztonsági csomag): szimmetrikus titkosítással[5] megakadályozza az üzenetek lehallgatását, ezáltal biztosítja a bizalmasságot.
— Internet Key Exchange (Internet kulccsere): a két fél között egyezteti az alkalmazott algoritmusokat, valamint megvalósítja a kulccserét.

Az IPSec azonban nem old meg minden biztonságtechnikai kérdést. Van, aki szerint túlzottan univerzális, de skálázhatósági problémák is felmerülnek a használatával kapcsolatban. [7]

Nem céltudatosan tervezett biztonsági paraméter, inkább a címtartomány megnövelésének hozadéka, hogy az érvényes címek és szolgáltatások szkennelése sokkal nehezebb az IPv6 hálózatokban, mint az IPv4 hálózatokban.

A tényleges szkennelés egy teljes IPv6 szegmensben akár 580 milliárd évig is eltarthat, mert a címtér 64 bitet használ. [8] Mindazonáltal a nagyobb címtér nem jelenti azt, hogy az IPv6 teljesen sebezhetetlen a

[4] Pont – pont kapcsolatnál hitelesítésre használhatunk szimmetrikus kulcsú titkosító algoritmusokat, mint például a DES-t, 3DES-t, vagy Blowfish-t, vagy használhatunk egyirányú hash algoritmusokat, mint például az MD5-öt vagy SHA-1-et. Multicast üzeneteknél a hash algoritmus kombinálva van aszimmetrikus aláíró algoritmussal. [6]

[5] Titkosításra mindig szimmetrikus kulcsú algoritmust kell használni, ez alól kivétel a NULL titkosítás. [6]

támadás e formájával szemben. Például a MAC címből ge-nerált EUI-64 címek esetén a gyártókódok szűrésével le lehet csökkenteni a szkennelési időt. [7]

Biztonsági aggályok

Az IPv6 komoly biztonsági fejlődést jelent az IPv4-hez képest, ennek ellenére számos problémával kell továbbra is megküzdenünk. A legfontosabb aggályokat próbáltam összegyűjteni a következő részben.

Az új protokoll kifejlesztése elhúzódott, ezért a meglevő IPv4 rendszerek fenntarthatósága érdekében olyan megoldások születtek, amelyek nemcsak a címek elfogyását igyekeztek megszüntetni, de a különféle támadási módok kivédésére is alkalmazhatóak.[6] Ezen megoldások miatt csökkent az IPv4 leváltására irányuló nyomás, vagyis a teljes átállás nagyon sokáig tarthat. Ebben az átmeneti időszakban, amikor az Interneten egyaránt megtalálhatóak lesznek az IPv4 és IPv6 rendszerek, dual stack megoldásokat kell alkalmazni. Mivel ennek során két infrastruktúrát is üzemeltetni kell, így azok hátrányai — például a biztonsági rések — együttesen jelentkeznek.

A teljes körű, zárt és kockázatarányos védelem létrehozása csak egy átgondolt tervezési folyamat után valósítható meg, amelynek új vagy rekonstruálandó informatikai rendszer esetén az adott feladat teljesítésére indított informatikai projekt keretében kell megvalósulnia. [9] Az IPv4-ről való fokozatos átállás során azonban ad hoc jellegű megoldások is megjelennek, amelyek komoly biztonsági problémát jelentenek.

Például dual stackes megoldásoknál előállhat az a helyzet — mondjuk egy DNS poisoning hatására —, hogy ugyanazon URL alatt más oldal jelenik meg IPv6 és IPv4 esetén. Ez akár különböző IPv6 specifikus phishing támadásokra is lehetőséget teremt. [7]

A [5] forrás a következő biztonsági réseket és hátrányokat emeli ki:

[6] Ilyen, az IPv4 képességeit kiterjesztő megoldás például a NAT, az IPSec, a GRE, a CIDR, MPLS stb.

— az export törvények miatt a használható titkosítási algoritmusok erőssége korlátozott,
— az IPSec a Public Key Infrastructure-re (PKI) alapul, amely még nem teljesen szabványosított,
— további fejlesztés szükséges az IKE protokoll, illetve a DoS és az elárasztásos támadások elleni védekezés területén.
— a DoS típusú támadások általi sebezhetőség, mivel a titkosítási eljárások proceszor-igényes folyamatok,
— a tűzfalak részére lehetetlenné válik a forgalmi analízis, ha használjuk az ESP titkosítási protokollt. Tunnel módban használva létre lehet hozni kapcsolatot egy nem megbízható állomással egy privát hálózaton belül, mivel az IP cím láthatatlan a tűzfal számára,
— az IPv6 autokonfigurációs követelményei lehetőséget nyújtanak bizonyos DoS támadásokra, mivel a rendszer sebezhetővé válik hamisított alhálózat maszkokat tartalmazó csomagokra.

A broadcast címek hiánya sem teszi az IPv6-ot biztonságosabbá. Az új jellegzetességben, a multicast címekben folytatódik a probléma forrása. Smurf-típusú támadások továbbra is lehetségesek a multicast forgalomban. Ez ellen a szükségtelen forgalom kiszűrésével lehet védekezni. [8]

Egy informatikai rendszer biztonságát bármilyen kommunikációs kapcsolat csökkenti. A biztonsági veszélyforrások az adminisztrációtól való távolság függvényében egyre jelentősebbek. [9] Kiemelten kell kezelni a mobil eszközöket, amelyeknél az adminisztrációtól való távolság alaphelyzetben is fennáll. Az IPv6 egyik újdonsága a mobilitás, amely a pozitív hozadékai mellett biztonsági kockázatot is rejt. A [8] a következőre hívja fel a figyelmet. A hordozhatóság a címek két típusát használja, a valós címet és a mobil címet. Az első egy tipikus IPv6 cím, amelyet egy extension header tartalmaz. A második egy átmeneti cím, amelyet az IP fejrész tartalmaz. A hálózatnak ezen jellemvonása miatt (néha bonyolultabb, ha figyelembe vesszük a vezeték nélküli mobilitást) a mobil node cím átmeneti összetevője ki lehet téve spoofing támadásnak a home agenten.

2007 májusában francia kutatók hívták fel a figyelmet egy komoly problémára. A routing header 0 DoS támadásával elérték, hogy egy 4 Mb/s-os adatcsomag 352 Mb/s-os forgalmat generáljon. [10] A hasonló

módszerrel elkövethető, rosszindulatú tevékenységek elkerülése érdekében javasolták az RH0 tiltását.

Hét hónap múlva, 2007 decemberében az RFC 5095[7] hivatalosan is megszüntette a routing header 0 használatát. [12] A leírtak jól mutatják, hogy az IPv6-ban rejlő hibák fokozatosan előkerülnek (amelyet az éles használat még inkább elő fog segíteni), és azok javítása folyamatosan történik.

A személyes tűzfalak egy része még nem kezeli az IPv6 címeket. A problémát nem is ez jelenti, hiszen a fejlesztőknek előbb-utóbb fel kell készíteni az új címzési rendszerre a programjaikat. Ismételten a felhasználó lesz a gyenge láncszem, aki nem figyel oda arra, hogy a védelmi rendszere ténylegesen ellátja-e a feladatát.

A biztonság egy másik aspektusa, hogy az FBI szerint az IPv6-ra való átállás megnehezíti az internetes nyomozásokat. A problémát a hibrid technológia okozza, az IPv6 és az IPv4 kapcsolatok ugyanazon a hálózaton osztoznak. Ha az új technológia végleg kiszorítja a régit, akkor megoldódik a fő gond, mert minden eszköznek saját IP címe lesz. Az adatfolyam lehallgatása azonban még továbbra is kérdéses marad. [13]

Összefoglalás

Az IPv4-ről való átállás egy olyan rendszerre, amely a mai (és vélhetően megfelelően távoli jövőbeni) követelményeknek megfelel, odázható, de nem elkerülhető. Tökéletes biztonság nem létezik, így törvényszerű, hogy hiába küszöböli ki az új rendszer a korábbi hibákat, már a bevezetéssel egy időben újak jelentkeznek. Ez azonban nem jelentheti azt, hogy megálljon a fejlődés és leragadjunk a megszokott struktúránál, sokkal inkább arra kell törekedni, hogy a potenciális veszélyekre minél korábban fény derüljön, és akár a bevezetett rendszer foltozásával, akár egy

[7] Az RFC (az angol Request For Comments rövidítése magyarul kéretik megkritizálni) egy olyan dokumentum, mely egy új Internet-szabvány beiktatásakor adnak közre. Az új szabvány első tervezete saját számmal kerül a nyilvánosság elé, egy adott időtartamon belül bárki hozzászólhat. Ezeket a hozzászólásokat rendszerezik, majd többszöri módosítás után a szabványtervezetet elfogadják, vagy eldobják. [11]

jövőbeli rendszer tervezésénél figyelembe vegyük (optimális esetben mindkettőnél).

Jelen váltásnál sok biztonsági problémát az IPv4 és IPv6 rendszerek közötti átjárás okoz. Ezek a kockázati tényezők megszűnnek, amikor az IPv6 teljesen kiváltja elődjét. Csak találgatni lehet, hogy ez mikorra következik be, hiszen a felhasználók számára jelenleg semmilyen kényszer nincs a váltásra, a jelenlegi megoldásokkal (NAT, IPv4 alatti IPSec stb.) még sokáig üzemelhetnek IPv4 rendszerek. A közintézmények is kerékkötői lehetnek az átállásnak, hiszen részben anyagi eszközeik korlátozottak, részben a központi rendszereket kell igénybe venniük. Erre példa, hogy sok intézményben még elavult DOS-os szoftvereket használnak (pl. a leltározásra SÁFÁR, a könyvelésre TATIGAZD programokat), azokat „fejlesztgetik”. A közoktatási intézmények Internet elérésére és egymás közötti kommunikációjára létrehozott SuliNet sebessége már rég nem felel meg a kor követelményeinek, átlagosnak számít a 4 Mbps/512 kbps-os kapcsolat, de van, ahol csak 1 Mbps/128 kbps sebesség érhető el. Ilyen infrastruktúra mellett nehéz elképzelni, hogy a közeljövőben komoly lépések történnek az IPv6 bevezetésére ezen a területen.

A tisztán IPv6-os rendszerekben is rejtőznek veszélyek, de már jelenleg is sok tapasztalat gyűlt össze, így kezdenek kialakulni a minél nagyobb biztonságot elősegítő szabályozások. Fontos szerepe van az emberi tényezőnek, azaz hogy mind a rendszerüzemeltetők, mind a felhasználók megtanulják, hogyan kell az IPv6-ot biztonságosan kezelni.

Az is elképzelhető, hogy az új generációs IP használata nem is lesz hosszú távú, csupán időt nyerünk egy még újabb, még megbízhatóbb rendszer kidolgozására. Azonban amennyiben ez az IPv6 jelentős átdolgozásával érhető el, akkor a kifejlesztésénél nehéz lesz megoldani, hogy sokkal nagyobb biztonság mellett az IPv6-ról való folyamatos átállás is gördülékenyen megvalósítható legyen. Egy IPv6-nál korszerűbb rendszerre váltás viszont csak az IPv4 címek teljes megszűnése után elképzelhető, ellenkező esetben a hálózati eszközöket és az alkalmazásokat mind a három rendszer használatára fel kellene készíteni.

Felhasznált Irodalom

[1] World IPv6 Launch. http://www.worldipv6launch.org
Letöltés ideje: 2012. június 25.

[2] Munk Sándor: A jövő Internete kutatások, egy védelmi/katonai kutatási program keretei. Hadmérnök, 2009/4. sz. pp. 289-302.

[3] Ferenczy Gábor: Az új generációs Internet.
Bolyai Szemle, 2002/3. sz. pp. 91-102.

[4] Kovács László (szerk.): Számítógép-hálózati hadviselés: veszélyek és a védelem lehetséges megoldásai Magyarországon. Tanulmány. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2012.

[5] Somodi Zoltán: Hálózati biztonság az IPv6 protokoll tükrében.
Műszaki Szemle, 2006/33. sz. pp. 38-42.

[6] Biczók Ádám: Virtuális magánhálózatok. Szakdolgozat.
BMF-NIK, Budapest, 2005.

[7] Szigeti Szabolcs: Biztonságosabb-e az IPv6?
http://videotorium.hu/hu/recordings/details/343,
Biztonsagosabb-e_az_IPv6_ Letöltés ideje: 2012. június 25.

[8] Sotillo, Samuel: IPv6 Security Issues
http://www.infosecwriters.com/text_resources/pdf/IPv6_
SSotillo.pdf Letöltés ideje: 2012. június 25.

[9] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság.
PRO-SEC, Budapest, 2007.

[10] Biondi, P., Ebalard. A.: IPv6 Routing Header Security
http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf
Letöltés ideje: 2012. június 25.

[11] Wikipédia: RFC http://hu.wikipedia.org/wiki/RFC
Letöltés ideje: 2012. június 25.

[12] Abley, J., Savola P., Neville-Neil G.: Deprecation of Type 0 Routing Headers in IPv6. RFC 5059, 2007.
http://tools.ietf.org/html/rfc5095
Letöltés ideje: 2012. június 25.

[13] McCullagh, Declan: FBI: New Internet addresses could hinder police investigations
http://news.cnet.com/8301-1009_3-57445157-83/fbi-new-internet-addresses-could-hinder-police-investigations
Letöltés ideje: 2012. június 25.