Bevezetés

Gyakran felmerül a kérdés, vajon az IPv6 protokoll hoz-e újat az informatikai biztonság területén. Korábban erre a kérdésre szinte azonnali igen volt a válasz: az IPv6 sokkal biztonságosabb, hiszen kötelező része az IPSec, amely megoldja a titkosítási és hitelesítési kérdéseket. Mára azonban kiderült, hogy a kép sokkal árnyaltabb, és egyáltalán nem olyan egyszerű az IPv4 és az IPv6 összehasonlítása a biztonság területén.

A protokollok összehasonlítása

Nyilvánvaló, hogy biztonsági szempontból csak teljes rendszereket lehet összehasonlítani, azonban feltételezve, hogy egy rendszerben csak egy komponenst –jelen esetben a hálózati protokollt – cserélünk ki, megállapíthatunk bizonyos változást az egész rendszer biztonságára vonatkozóan.
A következőkben egyrészt megvizsgáljuk az IPv6 címzési rendszere által hozott változásokat a biztonság területén, másrészt pedig az IPv6 újdonságait tekintjük át.

Célpontválasztás

A hatalmasra nőtt címtartomány felvet néhány érdekes kérdést. Az IPv4 hálózatok támadásának rendszerint az első lépése a felderítés, amely során gyakran alkalmazott módszer a hálózat letapogatása, a „szkennelés”, azaz az IP címek végigpróbálgatása. Hasonló módon működnek automatizált támadások, és vírusok is. Természetesen felmerül, hogy a szegmensenként 64 bites vagy még nagyobb címtartomány lehetetlenné teszi az ilyen fajta támadást. Ez igaz is, meg nem is. Valóban, IPv6-nál a címek sorban történő végigpróbálgatása nem nagyon vezet célra. Megfelelően szervezett letapogatás azonban célra vezethet. Ha a címeket DHCP-vel osztják a hálózatban, akkor megvan az esélye annak, hogy az adminisztrátorok a címeket nem egyenletes eloszlásban allokálják, hanem csoportokban. Így elegendő egy címet megszerezni (pl. forgalom figyeléssel) és utána annak környezetét letapogatni.

Állapotmentes autokonfiguráció esetében pedig ki lehet használni azt a tényt, hogy a cím interfész azonosító része (EUI-64 formátumban) az Ethernet címből származik. Az Ethernet cím pedig többek között tartalmazza a gyártó számára kiosztott azonosítót. Ha pedig feltételezzük, hogy egy nagy hálózatban több, azonos gyártótól származó Ethernet kártya van, akkor máris le lehet szűkíteni a vizsgálandó

tartományt. A hálózat lehallgatásával megfigyelhető a használt azonosító, vagy egyszerűen próbákat tehetünk népszerű típusokkal.

Ebből látható, hogy bizonyos mértékben a címtartományra építés „security by obscurity”, de részben igaz az, hogy, jóval nagyobb „intelligenciára” van szükség a hatékony szkenneléshez, így a férgek és vírusok dolgát vélhetően megnehezítheti.

Hasonló kérdést vet fel a NAT hiánya. IPv4-nél gyakran a NAT előnyének tartják, hogy elrejti a belső hálózatot. Az IPv6-ban viszont nincs NAT. Az egész szerencsére álprobléma, mert a NAT által megvalósított elrejtés megvalósítható megfelelő tűzfal szabályok alkalmazásával. Az nem is vitatható, hogy tűzfalakra viszont továbbra is szükség van. Igaz, jelenleg a nagy tűzfalgyártóknak csak kísérleti tűzfal megvalósításai vannak.

IPSec

Az már említettek alapján, a közhiedelemmel ellentétben az IPSec nem csodaszer, és egyelőre nem is látszik, hogy a közeljövőben alkalmaznák mindarra, amire annak idején elképzelték. Az IPSec képes arra, hogy hitelesítse és titkosítsa a csomagokat, ráadásul az IPv6 tervezése során kínosan ügyeltek arra, hogy minden IP szinten történjen (IPv4 esetén ez nincs így, az ARP vagy a DHCP pl. félig Ethernet szinten működik). Ebből következik, hogy elvileg az IPv6 minden funkciója védhető IPSec-kel. Gyakorlatilag viszont vannak problémák. Az IPSec szinte minden nem VPN jellegű felhasználásánál, főleg a tetszőleges végpontok közti kapcsolatra nem igazán van kidolgozva a megfelelően skálázható kulcsmenedzsment mechanizmus. Márpedig követelmény, hogy lehetőség szerint könnyen kezelhető és automatikusan működő legyen minden funkció. Így kijelenthető, hogy a protokoll általános működésében az IPSec nem hoz javulást.

Autokonfiguráció

Az IPv6 egyik leglátványosabb része az autokonfiguráció. Mivel ez (illetve tágabb értelemben az egész szomszédfelmérési protokoll) meglehetősen összetett, ezért vannak helyek, ahol biztonsági problémák jelentkezhetnek. Az autokonfiguráció során több olyan pont van, ahol különböző hamis információkkal támadást lehet intézni a rendszer ellen. Néhány ilyen jellegzetes pont:

- Hamis konfigurációs információkkal (érvénytelen prefix, stb.) csomópontok kommunikációképtelenné tehetőek.
- Hamis útválasztó hirdetésekkel egy teljes szegmens forgalma elterelhető, ez akár túlterheléses támadásra, akár közbeékelődéses támadásra felhasználható.
- A szomszédfelhívási kérésekre (elérhetőség és duplikált címek) adott hamis válaszokkal csomópontok elérhetetlenné tehetőek.

Természetesen ez mind kiküszöbölhető lenne IPSec AH hitelesítéssel, de ez az említett okok miatt körülményes.

Kétséget kizárólag az autokonfigurációs támadások lehetségesek, bár használhatóságuk korlátozott, mert a támadónak jelen kell lennie a kérdéses szegmensen, és megfelelő időzítéssel és értékekkel kell a támadást végrehajtani. A külső támadások ellen van pár egyszerű védekezés, például a szomszédfelmérési protokoll csomagjainak TTL mezeje a maximum érték, 255 kell, hogy legyen, így ellenőrizhető, hogy nem jött át útválasztón a csomag. Bizonyos robosztusságot ad a duplikált címek ellenőrzése, így az IPv4-nél gyakori hibát, amely során két azonos IP cím komoly problémákat okozhat, ez kiküszöböli.

Ugyanakkor azt is ki lehet jelenteni, hogy az autokonfiguráció átgondoltságával és robosztusságával mindenféle egyéb kiegészítés nélkül is megbízhatóbb és biztonságosabb, mint az IPv4.

Áttérési módszerek

Biztonsági szempontból az áttérési módszerek kritikusak. Egyrészt a módszerek komplexek, tehát hibákat rejthetnek, másrészt pedig „ideiglenesnek” tekintik őket, tehát az alkalmazók hajlamosak félvállról venni a precíz megvalósítást.

A legtöbb áttérési módszerrel felmerül a nehéz ellenőrizhetőség. Lássunk egy egyszerű példát: tunellinget használva összekötünk két IPv6 hálózatot, úgy hogy köztük a forgalom IPv4 felett megy. Az egyik hálózatból kijövő IPv6 csomagokat berakjuk IPv4 csomagok adatrészébe (encapsulaton), majd a másik hálózatban a beérkező csomagokat „kibontjuk”, kivesszük az IPv6 csomagot (decapsulation). Tegyük fel, hogy védeni szeretnénk a hálózatunkat az ellen, hogy kívülről olyan hamisított csomagok jussanak be, amelyek forráscíme a belső hálózatba tartozik. Ez a „address spoofing” tipikus támadási forma, azokat a szolgáltatásokat támadja,

amelyek megbíznak a saját hálózatukból származó csomagokban. Megelőzésük egyszerű, a hálózat szélén olyan tűzfal-szabályt kell használni, amely nem enged be kívülről olyan csomagot, amely forráscíme belső. Igen ám, de tunellezés esetén a tűzfal csak az IPv4 csomagot tudja ellenőrizni, hiszen számára a benne foglalt IPv6 csomag csak egyszerű adat. A támadó megteheti, hogy olyan IPv4 csomagot hamisít, amelyben nincs semmi gyanús, ugyanakkor a benne lévő IPv6 csomag viszont valóban hamis címet tartalmaz. A tunellt így felhasználhatjuk arra, hogy megkerülje a tűzfal által nyújtott ellenőrzési lehetőségeket. Természetesen a megoldás egyszerű, a kicsomagolás után az IPv6 csomagokat is ellenőrzés alá kell vetni, de a tapasztalat azt mutatja, hogy ez ritkán történik meg. Hasonló módon a tunellezés használható titkos kapcsolatok kialakítására, a tűzfal megkerülésével, mint ahogy erre ár volt párszor példa.

A különböző transzlációs megoldások is hasonló problémákat rejtenek, ha az üzemeltető nem gondoskodik a megfelelő biztonsági beállításokról és szűrőkről. Bizonyos módszerek (főleg a Teredo) pedig eleve arra épít, hogy megfelelő UDP csomagokkal „lyukat üt” a NAT-on és a tűzfalon, hogy így oldja meg az IPv6 kapcsolatot egy belső hálózatba. Érezhető, hogy itt különös gondot kell fordítani a biztonsági beállításokra.

Teljesítmény növelés

A teljesítmény növelés irányába tett lépéseknek is van kihatása a biztonságra. Elsősorban a fejlécek kezelése érdekes, abból a szempontból, hogy a jelenlegi előírások szerint bizonyos fejléceket csak a végpontok, a többit pedig a közbeeső csomópontok is vizsgálhatnak. Sajnos a tűzfalak nem esnek bele egyikbe sem, tehát ha valóban hatékonyan akarjuk egy tűzfalban vizsgálni a forgalmat, jelenleg meg kell szegni a vonatkozó RFC-ket! Persze ez nem okoz nagy gondot, és várható, hogy születik rá megoldás, de mindenképpen rávilágít arra a tényre, hogy az új feljéc-láncolási megoldás még tartogathat meglepetéseket.

Mobilitás

Az IP szintű mobilitás meglehetősen összetett mechanizmus, és bár felhasználhatósága talán nem létfontosságú. Mikor van arra szükség, hogy egy idegen hálózatban, saját IP címét megtartva működjön egy eszköz? Rendszerint teljesen megfelelő, ha kap valami IP címet, az pedig könnyen megoldható. Ettől függetlenül az

IPv6 mobilitás egy elegáns mechanizmussal biztosítja a feladat elvégzését. Érdekes, hogy bár régóta tudnak róla, hogy rengeteg biztonsági kérdés van körülötte, csak nemrég jelent meg az RFC3775, amely ezzel behatóan foglalkozik. A legtöbb kérdés egyébként nem IPv6 specifikus, inkább általános jellegű, mint például az idegen hálózatban történő authentikálás, vagy a hitelesített kapcsolat a honi-ágens és a mobil hoszt között. IPv6 szempontjából a mobilitással kapcsolatos opciós fejlécek az érdekesek, amelyek a mobil eszköz valós IP címét adja meg a vele kommunikáló feleknek. Ez ugyanis felvet mindenféle kételyeket a forgalom eltérítésével kapcsolatban, ha valaki ilyen fejléceket hamisít.

A jövő

Az IPv6 biztonsági kérdéseiről ma inkább találgatni lehet, mint biztosat mondani, de annyi kijelenthető, hogy az új protokoll elvileg rendelkezik azokkal a tulajdonságokkal, amelyek lehetővé teszik egy biztonságosabb rendszer megvalósítását. Ugyanakkor várható, hogy a bevezetés körüli bizonytalanság, kiforratlan rendszerek az első időben több gondot fognak okozni, mint amennyi IPv4-nél volt. Várható azonban az is, hogy hosszabb távon ez az arány megfordul, és az IPv6 biztonságosabb lesz, mint a régi protokoll.