IP TELEFÓNIA ÉS BIZTONSÁG

Telbisz Ferenc, telbisz@sunserv.kfki.hu
KFKI RMKI SzHK és Magyar Telekom PKI-FI

Bevezetés

Az analóg telefonbeszélgetéseket már több évtizede, gyakorlatilag a PCM technológia elterjedése óta digitálisan továbbítják. Ezek azonban vonalkapcsolt hálózatok voltak, ahol a kapcsolat létrehozásakor lefoglalják a maximálisan szükséges sávszélességet mindkét irányban és ezért a szolgáltatás minőségének (QoS: Quality of Service) a biztosítása nem jelentett problémát. (Ez – a lehetséges tömörítést is figyelembe véve – mintegy 6 – 15 -szeres túlfoglalást jelentett a sávszélességnél.) A csomagkapcsolt hálózatoknál, azok "best effort" jellege miatt a QoS biztosítása sokáig probléma volt, azonban a megnövekedett sávszélesség és a Diffserv [1] bevezetésével meg lehetett oldani a problémát és ezután már semmi akadálya nem volt annak, hogy a beszéd továbbítására is csomagkapcsolt IP hálózatokat használjunk. Ez előnyös a felhasználóknak, mert sokkal olcsóbbá (esetenként akár ingyenessé) vált a telefon (beszédátviteli) kapcsolat, és előnyös a szolgáltatóknak is, mert olcsóbbá vált a hálózat üzemeltetése.

Terminológia

Az IP telefónia, Internet és VoIP kifejezéseket gyakran szinonimaként használjuk, azonban nem pontosan ugyanazt jelentik:

- Az **IP telefónia** azt jelenti, hogy a telefon beszélgetés átvitele részben vagy egészen IP hálózaton történik.
- Az **Internet telefónia** ennek speciális esete, amikor a telefon beszélgetés átviteli útvonala, vagy legalább is annak egy része a "nyílt" Internetet használja.
- Végül a **VoIP** (Voice over IP) magát a technológiát jelenti, az architektúrát, a protokollokat, interface-eket, amelyeket az IP telefónia vagy Internet telefónia szolgáltatás használ.

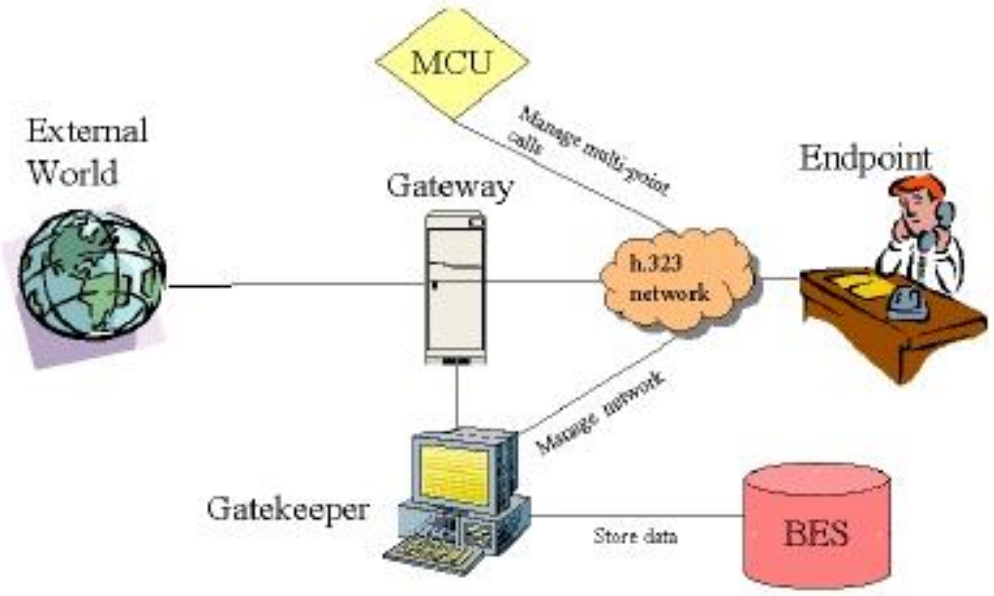
A VoIP architektúrája

Megtévesztő az az elképzelés, hogy mivel a VoIP is az IP hálózatot használja, az IP hálózati biztonság egyúttal megoldja az IP telefónia biztonságát is. A VoIP további elemeket és ennek következtében bonyodalmakat is ad hozzá az IP hálózati struktúrához. Ezért az alábbiakban nagyon vázlatosan áttekintjük a VoIP hálózati architektúrát és protokollokat. A legfontosabb különlegessége a VoIP protokolloknak, hogy a kapcsolat fölépítése, és a tényeleges adat (beszéd) forgalom más útvonalon történik. A kapcsolat létrehozását végző elemeket az egyes protokolloknál másként nevezik, de funkciójuk hasonló.

A különböző "proprietary" protokoll mellett többféle VoIP protokollt készítettek eddig a különböző szabványosító szervezetek. Ezek között a két legfontosabb a SIP és a H.323 protokoll. Ezek közül várhatóan a SIP lesz a domináns, ha már nem az jelenleg is.

H.323 architektúra

Az ITU készítette el a H.323-as szabványt, eddig négy verziója jelent meg, a V.1 elavult, a másik három meglehetősen hasonló, és fölfelé kompatibilis. (A H.323 szabványok nem tölthetők le ingyen az ITU honlapjáról, de jó tutoriális cikk található [2] alatt.) Valójában a H.323 egy átfogó szabvány, ami alá több további szabvány tartozik [3] Az architektúra az 1 ábrán látható.



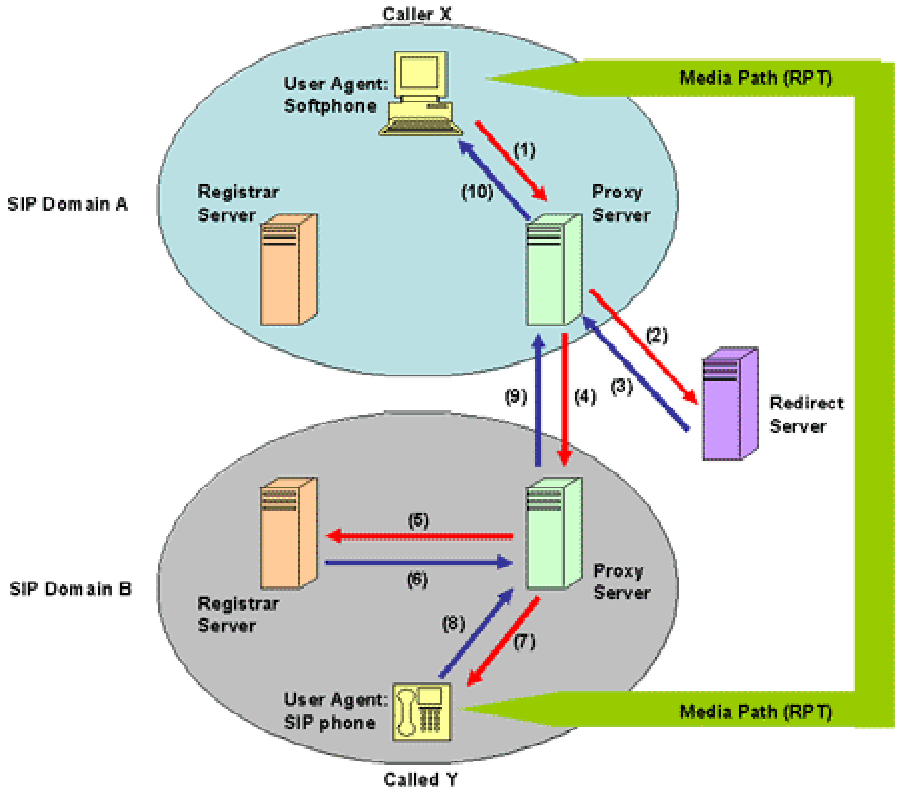
1. Ábra. H.323 architektúra

A BES (Back End Service) eszköz tartja nyilván a végpontokra vonatkozó adatokat, beleértve a jogosultságokat, szolgáltatásokat és konfigurációkat. A Gatekeeper-ben testesül meg a H.323 hálózati intelligencia, ez ellenőrzi a hívási jogosultságot, lebonyolítja a kapcsolat felépítését, a sávszélesség meglétének ellenőrzést. A Gateway jelenti a kapcsolatot a külvilág, a nyilvános telefonhálózat, más H.323 régiók felé. Az MCU (Multipoint Control Unit) a konferenciák (több végpont közötti szimultán kommunikáció) szervezését segíti.

SIP architektúra

Az IETF dolgozta ki a Session Initiation Protocol -t (SIP) [4]. A SIP architektúrában a H.323-nál több elem szerepel (2 ábra). A proxy szerver(ek) hozzák létre a kapcsolatot, de a "redirect server"-ek és a regisztrációs szerverek (registrar server) segítségével a SIP rendszer nyomon tudja követni a kommunikáló partnerek mozgását (helyváltoztatását).

Az ábrán látható a kapcsolat fölépítésénél az egyes akciók, fázisok sorrendje is.



2. Ábra. SIP architektúra

A nyilvános kapcsolt telefonhálózat és a VoIP összehasonlítása

A Nyilvános telefonhálózat (PSTN: Public Switched Telephone Network) és a VoIP hálózat meglehetősen különbözik egymástól. A legfontosabb különbségek láthatók a 3 Táblázatban. Ebből következően a hálózatbiztonság is természetesen különböző.

3. Táblázat

Nyilvános Kapcsolt Telefonhálózat	VoIP
Zárt hálózat, ahol a jelzések és az adatok (hang) magán hálózaton továbbítódnak, a végberendezések jól meghatározott helyen vannak	Nyílt hálózat, ahol a jelzések és az adatok az Internet felé nyitott hálózaton, vagy éppen az Internet-en továbbítódnak, a végberendezések helye általában nem jól meghatározott
A jelzésrendszerhez a végfelhasználó nem fér hozzá	A végfelhasználó módosíthatja a VoIP jelzéseket.
A hálózati elemek megbízhatóak és ellenőrzöttek	A hálózati elemekhez más is hozzáférhet, alkalmasint a működésük sem megbízható, mert könnyen támadhatók.
A primitív végberendezések kevésbbé támadhatók	A végberendezések könnyen támadhatók, mint általában az IT eszközök

Nyilvános Kapcsolt Telefonhálózat	VoIP
Működésüket a hatóságok meglehetősen szigorúan szabályozzák	Gyakorlatilag nincs hatósági szabályozás, mivel adathálózatok

A VoIP hálózatok sebezhetősége

A csomaghálózatok működése nagymértékben függ konfigurálható paraméterektől: a terminálok és telefonkészülékek IP és MAC (fizikai) címei, a routerek és tűzfalak címei, a VoIP eszközök (gatekeeper, proxy server, stb.) címei, stb. Ezen paraméterek nagy része dinamikusan osztódik ki pl. a berendezés ujraindításakor, vagy amikor egy VoIP telefont ujraindítanak vagy hozzáadnak a hálózathoz. A sok dinamikusan konfigurálható paraméter megannyi potenciális sebezhetőségi pont a behatolóknak, támadóknak. A VoIP szolgáltatásnál számolni kell az IP hálózatoknál fellépő valamennyi kockázattal, amihez néhány további telefonhálózati (VoIP) visszaélés lehetősége is járul.

Az alábbiakban lényegében csak az intézmények, vállalatok szempontjából tárgyaljuk a kockázatokat, veszélyeket, a szolgáltatók esetében ettől részben eltérő analízis lenne szükséges. Amennyiben azonban a nyilvános telefonszolgáltatást nyújtó távközlési vállalatok egyszerűen csak az IP protokollt használják a beszédtovábbításra, de továbbra is zárt (virtuális) hálózatot használnak, az alábbi kockázatoknak meglehetősen kevéssé vannak kitéve, mivel ezek a zárt hálózatok jól védhetők.

Támadási pontok

Speciálisan VoIP-hez kapcsolódó támadási pontok a következők:

1. **Hívásvezérlők (Call Controllers)**. Ezek a berendezések hozzák létre a hívási kapcsolatokat. A különböző protokolloknál eltérően nevezik őket, a SIP protokollnál ezek a "proxy szerver"-ek, "redirect server"-ek és regisztrációs szerverek, a H.323-nál a "gatekeeper"-ek és a "Multipoint Control Unit" eszközök. Támadási pont lehet a szükséges adatbázis szoftver is, akár a call control eszközökben, akár külön szerverben van implementálva.

2. **VoIP telefonok**. A PC-ben szoftverrel implementált eszközöket "***soft phone***"-oknak nevezzük, ahol egy alkalmazás bonyolítja le a hívásokat. Ez lehet különálló alkalmazás, de lehet integrálva az E-mail-hez. Ezeken a gépeken valamilyen operációs rendszer fut, és annak sebezhetősége természetesen fennáll. A hardver alapú berendezések ugyan hasonlítanak a hagyományos telefonokra, de sok járulékos szolgáltatásuk van és általában szoftverrel vezéreltek, ami többé-kevésbbé szintén támadható.

3. **VoIP protokollok**. A protokolloknak is lehetnek biztonsági hiányosságai, ill. az elmúlt időben néhányat jeleztek is mind a SIP-nél, min a H.323-nál. Ezek DoS (Denial of Service) támadások voltak, valamint nem engedélyezett kódok végrehajtása.

Támadási lehetőségek

A legfontosabb támadási fenyegetések a következők:

– ***Lehallgatás, adatgyűjtés***. Elég egy berendezést úgy konfigurálni, hogy a hálózati csatlakozásán megjelenő valamennyi forgalmat rögzítse, és máris értékes információhoz

juthat a támadó. Ez lehet egy-egy beszélgetés tartalma, vagy értékes konfigurációs információ, amit későbbi támadáshoz használhat fel akár a végpontok, akár a VoIP kiszolgáló eszközei ellen. A beszélgetés titkosításának a szükségessége megfontolható (l. alább), de a hívásfelépítéshez és a vezérléshez mindenképpen védett protokollokat ajánlatos használni.

- ***Csalás (spoofing)*** A támadó megszemélyesíthet egy jogosult felhasználót azáltal, hogy szabályos SIP vagyH.323 üzeneteket ad. Ilyen módon a támadó egyrészt a "call control" eszközt hamisíthatja, vagy esetleg éppen a korábban gyűjtött adatok felhasználásával ***hamis identitást*** vehet fel, aminek segítségével a rendszer olyan elemeihez férhet hozzá, amihez nincs jogosultsága. Lehetőség van egy másik személy identitásának a felvételére is, bár amennyiben beszédről van szó, a csalás, az idegen hang meglehetősen könnyen felismerhető, ha egy, a hívott által ismert személy identitását próbálja meg a támadó felvenni. (Beszédszintetizátor használatával további csalási lehetőségek is nyílnak, ezek azonban a hagyományos telefon esetében sem zárhatók ki.)

- ***Díjszabási csalás***: a felhasználó paramétereinek megváltoztatásával a támadó olyan szolgáltatásokat vehet igénybe, amihez nem jogosult. Ez utóbbi lehet pl. jogosulatlan távhívás.

- ***DoS (Denial of Service) támadás***, amikor a támadó a megtámadott végpontra, vagy hálózati elemre olyan csomagot küld, ami annál pl. rendszerösszeomlást okoz, vagy elárasztja a megtámadott végpontot, hálózatot vagy kapcsolatot olyan mennyiségű csomaggal, ami lehetetlenné teszi a normális működést (***DDoS: Distributed Denial of Servic***e). Tulajdonképpen ez nem VoIP specifikus támadás, minden IT rendszer esetében fennáll.

- ***Vírusok.*** Mivel a VoIP-t kiszolgáló rendszerek, a "call controller"-ek, de a végberendezések is (akár hardphone, akár softphone) lényegében számítástechnikai rendszerek, jórészt Intel architektúrájúak Windows operációs rendszerrel, ezért ugyanúgy ki vannak téve a vírustámadásoknak, mint bármilyen más hasonló IT rendszer.

- ***VoIP Spam***. A VoIP rendszerek ki vannak téve az automatikusan generált hangüzenet reklámoknak, SPAM üzenetek tömegének, amelyeket itt ***SPIT***-nek (Spam over Internet Telephony) hívunk. A támadó begyűjtheti a telefonszámokat, és ingyenes vagy olcsó hívásokkal áraszthatja el őket. Eddig valószínűleg a VoIP telefonok viszonylag alacsony száma miatt nem vált akuttá ez a probléma

- ***Visszaélés a TFTP protokollal.*** Sok VoIP gyártó a TFTP (Trivial File Transfer Protocol) protokollt használja a VoIP berendezések firmware vagy software felújítására. Ha a TFTP kapcsolatot nem védi szigorúan ellenőrzött hozzáférési lista (Access Control List), akkor a támadó mindenféle hamis információt tölthet a különböző berendezésekbe, aminek a következményei beláthatatlanok.

- ***Visszaélés az SMTP protokollal.*** A legtöbb VoIP eszköz valamilyen módon távolról vezérelhető az SMTP protokollal. Ha az SMTP-t nem védi erős és titkos jelszó, a támadó behatolhat ezekbe az eszközökbe, átkonfigurálhatja és hozzáférhetetlenné teheti őket mindenki más számára, beleértve a rendszeradminisztrátort is.

Néhány ajánlás

Természetesen a VoIP szolgáltatás, hálózat védelme meglehetősen összetett, bonyolult feladat, az alábbiakban csak néhány alapvető ajánlásra szeretnénk felhívni a figyelmet. Bővebb útmutatás található pl. az Egyesült Államok NIST intézete (National Institute of Standards and Technology) által kiadott ajánlásokban [6]

1. Lehetőleg használjunk különböző logikai hálózatot (VLAN) a hang és adathálózatra, mindegyikben különböző DHCP szerverrel.

2. A nyilvános kapcsolt telefonhálózat felé való kapcsolatot nyújtó "voice gateway"-nél lehetőleg tiltsuk le az adatházat felől jövő, ill. az adathálózat felé menő SIP, H.323 és egyéb VoIP protokollokat.

3. A VoIP menedzsmentjéhez feltétlenül IPsec vagy SSH eszközöket használjunk

4. A "softphone" eszközöket, amelyek a VoIP-t szolgáltatást közönséges PC-ken adják, lehetőleg ne használjuk ott, ahol az adatvédelem vagy a titkosság fontos.

5. Ahol szükséges, használjunk titkosítást a beszédforgalomban, bár megfontolandó, hogy sok vállalatnál a levélforgalom legalább annyira bizalmas adatokat tartalmaz, mint a beszéd, még sincsen titkosítva.

6. A tűzfalak és a NAT speciális megfontolásokat és problémákat jelentenek, és speciális megoldások szükségesek. Általában alkalmazás specifikus tűzfalak szükségesek ill. ajánlatosak.

A biztonsági eszközök használata, mivel lassítják, ill. lassíthatják a forgalom átbocsátását, könnyen mehet a szolgáltatás minőségére különösen érzékeny VoIP forgalom rovására, azt gyakorlatilag használhatatlanná téve.

A hagyományos telefonkészülékek áramszünet esetén is működnek, mert a tápellátásukat a telefon vonalon kapják. (Így pl. segélyhívásra is alkalmasak még akkor is, ha áramszünet van.) A VoIP eszközök áramellátása, akár speciális készülékek, akár PC-k, nem oldható meg a telefonhálózat felől, ezért megfelelő szünetmentes áramforrásra van szükség. Ezek karbantartási költsége megnövelheti a költségeket. Amennyiben szükség esetén néhány órás áramszünetnél hosszabb időt is át kell hidalni, generátorok is szükségesek, valamint azok üzemanyagát is tárolni kell, ami mind költségnövelő tényező.

Segélyhívó számok

A nyilvános kapcsolt telefonhálózatoknál a készülékek egy jól meghatározott helyen vannak, és ennek következtében a telefon szolgáltató el tudja végezni az alábbi négy feladatot:

- a hívást, mint segélyhívást tudja azonosítani,
- a segélyhívást a megfelelő helyre tudja kapcsolni,
- a hívó helyét meg tudja adni,
- meg tudja adni a visszahívási számot a segélyszolgálatnak.

A mobil telefonoknál a helymeghatározás már problémát jelentett, amit a mobil tornyokra alapozott háromszögelési eljárással és a GPS segítségével lehetett valamennyire megoldani.

A VoIP képes berendezések természetüknél fogva nomádikus berendezések is lehetnek (PDA vagy laptop). A jelzés az IP rétegben kezdődik, de az alkalmazási rétegben folytatódik. A VPN használatával pedig a felhasználó akár egy másik kontinensen is lehet.

Ezért az Egyesült Államokban jelenleg is (a 2006. év eleje) folyik a vita az FCC (Federal Communications Commission) és az IPCC (International Packet Communications Consortium) között arról, hogy mit és hogyan lehet megvalósítani [7]

Az Európai Unió a VoIP szabályozási kérdéseknél gyakorlatilag még nem jutott el a segélyhívó szám kérdéséhez, csak a probléma regisztrálása történt meg eddig (a 2006. év eleje).

Összefoglalás

A VoIP előnyeihez nem lehetett egészen ingyen hozzájutni. Ezek a kockázatok részben VoIP specifikusak, részben azonban minden, az Internet-e használó eszköz esetében fennálló kockázatok, az Internet természetéből kifolyólag. A kockázatok azonban kezelhetők, és semmi esetre nem lenne célszerű a VoIP szolgáltatásról lemondani.

Irodalom

[1] IETF: RFC 2474 és RFC 2475 és több más RFC is

[2] http://www.iec.org/online/tutorials/h323/

[3] http://www.openh323.org/standards.html

[4] J. Rosenberg et al.: SIP: Session Initiation Protocol. RFC 3261. June 2002

[5] http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

[6] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries: Security Considerations for Voice, Over IP Systems, NIST January, 2005, http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

[7] http://www.ipccforum.org/