IP Telefónia és Biztonság

Telbisz Ferenc

KFKI RMKI Számítógép Hálózati Központ
és
Magyar Telekom PKI-FI

Tartalomjegyzék

Bevezetés

- **Az analóg beszédet digitálisan továbbítják már több évtizede (PCM)**

  Digitalizálás a kerék feltalálásához mérhető:
  Kerék: haladó mozgás ⇒ forgó mozgás
  Digitalizálás: analóg jel ⇒ digitális jel

- **Hagyományos telefon: vonalkapcsolt hálózatok: PSTN (Public Switched Telephone Network)**
  - **max. sávszélességet (64 Kbps) lefoglalják**
    - **kapcsolat létrehozásakor**
    - **mindkét irányban**
  - **nincs QoS probléma**
  - **erőforrások túlfoglalása (6 – 15 szörös)**

Bevezetés

- A csomagkapcsolt (IP) hálózat "best effort":
  - QoS problématikus
    - Jitter
  - Megoldás
    - megnövekedett sávszélesség
    - Diffserv
- IP használat előnyös
  - a felhasználónak,
    - mert olcsóbb (esetleg ingyenes)
  - a szolgáltatónak,
    - mert olcsóbb az üzemeltetés

Terminológia

- **Terminológia**
  - **IP telefónia:**

    átvitel IP hálózaton (részben vagy egészben)
  - **Internet telefónia:**

    átvitel útonala: "nyílt" Internet (részben vagy egészben)
  - **VoIP (Voice over IP):**

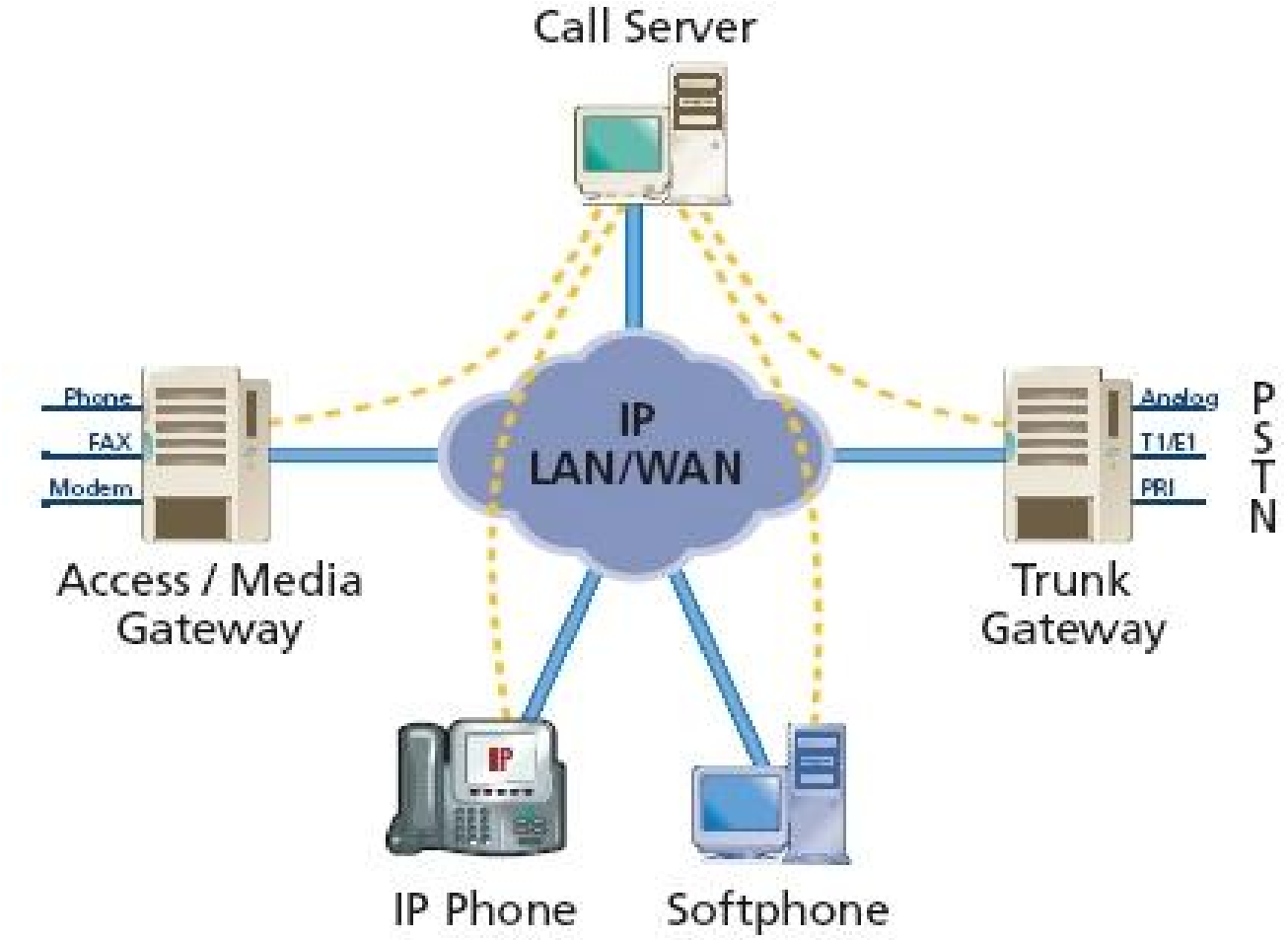
    technológia:
    - **architektúra**
    - **protokollok**
    - **interface-ek**

A VoIP architektúrája

- **IP biztonság nem oldja meg a VoIP biztonságot !**
- **VoIP-nél újabb elemek jelennek meg**
  - **IP phone, softphone**
  - **Call controller/server**
  - **Gateway-k**
- **A kapcsolat fölépítése és az adat (beszéd) forgalom más útvonalon történik**

A VoIP architektúrája

Kapcsolat létrehozása



A VoIP architektúrája

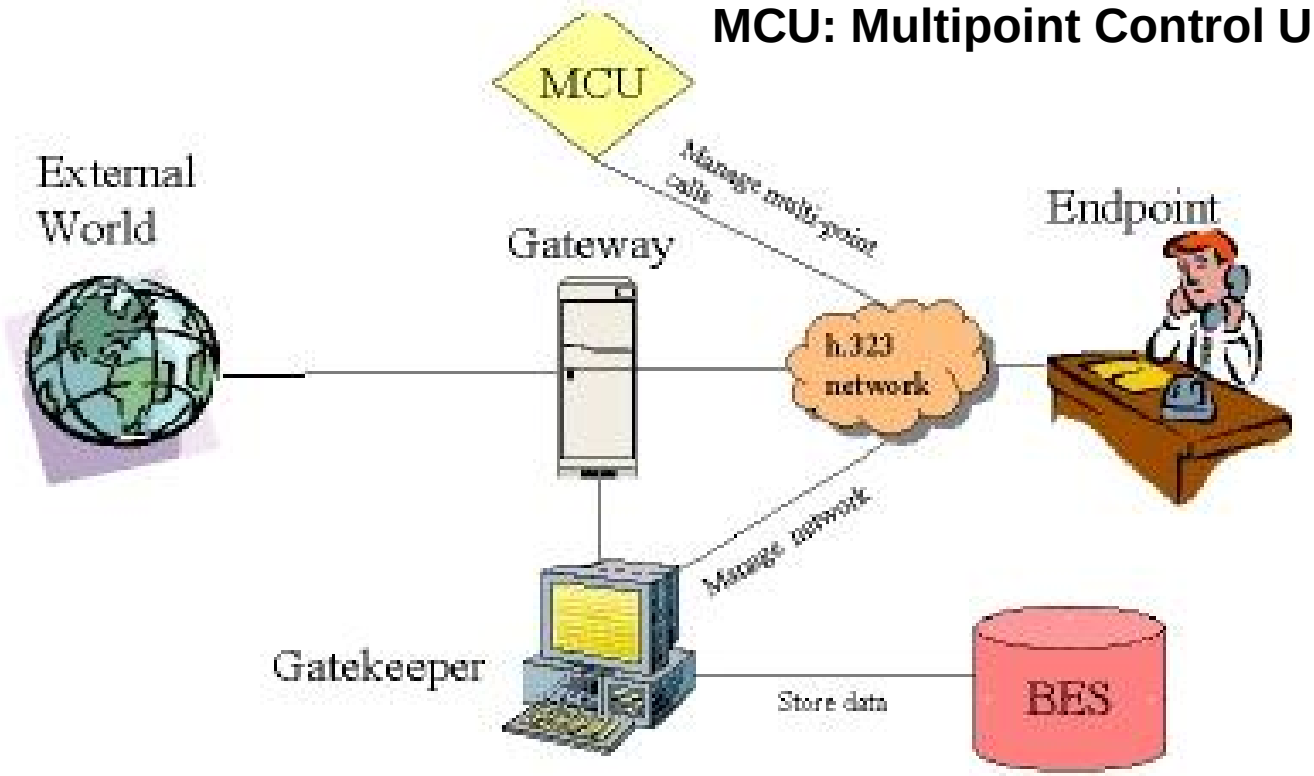
Adat (beszéd) forgalom

A VoIP architektúrája

- **Fejlődési útvonal**
  - **Proprietary (gyártóspecifikus) protokollok**
  - **Szabványos protokollok:**
    - **H.323**
    - **SIP (Session Initiation Protocol)**
    - **Egyéb protokollok (időben korábban)**

H.323 architektúra

- **ITU (International Telecommunication Union) (CCITT)**
- **H.323: ajánlás csoport**
- **Tutoriális: http://www.iec.org/online/tutorials/h323/**

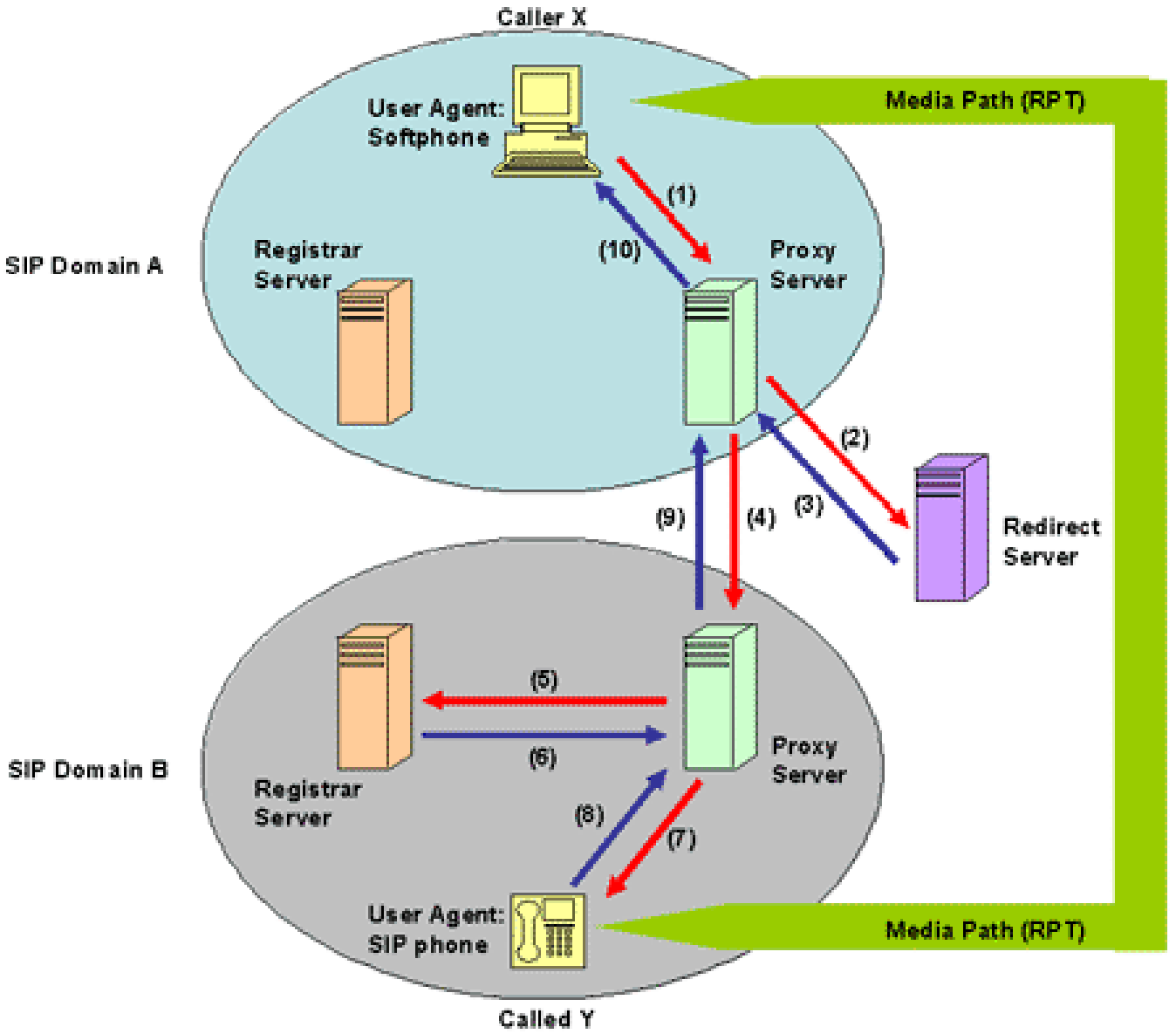


MCU: Multipoint Control Unit

BES: BackEnd Server

SIP architektúra

- IETF dolgozta ki
- J. Rosenberg et al.: SIP: Session Initiation Protocol. RFC 3261. June 2002
- H.323-hoz képest több elem



PSTN és VoIP összehasonlítása

Nyilvános Kapcsolt Telefonhálózat

- Zárt hálózat
  - jelzések és adatok magánhálózaton
  - végberendezések jól meghatározott helyen
- Jelzésrendszerhez a felhasználó nem fér hozzá
- A hálózati elemek
  - megbízhatóak
  - ellenőrzöttek

VoIP hálózat

- Nyílt hálózat
  - jelzések és adatok Interneten vagy Internet felé nyitott hálózaton
  - Végberendezések helye nem jól meghatározott
- Végfelhasználó módosíthatja a VoIP jelzéseket
- A hálózati elemek
  - nem megbízhatóak (támadhatók)
  - más is hozzájuk férhet

PSTN és VoIP összehasonlítása

Nyilvános Kapcsolt Telefonhálózat

- Primitív végberendezések kevésbé támadhatók
- Müködésüket a hatóságok szigorúan szabályozzák

VoIP hálózat

- Végberendezések könnyen támadhatók (IT eszközök)
- Gyakorlatilag nincs hatósági szabályozás

A VoIP hálózatok sebezhetősége

- Csomaghálózatok sebezhetőségének forrásai:
  - Konfigurálható paraméterek:
    IP és fizikai címek
  - Nagy részük dinamikusan osztódik ki
  - A konfigurálható paraméterek támadási lehetőségek
- Itt csak intézményi (vállalati) szempontból tárgyaljuk
- Szolgáltatóknál más analízis szükséges

A VoIP hálózatok sebezhetősége

- **Támadási pontok:**
  - **Hívásvezérlők**
    - **SIP: proxy server, redirect server, regisztrációs szerver**
    - **H.323: gatekeeper, Multipoint Control Unit, (DBS)**
  - **VoIP telefonok**
    - **Soft phone (PC + software)**
    - **VoIP telefon (ez is programmozott!)**
  - **VoIP protokollok**
    - **protokoll hibák (pl. DoS támadás lehetősége)**

A VoIP hálózatok sebezhetősége

- **Támadási lehetőségek, módok:**
  - **Lehallgatás, adatgyűjtés**
    Egyéb támadások kiindulópontja
  - **Csalás (spoofing): hamis cím, hamis identitás**
  - **Díjszabási csalás**
  - **DoS (Denial of Service) támadás**
  - **Vírusok és férgek (Windows !)**
  - **VoIP Spam: SPIT (Spam over IP Telephony)**
    Még nem elterjedt
  - **Visszaélés a TFTP protokollal**
  - **SMTP visszaélés**
    Erős jelszó védelem kell !

Néhány ajánlás

- Lehetőleg különböző logikai hálózat (VLAN) a hang és adathálózatra
  - Voice mail probléma
- A PSTN kapcsolati gateway-nél letiltandók a SIP, H.323, stb. protokollok az adathálózat felől/felé.
- VoIP menedzsment: IPsec vagy SSH kötelező!
- Softphone eszközöket lehetőleg ne használjunk.
- Titkosítás szükség szerint (IPsec)
  - Probléma: a jelzés csomagok titkosítása
    - Call controllerek, stb: bele kell nézniük a csomagokba
  - E-mail sem titkos

Néhány ajánlás

- **Tüzfalak és NAT: speciális megfontolás**
  - **Probléma:**
    - **A SIP alkalmazási szintű protokoll**
    - **Az IP címeket a hálózati réteg módosítja**
    - **Kapcsolat IP címei a csomag adatrészében vannak**
  - **ALG (Application Level Gateway)**

    Session Border Controller
- **A biztonsági eszközök lassíthatják a forgalmat:**

  QoS probléma

Néhány ajánlás

- **Áramszünet:**
  - **hagyományos telefon áramellátása a hálózat felől**
    - **segélyhívásra alkalmas**
  - **VoIP eszközök áramellátása:**
    - **szünetmentes áramforrás**
    - **költségnövelő**

Segélyhívó számok

- **Segélyhívás feladata:**
  - **mint segélyhívást azonosítja,**
  - **megfelelő helyre kapcsolja,**
  - **hívó helyét meg tudja adni,**
  - **segélyszolgálatnak megadja a visszahívási számot.**
- **Mobil telefonoknál is probléma a helymegadás:**
  - **Nincs fizikai cím: a bázisállomás (torony) nem elég pontos**
  - **háromszögelés ⇒ GPS koordiáták: térképre vetíthető**
- **VoIP hívó helye nem azonosítható**

  akár másik kontinensen is lehet (VPN)
- **USA-ban még folyik a vita**
- **EU még csak regisztrálta a problémát**

Zárszó

- **A VoIP mégsem "ingyenes"**

  Kockázatok forrása: Internet + VoIP,

  de a kockázatok kezelhetők

- **Személyes vélemény:**
  - **A VoIP "elkerülhetetlen"**
  - **Valóban komoly veszélyforrások:**
    - **Az operációs rendszer kockázati tényezői: vírusok, stb.**
    - **"Gépesített" SPAM támadási lehetőség**

Köszönöm a figyelmet