Zakonito prestrezanje v omrežjih naslednje generacije

Naim Maloku, Aljaž Tomaž

Povzetek — V sedanjih trendih zlivanja govornih in podatkovnih storitev se vedno pogosteje pojavlja zahteva po njihovem zakonitem prestrezanju. Podatki o prestreženi telekomunikaciji in vsebina prestrežene telekomunikacije oziroma kopije sporočil so stvari, ki bodo (so) zahtevane s strani zakonodajni organov in morajo biti na razpolago pri operaterjih oz. ponudnikih storitev [1][2]. V klasični telefoniji je zakonito prestrezanje izvedeno v večini primerov v sami komutacijski opremi. Ker gredo vsi pogovori nadzorovane osebe čez komutacijsko opremo je zakonito prestrezanje izvedeno relativno enostavno. S pojavom omrežij naslednje generacije (NGN – Next Generation Networks), kjer se po skupnem paketnem omrežju lahko prenašajo istočasno govor, podatki in slika, nimamo več idealnega okolja za spremljanje – nadzor teh oblik prometa, saj v naprej ne moremo točno vedeti poti po kateri bo komunikacija potekala. Proizvajalci komunikacijske opreme so postavljeni pred nove zahteve in tehnološke izzive. V članku so predstavljeni nekateri primeri izvedbe zakonitega prestrezanja klicev v omrežjih naslednje generacije.

Ključne besede — NGN, zakonito prestrezanje

Abstract — In the new environment of different fraudulent threat, telecommunication carriers' ability to ensure legal call interception has become more important than ever. The telecom service provider should be capable of providing law enforcement authorities with logged information regarding all calls originated and terminated by a particular subscriber, with possibility to record to the subscriber conversations. The legacy PSTN (Public Switched Telephone Network) manufacturers have supplied telecommunication operators with different solutions that enabled them to provide the required information. However, with the emergence of new NGN and VoIP packet based networks, new problems and challenges arise. In the following paper, we will present the possible solutions how the legal call interception is performed in PSTN, how the legal call interception can be providing in NGN and the possible problems existing on the IP networks.

Keywords — NGN, Legal Interception

I. UVOD

S popularnostjo Interneta in enostavnim dostopom do njega se je v zadnjem desetletju povečalo število njegovih uporabnikov in istočasno podjetij, ki so želela biti prisotna in dostopna "vsakomur". Na žalost so podjetja vsaj v začetku posvečala premalo časa na varovanju podatkov in na ta način omogočila skoraj idealno okolje za tiste, ki hočejo zagrešiti kriminalna dejanja. Dostopno je mnogo finančnih informacij: fondi in obveznice, delniške družbe, zaupne investicije, varnostni zakladi, itd. Zanimivo je, da razen trgovanja in izmenjave informacij med naštetimi primeri najdemo v izobilju informacije o posameznih transakcijah. Vlagatelji imajo vpogled v vse finančne in druge informacije ter imajo dostop do vseh udeležencev na trgu (ostalih investitorjev, podjetij, itd.). Vpliv interneta v svetu financ je najbolj razviden iz naslednjih podatkov:

- 22% vseh finančnih transakcij poteka sprotno oz. t.i. "on-line",
- 37% trgovin na drobno dela sprotno in
- 50% poslovnih posredovanj je izvedenih sprotno.

S pomočjo Interneta in arhitekture NGN so zlorabe težje izsledljive ker:

- kraj zločinov in zlorab ni več lokalno omejen,
- žrtve in akterji zlorab postanejo zaradi okolja nevidni en za drugega,
- obstaja prepričljivo orodje za zlorabe,
- stroški za postavitev spletne strani za zlonamerne namene so minimalni in
- razvoj novih tehnologij postaja vse hitrejši.

Zaradi zgoraj naštetih dejavnikov, se vse bolj uveljavlja prepričanje, da nadzor elektronskih komunikacij predstavlja neprecenljivo orodje za preprečitev in borbo zoper različna kriminalna, teroristična in zlonamerna dejanja. V času, ko je klasična telefonija predstavljala največjo omrežje komunikacije za povezovanje telefonskih aparatov, je bil proces nadzora in snemanja pogovorov relativno enostaven. Z napredkom tehnologij se je spreminjala industrijska struktura, povečalo se je število operaterjev in storitev, poslovno in privatno življenje je postalo odvisno od komunikacij, računalniki in podatki so postali v poslovnem smislu bolj pomembni kot govor in družbe so postale odvisne od mobilnih komunikacij. Pri tako hitrem razvoju in napredku tehnologij je postalo v tehničnem in pravnem smislu vse bolj problematično omogočiti dostop do elektronskih komunikacij za to pristojnim službam. Prav tako pa so proizvajalci telekomunikacijske opreme in operaterji postavljeni pred nov izziv – kako omogočiti zakonit

nadzor komunikacije, ki poteka na tehnologiji uvedeni z ravno nasprotnim namenom? Zakonito prestrezanje komunikacij je dobilo nov pomen zaradi same narave "zveze", ki je v novem tehnološkem okolju lahko v obliki govora, podatkov, slike ali kombinacija vse teh informacijskih oblik. Celo koncept "telefonske številke", ki je v določenem razvojnem obdobju telekomunikacij bil točno vezan na fizično lokacijo, predstavlja v novih okoliščinah samo identifikacijo komunikacije.

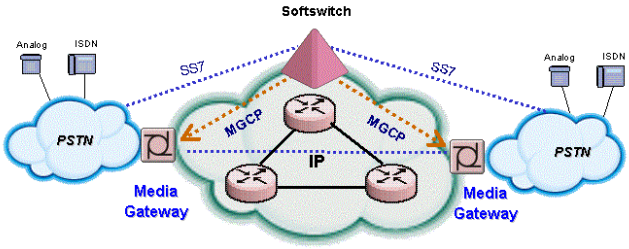
V članku bova predstavila možne rešitve za zakonito prestrezanje klicev v NGN in morebitne probleme, ki se lahko pojavijo v omrežjih IP (Internet Protocol).

II. Arhitektura NGN in Elektronski Nadzor

Omrežje naslednje generacije (NGN) je predvideno za prenos govornih in podatkovnih informacij. Koncept omrežij NGN ni enoumno določen. Trenutno lahko zasledujemo več kot eno vizijo arhitekture NGN, kar je posledica:

- različnih pristopov k "skupnem" omrežju,
- različnih institucij za standardizacijo in
- različnih definicij za storitve s posebnimi zahtevami za kvaliteto storitve (QoS – Quality of Service).

Slika 1 prikazuje možno arhitekturo NGN.



Slika 1: Arhitektura NGN

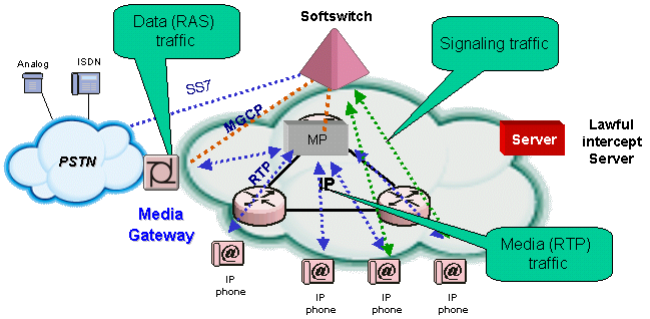
Elektronski nadzor je možno razčleniti na naslednje tri razrede storitev [3], [4]:

- zajem informacijske vsebine,
- zajem signalnih informacij (identifikacija komunikacijskih subjektov)in
- shranjevanje zajetih podatkov.

III. Tehnična rešitev

Zakonito spremljanje paketnega (IP) prometa bo v prihodnjih letih postalo eden izmed ključnih poglavij tehnologije IP. Sama izvedba bo odvisna od zakonodaje v kateri bodo rešitve govora prek IP (VoIP – Voice Over IP) implementirane. Spremljali bomo lahko več vrst prometa., kot recimo:

- spremljane samo signalnih informacij (informacije v zvezi s klicem). Ker v omrežjih IP ni običajnih telefonskih številk, se lahko tu uporabijo izvorni/ponorni naslov IP, tip komunikacije in, če je na razpolago, tudi druga oblika identifikacije (npr. kličoča in klicana številka). Druge informacije (npr. e-mail naslov) se prav tako lahko uporabijo kot možen identifikator, vendar realizacija takšnega sistema ni enostavna (pregledovanje koristne vsebine znotraj paketa IP). Pojavi se lahko problem spremljanja dvotonske večfrekvenčne signalizacije (DTMF–dual tone multi-frequency), ki so lahko prenesene v "ne signalizacijskem" kanalu, saj se lahko nahajajo znotraj istih paketov kot je govor. Težave predstavljajo tudi storitve kot npr. "hold/join/drop", uporabljene v konferenčnem klicukjer vsi udeleženci niso znotraj iste administrativne domene saj lahko vidimo le tiste informacije, ki so znotraj naše domene.
- spremljanje multi-medijskega prometa. Pri tem lahko recimo spremljamo samo VoIP promet, vendar se postavlja vprašanje kaj storiti z podatkovnim prometom in ali ga je sploh dovoljeno spremljati? Glavni problem, ki se pojavlja, je kako ločevati VoIP promet od podatkovnega prometa. Naprave za ločevanje paketov na osnovi aplikativnih podatkov so zelo zahtevne in posledično drage.



Slika 2: Zakonito prestrezanje prometa

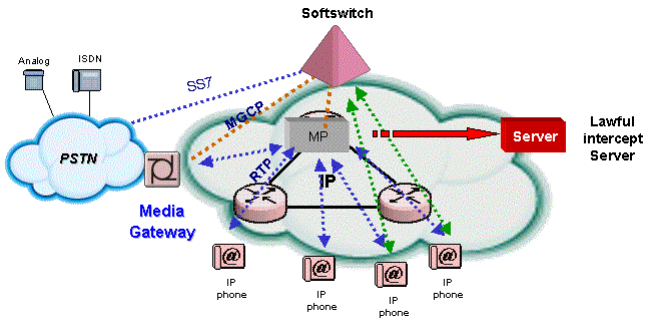
Glede na zgoraj omenjeno bi bilo smiselno v mešanih okoljih tradicionalne telefonije in NGN izvesti spremljanje prometa v elementu za prehod med mediji (MG – Media Gateway), kjer imamo vse potrebne informacije o vrsti klica (podatkovni ali govor). Kako pa to rešit v IP-IP komunikaciji?

Te problematike se lahko lotimo s centraliziranim ali decentraliziranim pristopom, ki pa lahko imata svoje izpeljanke. Prvi vključuje poseben strežnik (MP – Media Proxy) prek katerega gre vsa informacija (signalna in medijska), kjer se odvajajo želene informacije do strežnika za zakonito prestrezanje (Lawful intercept Server), ki analizira vsebino. Drugi pa vključuje postavitev "sond" na robove omrežja prav

tako z namenom odvajanja želenih informacij do strežnika, ki analizira vsebino. Obseg vsebin, ki jih analizira, je odvisen od posameznih potreb, izvedbe strežnika za zakonito pestrezanje in zakonodaje. Sama se bolj nagibava k različici, da sonde pošiljajo celoten promet nadzorovane naprave/uporabnika do strežnika za zakonito prestrezanje, ki glede na svoja pravila izlušči potrebne informacije. Takšen koncept je namreč mnogo lažje vzdrževati, saj je potrebno samo osrednje strežnike nadgrajevati z novimi/zahtevnejšimi pravili (storitvami/protokoli).Če bi namreč bilo potrebno "sonde" mesečno ali celo tedensko posodabljati z novo programsko opremo, bi to povzročilo mnogo težav (stabilnost programske opreme, certificiranje pravilnega delovanja, upravljanje naprav, razširljivost, itd.)

A. Centraliziran pristop

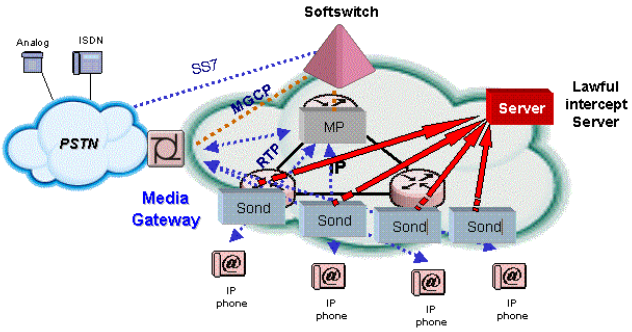
V tem primeru prikazanem na sliki 3 lahko vidimo, da s postavitvijo centralnega strežnika MP za vso komunikacijo poenostavimo tudi vse ostale problematične storitve, vendar se postavlja vprašanje o razširljivosti in zmogljivosti takšnega sistema. To velja še posebej, če se prek tega strežnika prenaša tudi ves podatkovni promet saj je potrebna velika zmogljivost obdelave, da se lahko iz celotnega informacijskega toka izlušči uporabna informacija. Ob vsem tem mora MP zaradi transportnega protokola v realnem času (RTP – Real time Transport Protocol) prav tako delovati v realnem času in skrbeti za signalizacijski in medijski promet IP terminalov.



Slika 3: Centralno prestrezanje klicev

B. Decentraliziran pristop

Druga rešitev predstavlja vključuje evolucijski pristop nadgradnje omrežja z dodatnim elementom (sondo), nadzorovanim s strani krmilnika prehoda med mediji (MGC – Media Gateway Controller). Njegove zmogljivostne in funkcionalne zahteve niso tako stroge, kot v prejšnjem primeru, saj mora na osnovi pravil spremljati le točno določeno obliko prometa, ki ga pa na robovih omrežja tudi ni toliko kot na osrednjem delu. Dodatni elementi ne vnašajo bistvenih zakasnitev v VoIP komunikaciji in prav tako ne spreminjajo informacij v signalizacijskih in medijskih paketih (sogovornik ne zazna da je nadzorovan, saj se ne spremeni pot). Nadgradnje takšnih naprav ali njihove izpeljanke bi lahko bili aplikativni posredniški strežniki, ki bi omogočali VoIP komunikacijo za npr. potrebe IP Centrex tudi prek požarnih pregrad in NAT naprav.



Slika 4: Prestrezanje klicev s pomočjo "sond"

Glavni problem prestrezanja IP paketov oz. VoIP komunikacije z decentraliziranim pristopom je v tem, da lahko katera koli naprava (uporabnik) vzpostavi VoIP klic tudi mimo MGC-ja in na osnovi tega lahko tudi mimo nadzornega sistema, če pozna naslov IP druge naprave (uporabnika) – direktni VoIP klic. Prav tako lahko uporabnik, ki se mu prestreza promet, izmenja med vzpostavljeno VoIP sejo tudi kontrolne informacije z drugim MGC-jem. Te informacije niso vidne v domačem okoljem. To problematiko lahko omejimo z uporabo distribuiranih sond na robovih omrežij, ki spremljajo ves ali omejen promet do/od nadzorovanega uporabnika.

IV. ZAKLJUČEK

Zakonodaja zahteva in predpisuje od ponudnikov telekomunikacijskih storitev vgradnjo programske opreme in vmesnikov za zakonito prestrezanje telekomunikacij katerih namen je zbiranje podatkov o prestreženi telekomunikaciji in njene vsebine ter njihovo posredovanje prek izročilnih vmesnikov do pristojnih služb. Zbrani podatki lahko vsebujejo kopijo sporočil prestrežene telekomunikacije, ter signalizacijske in druge informacije (podatki o sodelujočih v zvezi, času vzpostavitve, trajanju zveze, itd.). Čeprav je bilo zakonito prestrezanje zelo enostavno rešljivo v PSTN svetu, je vpeljava NGN omrežjih in uporaba IP tehnologij za prenos "vseh" podatkov vpeljala nove izzive na tem področju. Med ključnimi izzivi je nagnjenje IP tehnologije za preusmeritev pretoka informacij v času trajanja zveze s pomočjo pošiljanja vsebinskih tokov po različnih poteh. To pomeni, da je lahko pot informacijske

vsebine od kličočega do klicanega in pot v obratno smer različna. Zapletenosti situacije prispevajo tudi različni nestandardizirani protokoli, ki so bili razviti pred postopki standardizacije in niso v skladu s standardnimi predpisi. Rešitve, ki so prikazane v članku opisujejo določene osnovne zahteve, katere mora izpolniti oprema za zakonito prestrezanje v NGN. Razumljivo je, da kompletna rešitev zakonitega prestrezanja telekomunikacij predstavlja izjemno kompleksen problem, ki vključuje vse znane tehnologije za prenos podatkov (TDM, IP, brezžične komunikacije vključno s satelitskimi povezavami, itd.).

LITERATURA

[1] Zakon o telekomunikacijah (ZTel-1), Uradni list RS št. 30/01

[2] Pravilnik o programski opremi in vmesnikih za zakonito prestrezanje telekomunikacij, Ministrstvo za informacijsko družbo, Osnutek/A

[3] International Softswitch Consortium, "Lawfully Authorized Electronic Surveillance For Softswitch-based Networks", Draft March 27, 2002. http://www.softswitch.org/workinggroups/legal.asp

[4] ETSI ES 201 671 V.1.1.1 "Telecommunication Security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunication traffic" http://www.etsi.org

Naim Maloku (maloku@iskratel.si) je magistriral leta 2000 na Fakulteti za elektrotehniko, računalništvo in informatiko v Zagrebu. Rezultate njegovega strokovnega, znanstvenega in raziskovalnega dela najdemo področju telekomunikacijskih protokolov, NGN arhitekture, teorije multiagentov in na področju testiranja programske opreme. Ima veliko izkušenj pri vodenju in tehnični koordinaciji različnih skupnih projektov na področju NGN in nadzora SSN7 omrežja z različnim znanstvenim institucijami kot so Laboratorij za Telekomunikacije, FE Ljubljana in inštitut LONIIS iz S. Petersburga. Je avtor in soavtor več kot 15 referatov na strokovnih konferencah zunaj in v Sloveniji. Zaposlen je v podjetju ISKRATEL d.o.o., kjer je projektni vodja za produkte širokopasovnega dostopa, produktno projektni vodja na področju produktov za nadzor telekomunikacijskih omrežij in produktno projektni vodja za PBX sisteme.

Tomaž Aljaž (aljaz@iskratel.si) je magistriral leta 1999 na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru. Rezultate njegovega strokovnega, znanstvenega in raziskovalnega dela najdemo na dveh področjih. V zadnjem obdobju daje prednost sožitja telekomunikacijskih in podatkovnih omrežij ter uvajanju novih storitev, ki so v teh modernih integriranih informacijskih sistemih omogočene. Drugo pokriva področje analize različnih protokolov, ki prevladujejo v navedenih primerih.

Je avtor in soavtor več referatov na strokovnih konferencah v Sloveniji. Ima certifikate podjetja Cisco Systems s področja načrtovanja in konfiguriranja podatkovnih omrežij (CCNP in CCDP).

Zaposlen je v podjetju ISKRATEL d.o.o., kjer je produktni vodja za IP in konvergečne produkte. Prav tako je soavtor več pilotskih projektov podjetja ISKRATEL. Aktivno sodeluje pri izobraževanju uporabnikov iz področja računalnikih komunikacij.