Analiza tveganj arhitekture IMS

Avtor:
eData d.o.o.

KAZALO

1. UVOD

1.1 PREDSTAVITEV TEME

FMC (Fixed-Mobile Convergence) – fiksno mobilna konvergenca – se nakazuje na eni strani v prototipnih ponudbah pri številnih operaterjih v Evropi, Aziji in Severni ter Južni Ameriki, zlasti pri tistih operaterjih, ki so člani združenja FMCA, v obliki svežnjev storitev in VoIP-a preko WLAN (WiFi) omrežij. Na drugi strani pa se kaže v konsolidaciji in integraciji omrežij in platform na osnovi IP protokola. Privlačnost FMC je predvsem v tem, da omogoča govorne in multimedijske storitve neodvisno od vrste omrežja, dostopovne povezave, terminala in lokacije uporabnika. FMC storitve temeljijo na uporabi IP in SIP protokola pri vseh vrstah dostopa, zato se močno poenostavi izvedba storitev in njihovo upravljanje, kar vpliva na znižanje CAPEX in OPEX celotnega omrežja.

V IMS arhitekturi imamo veliko naprav, ki vršijo določene funkcije v sistemu. Naprave se med seboj povezujejo po standardiziranih vmesnikih. Vmesniki med elementi so notranjega in zunanjega tipa, kar pomeni da so izpostavljeni notranjim in zunanjim zlorabam. Zaradi tega potrebujemo analizo tveganj, kar je tudi namen te seminarske naloge.

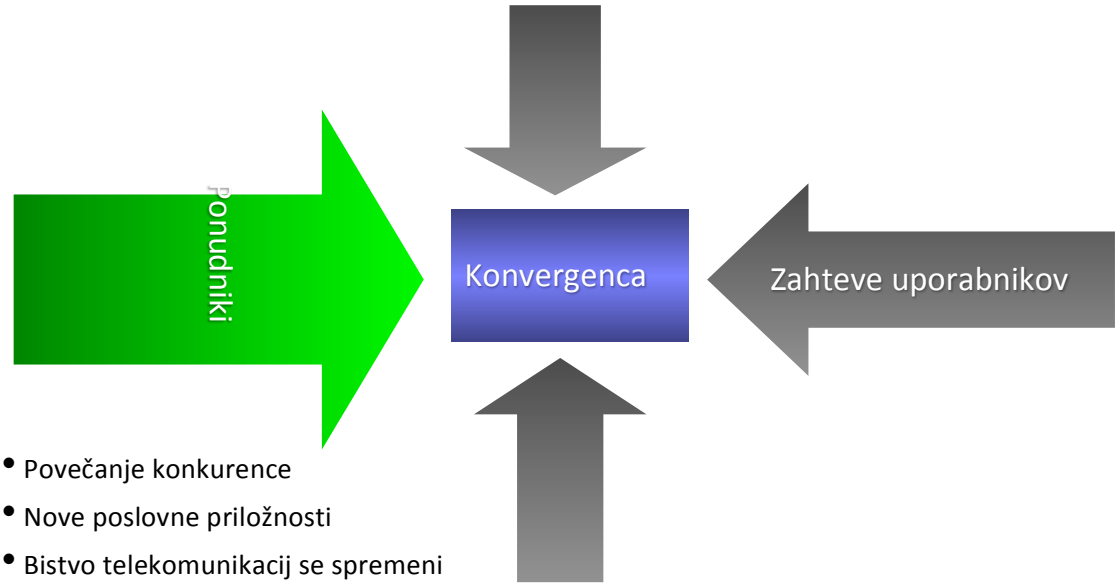
1.2 OSNOVE FMC

FMC (Fixed Mobile Convergence) je koncept, ki odpravlja zgornji problem z navedeno rešitvijo ter ima dolgoročni cilj, kot smo ga pravkar navedli. FMC odpravlja sedanje striktne meje med fiksnimi in mobilnimi telekomunikacijskimi omrežji, pri čemer kombinira mobilna omrežja s širokopasovnimi omrežji in brezžičnimi lokalnimi omrežji, npr. WLAN. FMC pomeni, da lahko uporabnik dobi »katerokoli storitev s katerekoli naprave preko kateregakoli omrežja«. Tako »popolna konvergenca« zahteva nov poslovni model in visoke investicije v nove tehnologije:

1. dostopovnih omrežij: HSDPA, WiFi, meshed WiFi, WiMax, xDSL, FTTx,
2. jedrnih omrežjih: IP/MPLS in/ali carrier grade Ethernet,
3. IP Multimedia Subsystem (IMS).

Konvergenco lahko definiramo v naslednjih treh kategorijah

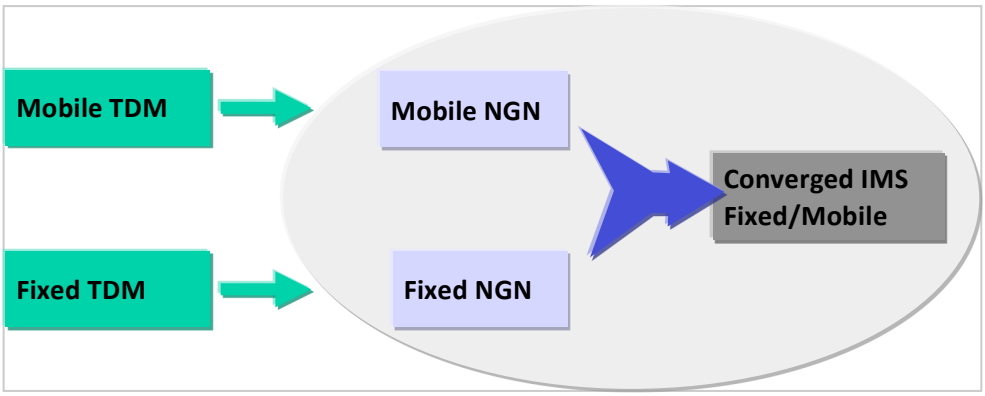
1. Konvergenca naprav; pomeni, da uporabljamo eno samo napravo, ki podpira številne tipe dostopa, npr. GSM, UMTS, WLAN, Bluetooth, WiMax. Dovoljuje uporabo večjega števila storitev in aplikacij in uporabo istih funkcij identifikacije in autentikacije.
2. Konvergenca storitev; pomeni, da kot končni uporabnik dobimo iste storitve neodvisno od dostopovne tehnologije in neodvisno od naprave, preko katere so nam te storitve omogočene.
3. Konvergenca omrežij; pomeni, da poveča učinkovitost ponudnika storitev in zmanjša njegove stroške s tem, da uporablja poenotene principe povezovanja za številna in različna dostopovna omrežja pri zagotavljanju različnih storitev končnim uporabnikom.



Slika 1: Na konvergenco vplivajo dejavniki prikazani na sliki.

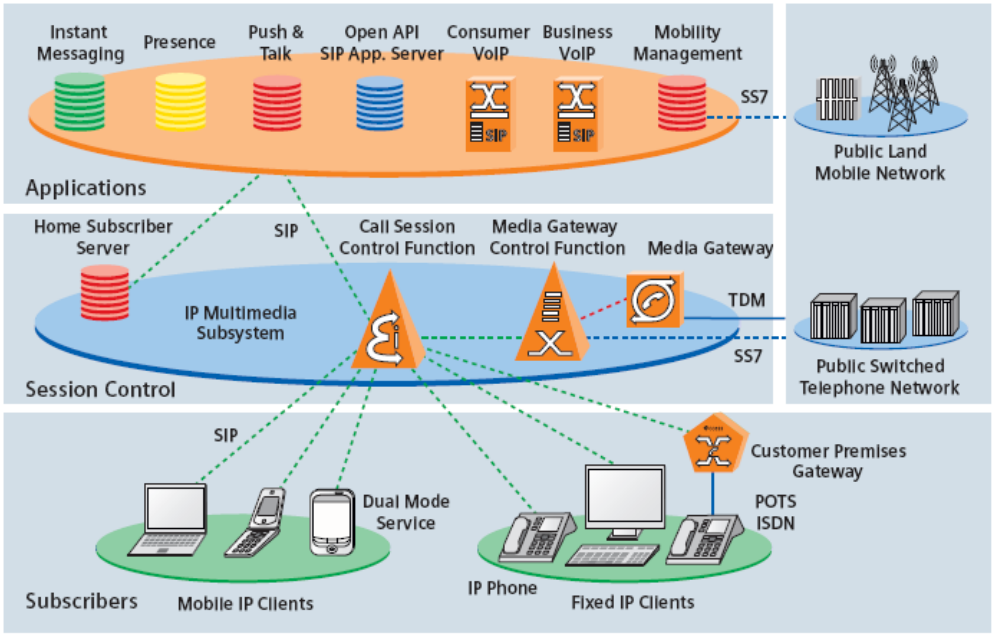
1.3 OSNOVE IMS

IMS je IP Multimedia Subsystem. Je standardizirana arhitektura, ki temelji na SIP protokolu. Izvorno je to mobilni (3GPP/3GPP2) standard. 3GPP deluje skupaj z ETSI TISPAN (fiksno omrežje NGN), da bo IMS specifikacija hkrati podprla različne tako žične kot radijske dostopovne tehnologije in zagotovila medsebojno delovanje bodočih omrežij in storitev z obstoječimi, predvsem z GSM in ISDN/PSTN omrežji in storitvami. UMTS Forum je osvojil naslednjo definicijo za IMS: »IMS je evolucija mobilne tehnologije tretje generacije (3G), ki bo preskrbela na osnovi IP protokola sprotne multimedijske komunikacije, vključujoč IP govor, od osebe k osebi«. IMS je okvir za zagotavljanje na IP/SIP temelječih storitev. IMS omogoča torej sprotne IP multimedijske komunikacijske storitve od uporabnika do uporabnika ne glede na njune lokacije. IMS zagotavlja celovit obseg komunikacijskih storitev z odprtim in varnim dostopom do številnih storitev (lastnih ali od drugih ponudnikov) z možnostjo prehoda na višjo kakovost seje (npr. iz seje teksta v sejo videa).



Slika 2: Prikaz migracija iz starih tehnologij v IP omrežja

Arhitekturo IMS-a tvorijo različne funkcijske ravnine, to so povezovalna ravnina, krmilna ravnina in aplikacijska ravnina. Na sliki 3 je ponazorjeno povezovanje različnih ravnim med seboj, tako da lahko opravljajo vsaka svojo funkcijo. Povezovalno ravnino sestavljajo usmerjevalniki in stikala oz. preklopniki, oboje se uporablja za jedrna in dostopna omrežja. Krmilno ravnino sestavljajo strežniki za nadzor omrežja, ki upravljajo vzpostavljanje klicev ali sej, spremembe in različice protokolov. Najpomembnejša od zgoraj omenjenih je funkcija 'krmiljenja klicne seje' (CSCF – Call Session Control Function), znana tudi kot SIP strežnik. Medmreženje z omrežji drugih operaterjev in drugih vrst omrežij nadzorujejo mejni prehodi Border Gateways (BG).



Slika 3: Prikaz IMS arhitekture, vir Nokia Siemens Networks (2006)

Aplikacijsko ravnino tvorijo aplikacije in strežniki z vsebino, ki izvajajo storitve s dodano vrednostjo za uporabnika. Podporniki splošnih storitev, kakor so opredeljeni v IMS standardu (kot recimo dosegljivost in upravljanje s seznamom skupin), so implementirani kot storitve v SIP aplikacijskem strežniku.

2. PROTOKOLI, VMESNIKI IN STORITVE

2.1 VMESNIKI

Dobra lastnost IMS arhitekture je standardizacija vmesnikov med različnimi gradniki IMS okolja. V okviru IMS arhitekture glede na namen uporabe ločimo notranje in zunanje vmesnike, nekateri vmesniki se pojavljajo hkrati tudi v dvojni vlogi, kot notranji in kot zunanji vmesniki. Notranji vmesniki so standardizirani za vse nivoje ravnin, kot tudi za dostop do zalednih informacijskih sistemov in zunanjih podatkovnih baz. Pravtako so standardizirani tudi povezovalni vmesniki med različnimi IMS okolja, ter med IMS-om in ne IMS okolji, kot so različni aplikacijski SIP strežniki in TDM centralami starih tehnologij. V naslednji tabeli so prikazani le najpomembnejši vmesniki, brez katerih se IMS arhitekture ne da implementirati. Ti vmesniki so bistveni tudi pri pripravi analize tveganj informacijskega sistema.

Ime Vmesnikov	IMS elementi	Opis	Protokol
Cr	MRFC, AS	Uporablja ga MRFC za dostop do dokumentov ali drugih podatkov iz AS	HTTP over dedicated TCP/SCTP channels
Cx	I-CSCF, S-CSCF, HSS	Uporablja se za komunikacijo med I-CSCF, /S-CSCF in HSS	Diameter
Dh	SIP AS, OSA, SCF, IM-SSF, HSS	AS ga potrebuje pri iskanju najprimerjnejšega HSS-a v multi-HSS okolju	Diameter
Dx	I-CSCF, S-CSCF, SLF	I-CSCF/S-CSCF ga potrebuje pri iskanju najprimerjnejšega HSS-a v multi-HSS okolju	Diameter
Gm	UE, P-CSCF	Uporablja se za komunikacijo med UE in CSCF-i	SIP
Go	PDF, GGSN	Operaterjem omogoča nadzor nad kvaliteto storitve v upravljalni ravnini in za izmenjavo tarifnih podatkov med IMS in GPRS omrežjem	COPS (Rel5), Diameter (Rel6+)
Gq	P-CSCF, PDF	Uporablja se za izmenjavo podatkov o dodeljevanju pravic med P-CSCF in PDF elementoma	Diameter
ISC	S-CSCF, I-CSCF, AS	Za izmenjavo sporočil med CSCF in AS	SIP
Ma	I-CSCF -> AS	Uporablja se za direktno usmeritev SIP sporočil javnim uporabniškim identitetam na AS-u	SIP
Mg	MGCF -> I-CSCF	MGCF element pretvarja ISUP siganlizacijo v SIP signalizacijo in posreduje SIP sporočila I-CSCF-ju	SIP
Mi	S-CSCF -> BGCF	Za izmenjavo sporočil med S-CSCF in BGCF	SIP

Mj	BGCF -> MGCF	Uporablja se za izmenjavo sporočil v lastnem omrežju med BGCF in MGCF	SIP
Mk	BGCF -> BGCF	Za izmenjavo sporočil med BGCFs v različnih IMS omrežjih	SIP
Mm	I-CSCF, S-CSCF, zunanje IP omrežje	Uporablja se za izmenjavo sporočil med IMS omrežjem in zunanjimi IP omrežji	SIP
Mr	S-CSCF, MRFC	Za izmenjavo sporočil med S-CSCF in MRFC	SIP
Mw	P-CSCF, I-CSCF, S-CSCF	Za izmenjavo sporočil med CSCFs	SIP
Rf	P-CSCF, I-CSCF, S-CSCF, BGCF, MRFC, MGCF, AS	Uporablja se za izmenjavo »offline« tarifnih podatkov z CCF elementom	Diameter
Ro	AS, MRFC, S-CSCF	Uporablja se za izmenjavo »online« tarifnih podatkov z ECF elementom	Diameter
Rx	P-CSCF, PCRF	Za izmenjavo podatkov o politiki delovanja in podatkov o zaračunavanju med P-CSCF in PCRF (Policy and Charging Rule Function). Nadomešča tudi Gq referenčno točko.	Diameter
Sh	SIP AS, OSA SCS, HSS	Uporablja se za izmenjavo informacij med SIP AS/OSA SCS in HSS-om	Diameter
Sr	MRFC, AS	Uporablja ga MRFC za dostop do dokumentov ali drugih podatkov iz AS	HTTP
Ut	UE, AS (SIP AS, OSA SCS, IM-SSF)	Omogoča upravljanje in preverjanje nastavitev uporabniških storitev	HTTP(s), XCAP

Tabela 1: Najpomembnejši IMS vmesniki

2.2 STORITVE

IMS za svoje delovanje potrebuje določene funkcionalnosti, ki omogočajo uspešno komunikacijo med različni IMS elementi. Te funkcionalnosti imenujemo drugače tudi IMS storitve, ki jih potrebuje arhitektura za komuniciranje med različnimi entitetami, za premešlanje med različnimi tehnologijami, prevajalnimi in poizvedovalnimi tehnologijami, dostopa do imeniških strežnikov in varnostnih mehanizmov. V naslednji tebeli so navedene vse storitve in njihovi grobi opisi, ki so dovolj za razumevanje tematike.

Ime storitve	**Opis storitve**
Call Control Service	Call Control Service vsebuje vse korake vzpostavitve zveze, poročanja delovanja zveze, vmesnih informacij storitve in ruženja zveze. To storitev izvaja nadzornik sej (Call Controller). Znotraj posameznega omrežja je lahko več nadzornikov sej.
Directory Service	VoIP protokoli uporabljajo "Directory Service" tipično za prevajanje

	logičnih imen, uporabniških imen, E.164 imen, DNS imen in raznih dopolnitev v enolično določeno uporabniško točko.
Gateway Service	Velikokrat se pojavi potreba po komunikaciji med različnimi vrstami omrežij. "Gateway Service" storitev omogoča prevajanje prometa med različnimi vrstami omrežij. Najpogosteje govorimo o prehodu med IP in TDM omrežji.
Network Service	VoIP storitev velikokrat potrebuje osnovne povezovalne protokole za uspešno vspostavitev komunikacije med dvema odjemalcema. Med te storitve štejemo DNS, TFTP, FTP, DHCP, HTTP, Telnet, RADIUS in DIAMETER.
Session Border Control Functions	Na določenih robnih točkah našega omrežja potrebujemo niz funkcionalnosti procesiranja in filtriranja zvez ter varnostnih mehanizmov (med različnimi avtonomnimi sistemi, med dostopnim in jedrnim omrežjem, itd..).

Tabela 2: IMS storitve

2.3 PROTOKOLI

V okviru IMS arhitekture je primarni sejni protokol SIP protokol. SIP protokol je protokol, ki za svoje delovanje potrebuje nižje ležeči IP protokol, zaradi tega tudi IMS protokoli uporabljajo za vso svojo komunikacijo IP protokol. Poglejmo si najpogostejše in največkrat uporabljene protokole za komunikacijo med entitetami znotraj in izven IMS sistema.

Protokol	Opis protokola
COPS	Common Open Policy Service. Zelo enostaven protokol za povpraševanje in izmenjavo podatkov o politiki delovanja med strežnikom in odjemalci. [IETF-COPS]
DHCP	Dynamic Host Configuration Protocol. Protokol za avtomatsko pridobitev različnih TCP/IP nastavitev (IP naslov, maska omrežja, privzeti usmerjevalnik, DNS strežnik, itd.) na odjemalcih. [IETF-DHCP]
DIAMETER	Diameter protocol omogoča AAA framework za aplikacije kot so dostop do omrežja ali prenosljivost IP nastavitev. [IETF-DIAMETER]
DNS	Domain Name Service je omrežna storitev, ki naredi prevedbo domesnkega imena v IP naslov. [IETF-DNS]
FTP	File Transfer Protocol je protokol za prenos podatkov, ki za svoje delovanje uporablja nižjeležeči TCP protokol. [IETF-FTP]
H.323	Skupek specifikacij, ki definirajo uporabo protokolov (kot so H.225, H.245, and T.120) za prenos multimedijske vsebine preko komunikacijskih omrežij. [ITU-TH323]
HTTP	Hypertext Transfer Protocol je aplikacijski protokol za distribuirane, medijske informacijske sisteme. Hkrati je tudi privzeti protokol za prenos spletnih vsebin in dokumentov. [IETF-HTTP]
IP	Internet Protocol (IP) je usmerjevalni protokol (layer 3). IP protokol se uporablja v javnem internetnem omrežju. [IETF-IP]
Megaco / MGCP	Megaco in MGCP (Media Gateway Control Protocol) je protokol, ki se uporablja za sporazumevanje in nadzor medijskih prehodov in odjemalcev. Megaco protokol je znan kot H.248. [IETFMEGACO],[IETF-MGCP]

RADIUS	Remote Authentication Dial-In User Service protokol se uporablja za centralizirano avtentikacijo, avtorizacijo in zaračunavanje za klicni, širokopasovni in brezžični dostop ter za VPN omrežja. [IETF-RADIUS]
RTP	Real Time Protocol se uporablja za izmenjavo multimedijskih tokov, kot je govor in video med odjemalci. [IETF-RTP].
RTCP	Real Time Control Protocol se uporablja za nadzor nad RTP sejami. [IETF-RTCP]
SIP	Session Initiation Protocol je aplikacijski signalni protokol za vspostavljanje in zaključevanje multimedijskih sej ali govornih tokov. [IETF-SIP]
SNMP	Simple Network Management Protocol je upravljalni protokol, ki se uporablja za prenašanje in spreminjanje podatkov iz upravljanih naprav. [IETF-SNMP]
SS7	Signaling System Number 7. SS7 je signalizacijski protokolni sklad, ki se uporablja v Public Switched Telephone Network (PSTN) za izmenjavo signalizacijskih informacij med telefonskimi centralami.
TCAP	Transaction Capabilities Application Part. TCAP je protokol, ki podpira izmenjavo storitev v žičnih in brezžičnih telefonskih omrežjih.
TCP	Transmission Control Protocol se pogosto uporablja kot transportni protokol (4-ti nivo) za zanesljive sejno orientirane komunikacije in je sestavni del TCP/IP protokolnega sklada, ki se za primarno komunikacijo uporablja tudi v internetu. TCP je sejno orientiran protokol, kar pomeni da se mora prvo uspešno vzpostaviti seja predno si pošiljatelj in prejemnik izmenjata podatke. [IETFTCP]
Telnet	Telnet protokol se uporablja za vspostavitev daljinske tekstovno orientirane seje med dvema napravama. [IETF-TELNET]
TFTP	Trivial File Transfer Protocol je preprost protokol, ki uporablja UDP protokol za izmenjavo datotek. [IETF-TFTP]
UDP	User Datagram Protocol je protokol transportnega nivoja (4-ti nivo).UDP protokol ni, za razliko od TCP-ja, sejno orientiran protokol in ne preverja uspešnosti prenosa podatkov in ne omogoča ponovnega pošiljanja izgubljenih oz. okvarjenih paketov. [IETF-UDP]

Tabela 3: Najpogosteje uporabljeni protokoli v IMS okolju

3. SOCIOLOŠKE GROŽNJE

Arhitektura IMS ponuja uporabnikom veliko različnih možnosti. Uporabniki dostopajo do sistema direktno in posredno. Sociološke grožnje so pomemben del, ki ga moramo upoštevati pri analizi. Družbene potrebe varnosti in zasebnosti so zelo pomembne. Načrtovalci jih morajo uravnovesiti med druge življenjskih potrebe, kot sta naprimer donosnost naložb in udobje. Umestitev varnosti in zasebnosti v družbeni kontekst lahko naredimo na različne načine:

- Osnovni večstrankarski svobodni model, ki se uporablja za vsak javni komunikacijski sistem;
- Osnovni model opredeljuje zasebnosti in jo povezuje z varnostjo;
- Model družbene odgovornosti, ki temelji na splošno sprejetih načel v civilnem in splošnem pravnem redu.

Vsi ti modeli zagotavljajo enostaven okvir za uravnoteženje in varnost zasebnosti z drugimi potrebami.

3.1 VRSTE SOCIOLOŠKIH GROŽENJ

3.1.1 Osnovni večstrankarski svobodni model

Sodobni interaktivnih komunikacijski sistemi lahko vsebujejo več kot dve osebi v eni seji, kjer osebe hitro menjajo posamezno vlogo v komunikaciji:

- izvorni pobudnik seje,
- Oseba se pridruži seji,
- prejemnik seje,
- podiralec seje (zaključitev),
- zavrnitev zahteve po seji.

Večstrankarskih svoboda je kontinuiteta svobode, ki se poraja, ko si vloge izmenjuje nedoločeno število ljudi, ki imajo lahko različne potrebe in hotenja. Večstrankarski svoboda je praktično obvezen pogoj za vse razširljive sporočilne sisteme. Ta zahteva je implicitna zlasti za VoIP storitve. Osnovni večstrankarski svobodni model je komunikacijski sistem, ki izpolnjuje naslednja merila za vse uporabnike:

- Uporabnik lahko povabi kogarkoli,
- Uporabnik se lahko pridruži večim strankam hkrati,
- Uporabnik lahko zavrne povabilo,
- Uporabnik lahko zapusti sejo,
- Uporabnik lahko navede soglasje za katerikoli stik ali za vse stike ter poročanja,
- Uporabnik lahko zavrne soglasje za katerikoli stik in za vse stike ter poročanja,
- Uporabniku je zagotovljena zakonsko zahtevana zaupnost in imuniteta,
- Uporabnik lahko določi lastno politiko.

3.1.2 Zasebnost; varnost kot dvojna zasebnost

Koncept zasebnosti je privilegij posameznika pred nedovoljenimi posegi v komunikacijske sisteme. Nedovoljeni posegi so prisluškovanja, prekinitve, zakasnitve in spremembe vsebin. Nedovoljen poseg je definiran kot poskus nezakonitega vdora v komunikacijske tokove posameznikov. Varovanje zasebnosti ločujemo na:

- Pravica do ščitenja zasebnosti,
- Metodologija zagotavljanja zasebnosti,
- Načini ščitenja kominikacijskih sistemov in vsebin pred nedovoljenimi posegi.

3.1.3 Model sociološke odgovornosti

Osnovni model družbene odgovornosti določajo nameni in učinki ravnanja oseb predno se sprejme ocene kaj naj sistemi zanikajo, prenašati ali dovoljujejo. Namen je merjen z stanjem zavesti, ki je zakonodajno nesporno vključujoč ukrepe, ki so namensko naravnani. Nameni so lahko nepremišljeni, zavedajoči, malomarni ali pa razumni.

3.1.4 Lažne navedbe

Osnovni Izraz lažnih navedb generično pomeni napačne ali zavajajoče komunikacije. Zavajanje vključuje dostavo napačnih podatkov o identiteti, lastniku pravic, organu in ostalih lažnih pravicah drugih strank v posredovanih informacijah. Pod sklop lažnih navedb štejemo:

1. Lažna identiteta,
2. Lažni avtoritetni organ,
3. Lažne pravice,
4. Napačno predstavljena oz spremenjena vsebina.

3.1.5 Kraja storitev

Kraja storitev je kakršnokoli nezakonito pridobivanje gospodarske koristi storitve ponudnika z namenom nezakonitega prilaščanja pravic ali pridobivanja nezakonitih prihodkov oz. premoženja. Med tovrstne kraje štejemo:

1. Nedovoljeno brisanje ali spreminjanje računskih zapisov,
2. Nedovoljeno izogibanje zakonitih sistemov prestrezanja,
3. Nedovoljeno zaračunavanje,
4. Prevzem pravic ponudnikom storitev,
5. Prevzem pravic lastnikom vsebin.

3.1.6 Nezaželjeni stiki

Nezaželeni stiki so stiki brez vnaprejšne privolitve posameznika v komunikacijo. Še hujša oblika nezaželenih stikov so poskusi po ponovnih komunikacijah ob predhonem nestrinjajo oz. zavrnitvi predhodne zahteve po vspostavitvi komunikacije. Vrste nezaželenih stikov so:

1. Nadlegovanje,
2. Izsiljevanje,
3. Vsiljevanje nezaželenih vsebih.

4. IDENTIFIKACIJA MEHANIZMOV ZLORAB, NAPADOV IN KRAJ IDENTITET

Tako uporabnikom kot operaterjem predstavlja glavno prioriteto zanesljiva, varna komunikacija. Pri IMS-u lahko operaterji implementirajo storitve od konca do konca (E2E), zasnovane na številnih temeljnih kamnih IMS-ove varnostne in omrežne arhitekture. Mednje sodi temeljna IMS-ova lastnost, da se od operaterja nadzorovane storitve nudijo avtenticiranim uporabnikom. Izvirni operater ima odgovornost od konca do konca (E2E) v skupnosti operaterjev. Nobena storitev se ne dobavlja anonimnim ali dvomljivim končnim uporabnikom, niti se storitev ne posreduje anonimnim ali zaupanja nevrednim operaterjem in podjetjem. Veriga odgovornosti je zasnovana na naslednjem:

- IMS avtentikaciji,
- krmiljenih IMS storitvah, ki nudijo storitve avtoriziranim uporabnikom,
- sporazumih med operaterji, ki odrejajo odgovornost in podobno,
- varnim medsebojnim povezovanjem med omrežji.

Poleg tega se pri koristnem prenosu (v prvi vrsti neglasovnem in video) preverja, če ima kakšen virus. Varnost dostopne domene se zagotavlja prek avtentikacije uporabnikov in 'enkratne prijave' t.i. single sign on (SSO) za vse storitve do katerih je uporabnik avtoriziran. Varnost omrežne domene mora biti zagotovljena preko:

1. zaščite na spletni strani za gostujoče rešitve,
2. krepitve vozlišč,
3. protivirusne zaščite in
4. nadzorovanega prijavljanja.

Vsak sistem ima svoje slabosti. Napad je nedovoljen dostop ali poskus dostopa do sistema. Napak se dogodi, ko se odkrije ranljivost sistema. Glede na vrsto napada jih ločujemo v dve skupini:

- pasivni napadi,
- aktivni napadi.

Pasivni napadi, kot je »eavesdropping« poskušajo priti do informacijskih podatkov, včasih pa pasivnost lahko preraste v agresijo. Aktivni napadi pa so tisti, ki poskušajo spremeniti in pokvariti podatke ter onesposobiti delovanje sistema. Napadalce na SIP oz. IMS med seboj ločimo na več skupin:

- Napadalci, ki IMS napadejo tako kot vsak IT sistem. Ti so lahko zunanji hekerji ali pa notranje zlonamerne osebe.
- Napadalci, katerih tarča je SIP protokol, torej SIP transakcije. Tu zopet poznamo dve različni vrsti. Prva so napadi s tretje strani, kjer napadalec ni del napadene SIP transakcije (pošiljanje in sprejemanje), ti lahko spremenijo SIP sporočilo in v transakciji pride do napake. Druga vrsta so napadi, kjer je napadalec del SIP transakcije. Napadalec poskuša pridobiti vitalne podatke od SIP strežnika ali SIP odjemalca, kot so npr. identifikacijski podatki,…

Različne vrste groženj za IMS vsebujejo računske zlorabe, kraje identitet, kraje podatkov in motnje delovanju storitev. Če implementacija govorne signalizacije (SIP), dobave govorne storitve (RTP) in nadzornih protokolov (RTCP) ni dovolj dobro in skrbno pripravljena za avtentikacijske mehanizme in za end-to-end (E2E) integriteto storitve imajo napadalci priliko zlorabiti sistem. V naslednjih razdelkih bodo obravnavane nevarnosti oz. grožnje za IMS arhitekturo. Nevarnosti smo razdelili na naslednje sklope:

- splošno znane IP nevarnosti in napadi,
- znani DoS napadi usmerjevalnega in transportnega nivoja (L3 in L4),
- splošno znani DoS napadi aplikacijskega nivoja (L7),
- nevarnosti za IMS avtentikacijo,
- nevarnosti za IMS oz. SIP signalni promet,
- nevarnosti za sejni in govorni (RTP) promet,
- nevarnosti infrastrukturnih in internih napadov.

Splošno znani DDoS napadi (Distributed DoS Attacks) predstavljajo zelo resno nevarnost.

4.1 SPLOŠNO ZNANE IP NEVARNOSTI IN NAPADI

V tem poglavju sem povzel splošne znane nevarnosti in napade, ki veljajo za internetni promet. Napad je nedovoljen dostop ali poskus dostopa do sistema. Napak se dogodi, ko se odkrije ranljivost sistema. Pasivni napadi, kot je »eavesdropping« poskušajo priti do informacijskih podatkov, včasih pa pasivnost lahko preraste celo v agresijo. Aktivni napadi pa so tisti, ki poskušajo spremeniti in pokvariti podatke ter onesposobiti delovanje sistema. Splošno znane IP nevarnosti in zlorabe so naslednje:

- “Eavesdropping” napadi,
- “Spoofing” napadi,
- “Man-in-the-Middle” napadi,
- “Replay” napadi,
- “Modification” napadi,
- “Hijacking“ in “Termination” napadi,
- “Implementation Dependent” napadi,
- “Buffer Overflow” napadi.

»Eavesdropping« je zlonamerna metoda, ki prestreza RTP medijske tokove in spreminja SIP signalizacijska sporočila. V SIP signalizacijskih sporočilih se prenašajo tudi podatki o uporabniških lokacijah, ključih za dekripcijo medijskih tokov, IVR signalizacijski podatki, občutljivi podatki o topologiji omrežja, itd..

Kako se lahko zaščitimo ?

Obramba pred »eavesdropping« metodo je kodiranje podatkov s pomočjo kodirnih mehanizmov kot je uporaba SRTP protokola, uporaba IPsec protokola ali pa TLS protokola za kodiranje SIP sporočil, mogoče tudi RTP prometa.

Naslednje vrste napadi so »Spoofing« napadi. Pri spoofingu govorimo o zlorabi identitet uporabnikov ali strežnikov. Napadalec lahko zlorabi identiteto avtoriziranega uporabnika za določeno storitev. Za primer če nimamo implemetiranega preverjanja IMS entitet (identity) lahko povemo, da napadalec z spremembo podatkov v UA enostavno lahko prepiše v sporočilu INVITE naslov From:”napadalec“ v From:”uporabnik“. Drug primer pa je uporaba ukradenega ali

uganjenega uporabniškega imena in gesla. Enostavnejši spoofing napadi na SIP protokol imajo podobne lastnosti kot »phishing« napadi na SMTP protocol. Dodatna ranljivost je premajhno polje na prikazovalnikih SIP terminalov za prikaz identitete klicatelja. Če napadalec za informacijo o klicatelju v SDP sporočilo vrine predolgo ime za polje »Display Name«, potem klicani UA SIP terminal ne more prikazati na prikazovalniku identiteto klicatelja.

Kako se lahko zaščitimo ?

Za ta napad imamo zelo učinkovito obrambno metodo, to je uporaba avtentikacije sporočil s pomočjo HTTP Digest ali IMS AKA protokola.

Ko napadalec prestreže sporočilo in spremeni vsebino sporočila govorimo o Man-in-the-middle napadu. Napadalec prestreženo SIP sporočilo lahko spremeni ali celo ustvari novo SIP sporočilo. Posledice tega napada so ukradena registracijska sporočila, prekinitve aktivnih sej, prevzem aktivne seje, zloraba identitete, dodajanje šuma v sejo, povzročanje zakasnitev, ipd… Man-in-the-middle napadi so zelo pogosti v WLAN omrežjih kot so Hot-Spot in Hot-Zone točke. Veliko WLAN omrežij je zelo slabo zaščitenih.

Kako se lahko zaščitimo ?

Zaščitimo se z avtentikacijo obeh končnih točk, za ščitenje integritete E2E pa je potrebno uporabiti znane mehanizme za integriteto sporočil kot so:

- enkripcija (encrypt),
- prstni odtisi (fingerprint),
- podpisi (sign).

»Replay« napadi uporabljajo metodo ponavljanja pošiljanja originalnega sporočila strežniku, ki mora vsa sporočila seveda obdelati. Če se nezaščiteno SIP sporočilo ponovi velikokrat lahko pride do zaustavitve storitve. Posledice tega napada so lahko finančne izgube, slaba publiciteta, izguba ugleda, razkritje informacij …

Kako se lahko zaščitimo ?

Z uporabo mehanizmov za ščitenje integritete (encrypt/fingerprint/sign) in uporabe številčenja sporočil (sequence number), za SIP je to kombinacija CSeq in Call-ID podatkov v glavi sporočil, lahko preprečimo tovrstne napade.

Poznamo tudi »Modification« napade. Zagotoviti moramo, da je poslano sporočilo enako prejetemu sporočilu, torej v omrežju med uporabnikoma ne sme priti do spremembe v poljih sporočila. Če ne uporabljamo zaščite integritete in varnostnih mehanizmov v komunikacijskem protokolu lahko napadalec ponaredi posamezna polja v sporočilu. S tem lahko napadalec dobi dostop do storitev do katerih ni upravičen, blokira lahko druge uporabnike, uspe mu lahko ukrasti identiteto uporabnika, lahko tudi posega v aktivne seje.

Kako se lahko zaščitimo ?

Zaščitimo se z enakimi mehanizmi kot pri »Replay« napadih.

Obstajajo tudi »Hijacking« in »Termination« napadi. Napadalec lahko uporabi REGISTER sporočilo, da zamenja identiteto napadenega s svojo identiteto. Če mu to uspe lahko ukrade seje oz. pogovore (Call Hijacking). Z uporabo REGISTER sporočila lahko de-registrira uporabnika iz sistema, s tem pa se vsi klici na omenjenega uporabnika končajo neuspešno, uporabnik ni več registriran in klicatelji dobijo sporočilo »uporabnik ni dosegljiv«. Drug primer je uporaba REFER sporočila. To sporočilo se uporablja za preusmerjanje klicev drugam, na druge UA. Posledice tega napada je sprememba preusmerjanja na novo lokacijo, uporabniku zvoni potem pa se klic prenese

na novega odjemalca, ki je lahko napadalec ali pa nekdo tretji. Z uporabo BYE sporočila pa lahko napadalec zaključi seje nasilno, prekini aktivne povezave. Še ena uporabnost je poneverba "6xx" sporočil. S tem lahko napadalec povzroči stanje, da se klicane noče oglasiti, lep primer je sporočilo "Cancel". Ker pa je SIP večinoma UDP, pa lahko s spremenjenimi ICMP sporočili "port unreachable" tudi neke vrste DoS napad. Prav tako se lahko zlorabi sporočilo ACK.

Kako se lahko zaščitimo ?

Uporaba avtentikacije prepreči vse vrste teh zlorab.

»Implementation Dependent« napadi so tudi velikokrat uporabljeni pri napadih. Poznamo veliko implementacij protokolov, ki nimajo ustreznega mehanizma za popravljanje napak. Obstaja nekaj predvidevanj v protokolih, kot je na primer maksimalna dolžina polja, konsistenca sporočila,… Če pride v protokolu do neustrezno oblikovanega sporočila, lahko hitro pridemo do situacije, ko postane sistem nestabilen ali pa se celo lahko ponovno zažene oz. celo ugasne. "Ping of Death" je primer takšnega napada. Zlorabi se ICMP paket, kjer se mu spremeni velikost preko vseh protokolnih omejitev. Zlorabi se lahko tudi TCP/IP protokol. Primer je lahko, da imata prejemnik in pošiljatelj isto vrednost za podatkovni par IP naslov/število port-a. Večino teh hroščev bodo proizvajalci operacijskih sistem prej ali slej odpravili. Zavedati pa se moramo, da obstajajo in da se bodo pojavljali vedno novi.

Kako se lahko zaščitimo ?

Najboljša zaščita je redno osveževanje popravkov, ki jih objavljajo programske hiše.

»Buffer overflow« napadi so zelo pogosti IT varnostni problem. Statistično je skoraj vsako drugo poročilo oz. popravek napisan zaradi te ranljivosti. »Buffer« je določen del spomina, ki se uporablja, da aplikacija začasno hrani podatke. Če aplikacija poskuša zapisati več podatkov, kot jih ima trenutno na razpolago, pride do omenjenega problema, kjer lahko prepiše podatke drugi niti ali drugi aplikaciji. Zelo vešč napadalec lahko z branjem in vpisovanjem v »buffer« prevzame nadzor nad aplikacijo. Manj vešč napadalec lahko povzroči nedelovanje sistema. Na splošno je zelo težko predvideti, kateri del je bil »nezaželeno« prepisan ali spremenjen s strani napadalca. Kakorkoli, ker pa »buffer« dela na procesorskem skladu pa postane zanimivo. Procesorski sklad je polje, ki omogoča klicanje funkcij, shranjevanje podatkov, itd… Ta zloraba lahko zelo nevarna.

Kako se lahko zaščitimo ?

Zaščita pred »Buffer overflow« napadom na strani odjemalca je v zaščiti operacijskega sistema odjemalca. Pri zaščiti pred »Buffer overflow« napadom na strani strežnika lahko uvedemo določene protiukrepe. Na nivoju operacijskega sistema strežnika lahko:

- zaklenemo velikosti »buffer«-ja,
- stalno preverjamo dolžino C knjižnic,
- uporabljamo »varen« programski jezik, kot je npr. Java ali Jainslee
- promptno instaliramo varnostne popravke,
- uporaba ne-zagonskih skladov,
- preverjanje skladov,
- povezovanje z varnimi knjižnicami (objavljene kot »trusted« s strani proizvajalca OS-a).

4.2 SPLOŠNO ZNANI DOS NAPADI

Za DoS napade označimo vse tiste napade, kjer je namen uporabniku onemogočiti storitev. S tem napadom se napadeni strežnik (žrtev) obremeni z jalovim prometom tako, da je prezaseden in ne more več opravljati svojega namena, v našem primeru ponujati IMS storitve. Poleg IMS aplikacijskega strežnika, so lahko napadene še požarne pregrade, usmerjevalnike, strežnike v DMZ coni, ostale aplikacijske strežnike (web services, SMTP strežnik, IM, strežnik prenosljivosti številk,..). Splošno znani DoS napadi omrežnega in transportnega nivoja (L3/L4) so:

- »Bandwidth Exhaustion« napadi,
- »Packet Fragmentation and Reassembly« napadi,
- »Router« napadi,
- »Land« napadi,
- »Flooding« napadi,
    - »Network Flooding« napadi,
    - »Firewall/BGW Flooding« napadi,
- »Chargen« napadi,
- »Operating System Specific DoS« napadi.

Najbolj enostaven napad je napad porabe pasovnih širin (Bandwidth Exhaustion Attacks), ki ga lahko izvede tudi laik. Napadalec pošlje večjo količino prometnih podatkov žrtvi. Uporablja se različne tipe protokolov. Če je napad enostavno narediti, pa je obramba pred njim zelo zapletena. Potrebujemo sodelovanje različnih omrežnih elementov, da se nepotrebne pakete na poti zavrže.

Kako se lahko zaščitimo ?

Uporaba DPI naprave je zelo učinkovita rešitev.

»Packet Fragmentation and Reassembly« napadi so napadi, kjer napadalec upa, da bo prejemnik dobil stotine ali tisoče zelo fragmentiranih preverjenih povezav. Fragmentacija zelo obremeni procesno moč, ker se mora potruditi sestaviti delčke povezav v celoto, da lahko izvede operacijo in odgovori, če je potrebno. Dober heker pošlje poplavo fragmentov, ki jih poskuša prikazati kot legitimen promet žrtvi, učinek na žrtev je preobremenitev procesorja, premajhen spomin in »buffer«, posledična lahko žrtev zablokira.

Kako se lahko zaščitimo ?

Zelo učinkovita zaščita pred tovrstnimi napadi so zaščitne funkcionalnosti aplikacijskih strežnikov. Aplikacija mora imeti vsebovano programsko logiko, ki dopušča oz. omejuje fregmentacijkse metode. Fregmentacijsko metodologijo se da ločiti, na izvormo fregmentacijo ali na vmesno fregmentacijo.

Napad na usmerjevalnike (router attack) je eden najtežje izvedljivih napadov. To je napad na usmerjevalne tabele usmerjevalnika. Napade se ga z informacijam o preusmerjanju (re-routing). Vršita se dve vrsti napada, prvi je polnjenje usmerjevalnih tabel z neustreznimi podatki o usmerjanju, drugi je poskus narediti loop-e usmerjevalniku. Velikokrat napadalci poskušajo z kombinacijo loop-ov in »eavesdropping« metode.

Kako se lahko zaščitimo ?

Pravilna zaščita je ustrezna usmerjevalna politika. V usmerjevalni politiki morajo biti vključene omejitve cen posameznih povezav, dovoljevanje oz. preprečevanje dinamike spreminjanja usmerjevalnih zapisov, omejevanje usmerjanja glede na vrsto vmesnikov, ki so lahko notranji ali zunanji, itd..

»Land« napadi (Land Attack) so napadi s uporabo Lanc C programske opreme. Land C je program, ki pošilja validirane TCP pakete prejemniku. V TCP paketih sta pošiljateljev in prejemnikov IP naslov enaka, pošiljateljev IP naslov je ponarejen. Prejemnik poskuša paket poslati nazaj, vendar ga pošlje sam sebi. Lahko pa je še bolj kompliciranо procesiranje če se uporabi kombinacijo IP naslov/port. Land je kombinacija SYN paketov skupaj z IP spoofing paketi, enako velja tudi za SYN-ACK pakete.

Kako se lahko zaščitimo ?

Uporaba naprednih varnostnih naprav, ki varujejo aplikacijske strežnike je dovolj dobra zaščita. Land napadi so zelo znana grožnja, obrambo pred njo pa omogočajo skoraj vse požarne pregrade.

Pri »Flooding« napadih oz. poplavljanju ločimo poplavljanje požarne pregrade in poplavljanje omrežja za požarno pregrado. Primeri poplavljanja omrežja so :

- SYN poplava,
- ICMP poplava,
- UDP poplava,
- »Smurf« napadi (ICMP na broadcast naslove).

Primeri poplavljanja požarne pregrade pa so:

- poplava tabele sej (Session Table Flood),
- SYN-ACK-ACK Proxy poplava.

Kako se lahko zaščitimo ?

Trenutno ne poznamo posembnih metod zaščite. Priporoča pa se določeno predimezioniranje opreme glede procesne moči in spomina, da lahko strežniki opravljajo svoje delo kljub napadu.

»Chargen« napadi (Chargen attack) so napadi s uporabo »Chargen« programske opreme. Aplikacija “Chargen” je generični serijski znakovni generator. Primarna uporaba je implementirana s UDP paketi, vendar se ga lahko po-uporabi tudi za TCP pakete, oz. za kombinacijo TCP in UDP paketov. Uporablja port 19. Port 19 je večinoma odprt na vseh operacijskih sistemih. Hekerji poskušajo preko port-a 19 poslati veliko količino podatkovnih smeti, z namero da uporabijo čim večjo procesno moč žrtve.

Kako se lahko zaščitimo ?

Trenutno ne poznamo posembnih metod zaščite. Priporoča pa se določeno predimezioniranje opreme glede procesne moči in spomina, da lahko strežniki opravljajo svoje delo kljub napadu.

Naslednje vrste napadi so napadi na operacijske sisteme (OS Specific DoS Attacks). Napadalec poskuša napasti sistem s pomočjo zlorabe ranljivosti operacijskega sistema. Če napadalec poleg IP naslova ugotoviti tudi izbrani operacijski sistem, potem se mu ni treba poslužiti brutalnega napada, ampak lahko izbere bolj prefinjene metode, lahko si izbere paket ali dva, ki določeni OS lahko onesposobi(ta).

Napad se izvrši z zelo malo truda, primera pa sta:

- Ping of Death Attack,
- Teardrop Attack.

Kako se lahko zaščitimo ?

Posodabljanje operacijskega sistema in instaliranje verificiranih popravkov je trenutno edina in seveda tudi najboljša zaščita pred napadom.

4.3 ANALIZA GROŽENJ

Pri analizi groženj sem nevarnosti, ki pretijo storitvenim strežnikom segmentiral glede na:

1. metodologijo, ki jo izvor nevarnosti uporablja,
2. željeni cilj grožnje,
3. nivo delovanja,
4. zahtevi po avtentikaciji in
5. protokolu zlorabe.

Pomembna je korelacija med posameznimi nevarnostmi in uporabljenimi omrežji za posamezne storitve. V tabeli 4 so navedene nevarnosti glede na dostop do IMS arhitekture.

Vrsta dostopa	Mobilni	Brežični	Fiksni (žični)	Med-omrežno povezovanje
Poplavljanje L3 in L4 nivoja	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo
Ranljivost OS omrežnih elementov	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo
SIP DoS napadi	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo
Zgodnje IMS nevarnosti	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Ni nevarnosti
Nevarnosti povezane s HTTP Digest in SIP	Ni nevarnosti	Ni nevarnosti	Nevarnosti obstajajo	Ni nevarnosti
Napadi na odjave UE	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo
»SIP-Header Content Piggybacking« napadi	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo
»Bypassing« napadi	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo
Ponovna registracija v IMS ob spremembi IP naslova širokopasovnega uporabnika	Ni nevarnosti	Ni nevarnosti	Nevarnosti obstajajo	Ni nevarnosti
Nevarnosti za (RTP) medijski promet	Ni nevarnosti	Ni nevarnosti	Nevarnosti obstajajo	Nevarnosti obstajajo
Nevarnosti iz omrežij drugih IMS operaterjev	Ni nevarnosti	Ni nevarnosti	Ni nevarnosti	Nevarnosti obstajajo
SIP SPAM napadi	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo
Virusi in črvi	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo
IPv6 napadi	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo	Nevarnosti obstajajo

Tabela 4: Spisek nevarnosti glede na dostopna omrežja

5. ANALIZA VARNOSTNIH TVEGANJ

5.1 METODOLOGIJA OCENJEVANJA TVEGANJ

V IMS omrežju se pretaka veliko različnih vrst prometa. Med temi je tudi nazaželeni promet, ki ga želimo čim bolj omejiti. Če med seboj logično ločimo omrežja smo »broadcast« promet omejili le na naprave, ki ga morajo obdelovati. Pri uvajanju arhitekture IMS je potrebno logično ločiti omrežja med seboj, glede na funkcionalnost, ki jo opravljajo. V nadaljevanju sledi analiza varnostnih tveganj za vmesnike, ki jih uporabljamo v IMS arhitekturi. Vmesniki se pojavljajo v različnih omrežjih v okviru IMS arhitekture, zaradi tega je potrebno narediti ločeno analizo tveganj za posamezne vmesnike.

Pri izboru metode za ocenjevanje tveganj sem se odločil za kvalitativno metodo predvsem zaradi kompleksnosti uporabe vmesnikov in vloge vmesnikov v IMS arhitekturi. Imamo veliko dejavnikov, ki vplivajo na verjetnost uresničitve škode in posledično tudi kompleksnega izračuna stroškov, ki nastanejo ob uresničitvi.

Pri analizi verjetnosti uresničitve grožnje varnosti sem upošteval vpliv naslednjih kriterijev:

- Tip vmesnika (notranji, zunanji)
- Dostop uporabnikov do vmesnikov
- Medomrežni dostop
- Redundančni vmesniki

Pri analizi pričakovanih stroškov zaradi uresničitve grožnje varnosti sem upošteval vpliv naslednjih kriterijev na direktne stroške:

- Vpliv odpovedi vmesnika na odpoved ostalih vmesnikov,
- Vpliv odpovedi vmesnika na odpoved nedelovanja storitve,
- Vpliv odpovedi vmesnika na odpoved nedelovanja celotne arhitekture,
- Poprečen čas odprave napake (MTTR),
- Ekonomski stroški nastali z odpravo napake
- Ekonomski stroški nastali z uveljavljanjem finančnih kazni zaradi nedelovanja.

Pri analizi stroškov niso upoštevani posredni stroški nastali z izgubo uporabnikov oz. nezadovoljstvom le teh.

5.2 OCENA TVEGANJ ZA VMESNIK CR

Vmesnik Cr se uporablja v notranjih omrežjih, predvsem v omrežju med jedrom IMS-a in aplikacijskimi strežniki različnih domen. Uporabniki do vmesnika Cr nimajo neposrednega dostopa. Pravtako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki Cr niso redundančno vpeti med IMS jedro in aplikacijske strežnike, načeloma pa je aplikacijskih strežnikov v IMS arhitekturi lahko več, zaradi tega je tudi več Cr cmesnikov.

Odpoved Cr vmesnika ne vpliva na odpovedi ostalih vmesnikov in na odpoved celotnega sistema, vpliva pa na odpoved delovanja storitve. Povprečen čas odprave napake je 60 minut. Ekonomski stroški nastali z odpravo napake so zelo majhni. Odpoved Cr vmesnika na uveljavljanje finančnih kazni ne vpliva.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	**3**	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.3 OCENA TVEGANJ ZA VMESNIK CX

Vmesnik Cx se uporablja v notranjih omrežjih za komunikacijo med i-CSCF, s-CSCF in HSS strežniki. Uporabniki do vmesnika Cx nimajo neposrednega dostopa. Pravtako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki Cx niso redundančno vpeti med strežnike, načeloma pa je HSS strežnikov v IMS arhitekturi lahko več, zaradi tega je tudi več Cx cmesnikov.

Odpoved Cx vmesnika ne vpliva na odpovedi ostalih vmesnikov in na odpoved celotnega sistema, vpliva pa na odpoved delovanja storitve. Povprečen čas odprave napake je 60 minut. Ekonomski stroški nastali z odpravo napake so zelo majhni. Odpoved Cx vmesnika na uveljavljanje finančnih kazni vpliva v posameznih primerih.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	**4**	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.4 OCENA TVEGANJ ZA VMESNIK DH

Vmesnik Dh se uporablja v notranjih omrežjih za komunikacijo med aplikacijskimi strežniki in najprimernejšim HSS strežnikom. Uporabniki do vmesnika Dh nimajo neposrednega dostopa. Pravtako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki niso redundančno vpeti med strežnike, načeloma pa je HSS strežnikov v IMS arhitekturi lahko več, zaradi tega je tudi več tudi Dh vmesnikov.

Odpoved Dh vmesnika ne vpliva na odpovedi ostalih vmesnikov in na odpoved celotnega sistema, vpliva pa na odpoved delovanja storitve. Povprečen čas odprave napake je 30 minut. Ekonomski stroški nastali z odpravo napake so razmeroma nizki. Odpoved Dh vmesnika na uveljavljanje finančnih kazni ne vpliva.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi uresničitve grožnje (C)	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	**3**	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.5 OCENA TVEGANJ ZA VMESNIK DX

Vmesnik Dx se uporablja v notranjih omrežjih za komunikacijo med i-CSCF/S-CSCF strežniki in najprimernejšim HSS strežnikom v multi HSS okolju. Uporabniki do vmesnika Dx nimajo neposrednega dostopa. Pravtako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki niso redundančno vpeti med strežnike, načeloma pa je HSS strežnikov v IMS arhitekturi lahko več, zaradi tega je tudi več tudi Dx vmesnikov.

Odpoved Dx vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved celotnega sistema in tudi ne vpliva na odpoved delovanja storitve. Povprečen čas odprave napake je 30 minut. Ekonomski stroški nastali z odpravo napake so razmeroma nizki. Odpoved Dx vmesnika na uveljavljanje finančnih kazni ne vpliva.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi uresničitve grožnje (C)	0	0	1	2	1	2	3	2	3	4
	1	1	**2**	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.6 OCENA TVEGANJ ZA VMESNIK GM

Vmesnik Gm se uporablja na dostopu uporabnikov in njihovih naprav do različnih P-CSCF strežnikov. Vmesnik Gm je zunanji vmesnik. Uporabniki imajo do vmesnika Gm neposreden dostop. Vmesnik se ne uporablja na medomrežnih povezavah. Posamezni vmesniki niso redundančno vpeti v sistem. Vmesniki Gm se med seboj ločujejo glede na vrsto dostopa do P-CSCF strežnika, ki je lahko žični, brezžični, mobilni, širokopasovni, itd...

Odpoved Gm vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved celotnega sistema, zelo močno pa vpliva na odpoved delovanja storitve. Povprečen čas odprave napake je 2 uri. Ekonomski stroški nastali z odpravo napake so visoki. Odpoved Gm vmesnika direktno vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	**7**	8
	5	5	6	7	6	7	8	7	8	9

5.7 OCENA TVEGANJ ZA VMESNIK GO

Vmesnik Go se uporablja v notranjih omrežjih za nadzor nad kvaliteto storitve v upravljalni ravnini in za izmenjavo tarifnih podatkov med IMS in GPRS omrežjem. Uporabniki do vmesnika Dx nimajo dostopa. Vmesnik se uporablja na medomrežnih povezavah med IMS in GPRS omrežji. Vmesniki niso redundančno vpeti.

Odpoved Go vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved celotnega sistema in tudi ne vpliva na odpoved delovanja storitve, ker je namenjen le za nadzor nad delovanjem kvalitete GPRS storitev. Povprečen čas odprave napake je 6 ur. Ekonomski stroški nastali z odpravo napake so srednje visoki. Odpoved Go vmesnika na uveljavljanje finančnih kazni ne vpliva.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	**2**	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7

	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.8 OCENA TVEGANJ ZA VMESNIK GQ

Vmesnik Gq se uporablja v notranjih omrežjih za izmenjavo podatkov o dodeljevanju pravic med različnimi P-CSCF in PDF elementi. Uporabniki do vmesnika Gq nimajo neposrednega dostopa. Pravtako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki niso redundančno vpeti med strežnike, načeloma pa je P-CSCF strežnikov v IMS arhitekturi lahko več, zaradi tega je tudi več tudi Gq vmesnikov med posameznimi P-CSCF strežniki in skupnim PDF strežnikom.

Odpoved Gq vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved celotnega sistema in tudi ne vpliva na odpoved delovanja storitve. Povprečen čas odprave napake je 3 ure. Ekonomski stroški nastali z odpravo napake so razmeroma nizki. Odpoved Gq vmesnika ne vpliva uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	**1**	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.9 OCENA TVEGANJ ZA ISC VMESNIK

Vmesnik ISC se uporablja v notranjih omrežjih med jedrom IMS-a in aplikacijskimi strežniki različnih domen. Uporabniki do vmesnika ISC nimajo neposrednega dostopa. Pravtako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki ISC niso redundančno vpeti med IMS jedro in aplikacijske strežnike, načeloma pa je aplikacijskih strežnikov v IMS arhitekturi lahko več, zaradi tega je tudi več ISC cmesnikov.

Odpoved ISC vmesnika ne vpliva na odpovedi ostalih vmesnikov in na odpoved celotnega sistema, vpliva pa na odpoved delovanja storitve. Povprečen čas odprave napake je 60 minut. Ekonomski stroški nastali z odpravo napake so zelo majhni. Odpoved ISC vmesnika na uveljavljanje finančnih kazni ne vpliva.

Verjetnost uresničitve grožnje (P)	N			S			V		
Stopnja ranljivosti	N	S	V	N	S	V	N	S	V

stroški zaradi (C) uresničitve grožnje										
	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	**3**	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.10 OCENA TVEGANJ ZA VMESNIK MA

Vmesnik Ma se uporablja za direktno usmeritev SIP sporočil javnim uporabniškim identitetam na AS-ih. Uporabniki do vmesnika Ma nimajo neposrednega dostopa. Pravtako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki niso redundančno vpeti med farmo AS strežnikov in i-CSCF strežnikom.

Odpoved Ma vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved celotnega sistema in tudi ne vpliva na odpoved delovanja storitve. Vpliva le na trenutno povpraševanje o dodeljevanju dodatnih storitev vzpostavljenim sejam. Povprečen čas odprave napake je 2 ure. Ekonomski stroški nastali z odpravo napake so razmeroma nizki. Odpoved Gq vmesnika ne vpliva uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	**1**	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.11 OCENA TVEGANJ ZA VMESNIK MG

Vmesnik Mg se uporablja v notranjih omrežjih med i-CSCF elementom in MGCF elementom. MGCF element pretvarja ISUP siganlizacijo v SIP signalizacijo in posreduje SIP sporočila I-CSCF-ju. Uporabniki do vmesnika Mg nimajo neposrednega dostopa. Pravtako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki Mg niso redundančno vpeti v arhitekturo.

Odpoved Mg vmesnika vpliva na odpoved nekaterih ostalih vmesnikov, ne vpliva pa na odpoved celotnega sistema. Velik vpliv ima na odpoved delovanja funkcionalnosti gradje novih sej in podiranja obstoječih sej med različnimi omrežji. Povprečen čas odprave napake je 2 uri.

Ekonomski stroški nastali z odpravo napake so zanemarljivi. Odpoved Mg vmesnika ne vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	**3**	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.12 OCENA TVEGANJ ZA VMESNIK MI

Vmesnik Mi se uporablja v notranjih omrežjih med S-CSCF in BGCF elementom. Uporabniki do vmesnika Mi nimajo neposrednega dostopa. Prav tako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki Mi niso redundančno vpeti v arhitekturo.

Odpoved Mi vmesnika vpliva na odpoved nekaterih ostalih vmesnikov, ne vpliva pa na odpoved storitve in na odpoved celotnega sistema. Povprečen čas odprave napake je 90 minut. Ekonomski stroški nastali z odpravo napake so zanemarljivi. Odpoved Mi vmesnika ne vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	**3**	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.13 OCENA TVEGANJ ZA VMESNIK MJ

Vmesnik Mj se uporablja za izmenjavo sporočil v lastnem notranjem omrežju med BGCF in MGCF. Uporabniki do vmesnika Mj nimajo neposrednega dostopa. Prav tako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki Mj niso redundančno vpeti v arhitekturo.

Odpoved Mj vmesnika vpliva na odpoved nekaterih ostalih vmesnikov, ne vpliva pa na odpoved storitve in na odpoved celotnega sistema. Povprečen čas odprave napake je 60 minut. Ekonomski stroški nastali z odpravo napake so majhni. Odpoved Mj vmesnika ne vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	**0**	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.14 OCENA TVEGANJ ZA VMESNIK MK

Vmesnik Mk se uporablja za izmenjavo sporočil med različnimi BGCF's v različnih IMS omrežjih. Uporabniki do vmesnika Mk nimajo neposrednega dostopa. Vmesnik se uporablja na medomrežnih povezavah. Vmesniki Mk večinoma niso redundančno vpeti v arhitekturo.

Odpoved Mk vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved storitve in na odpoved celotnega sistema. Povprečen čas odprave napake je 4 ure. Ekonomski stroški nastali z odpravo napake so odvisni od pogodb med različnimi operaterji. Odpoved Mk vmesnika vpliva na uveljavljanje finančnih kazni medoperaterskih pogodb.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	**5**	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.15 OCENA TVEGANJ ZA VMESNIK MM

Vmesnik Mm se uporablja za izmenjavo sporočil med i-CSCF in S-CSCF strežniki in zunanjimi IP omrežji. Uporabniki do vmesnika Mm nimajo neposrednega dostopa. Vmesnik se

uporablja na medomrežnih povezavah. Vmesniki Mm večinoma niso redundančno vpeti v arhitekturo.

Odpoved Mm vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved storitve in na odpoved celotnega sistema. Povprečen čas odprave napake je 4 ure. Ekonomski stroški nastali z odpravo napake so odvisni od pogodb med različnimi operaterji. Odpoved Mm vmesnika vpliva na uveljavljanje finančnih kazni medoperaterskih pogodb.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	**6**	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.16 OCENA TVEGANJ ZA VMESNIK MR

Vmesnik Mr se uporablja za izmenjavo sporočil med S-CSCF strežnikom in MRFC elementom v notranjem delu IMS omrežja. Uporabniki do vmesnika Mr nimajo neposrednega dostopa. Vmesniki Mr večinoma niso redundančno vpeti v arhitekturo.

Odpoved Mr vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved storitve in na odpoved celotnega sistema. Povprečen čas odprave napake je 2 uri. Ekonomski stroški nastali z odpravo napake so razmeroma majhni. Odpoved Mr vmesnika ne vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	**0**	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.17 OCENA TVEGANJ ZA VMESNIK MW

Vmesnik Mw se uporablja v notranjih omrežjih med različnimi CSCF strežniki, torej med i-CSCF, P-CSCF in S-CSCF elementi. Uporabniki do vmesnika Mw nimajo neposrednega dostopa. Prav tako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki Mw uporabljajo redundančne poti med strežniki na sejnem nivoju.

Odpoved Mw vmesnika vpliva na odpoved celotnega sistema. Povprečen čas odprave napake je 120 minut. Ekonomski stroški nastali z odpravo napake so visoki. Odpoved Mw vmesnika v vsakem primeru vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	**7**	6	7	8	7	8	9

5.18 OCENA TVEGANJ ZA RF VMESNIK

Vmesnik Rf se uporablja v notranjih omrežjih med različnimi CSCF strežniki in strežniki, ki beležijo dogodke povezane z delovanjem storitev, torej med i-CSCF, P-CSCF, S-CSCF, BGCF, MRFC, MGCF in AS strežniki. Uporabniki do Rf vmesnika nimajo neposrednega dostopa. Prav tako se vmesnik ne uporablja na medomrežnih povezavah. Vmesnik Rf ne uporablja redundančne poti med strežniki na sejnem nivoju.

Odpoved Rf vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved storitve in na odpoved celotnega sistema. Odpoved Rf vmesnika vpliva na zakasnitev nalog beleženja in zaračunavanja storitev. Povprečen čas odprave napake je 3 ure. Ekonomski stroški nastali z odpravo napake so visoki. Odpoved Rf vmesnika ne vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7

	4	**4**	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.19 OCENA TVEGANJ ZA RO VMESNIK

Vmesnik Ro se uporablja v notranjih omrežjih med S-CSCF, MRFC in AS strežniki. Uporabniki do Ro vmesnika nimajo neposrednega dostopa. Prav tako se vmesnik ne uporablja na medomrežnih povezavah. Vmesnik Ro ne uporablja redundančne poti med strežniki na sejnem nivoju.

Odpoved Ro vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved storitve in na odpoved celotnega sistema. Odpoved Ro vmesnika vpliva na zakasnitev beleženja in zaračunavanja storitev. Povprečen čas odprave napake je 3 ure. Ekonomski stroški nastali z odpravo napake so visoki. Odpoved Rf vmesnika ne vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	**4**	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.20 OCENA TVEGANJ ZA RX VMESNIK

Vmesnik Rx se uporablja v notranjih omrežjih med P-CSCF in PCRF strežniki za izmenjavo podatkov o politiki delovanja in podatkov o zaračunavanju. Uporabniki do Rx vmesnika nimajo neposrednega dostopa. Prav tako se vmesnik ne uporablja na medomrežnih povezavah. Vmesnik Rx ne uporablja redundančne poti med strežniki na sejnem nivoju.

Odpoved Rx vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva na odpoved storitve in na odpoved celotnega sistema. Odpoved Rx vmesnika vpliva na izgubo podatkov o zaračunavanju. Povprečen čas odprave napake je 3 ure. Ekonomski stroški nastali z odpravo napake so visoki. Odpoved Rx vmesnika ne vpliva na uveljavljanje finančnih kazni, vpliva pa na znižanje izstavljenih mesečnih računov uporabnikom.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
sni ure (C)	0	0	1	2	1	2	3	2	3	4

	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	**5**	6	7	6	7	8	7	8	9

5.21 OCENA TVEGANJ ZA VMESNIK SH

Vmesnik Sh se uporablja v notranjih omrežjih za komunikacijo med aplikacijskimi strežniki SIP AS, OSA SCS in HSS strežniki. Uporabniki do vmesnika Sh nimajo neposrednega dostopa. Pravtako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki niso redundančno vpeti med strežnike.

Odpoved Sh vmesnika ne vpliva na odpovedi ostalih vmesnikov, na odpovedi delovanja storitev in na odpoved celotnega sistema. Povprečen čas odprave napake je 3 ure. Ekonomski stroški nastali z odpravo napake so srednje visoki. Odpoved Sh vmesnika na uveljavljanje finančnih kazni ne vpliva.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	**2**	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.22 OCENA TVEGANJ ZA VMESNIK SR

Vmesnik Sr se uporablja v notranjih omrežjih. Uporablja ga MRFC za dostop do dokumentov ali drugih podatkov iz AS. Uporabniki do vmesnika Sr nimajo neposrednega dostopa. Prav tako se vmesnik ne uporablja na medomrežnih povezavah. Vmesniki niso redundančno vpeti med strežnike.

Odpoved Sr vmesnika ne vpliva na odpovedi ostalih vmesnikov, na odpovedi delovanja storitev in na odpoved celotnega sistema. Povprečen čas odprave napake je 4 ure. Ekonomski stroški nastali z odpravo napake so srednje visoki. Odpoved Sr vmesnika ne vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	**3**	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

5.23 OCENA TVEGANJ ZA VMESNIK UT

Vmesnik Ut se uporablja na dostopu v IMS omrežje. Uporabniki preko Ut vmesnika dostopajo do spletnih storitev upravljanja in preverjanja nastavitev lastnih storitev. Vmesnik povezuje uporabniške naprave (UE) in sledeče aplikacijske strežnike SIP AS, OSA SCS in IM-SSF. Vmesnik Ut je zunanji vmesnik. Uporabniki imajo preko vmesnika Ut neposreden dostop do strežnikov. Vmesnik se ne uporablja na medomrežnih povezavah. Posamezni vmesniki niso redundančno vpeti v sistem.

Odpoved Ut vmesnika ne vpliva na odpovedi ostalih vmesnikov, ne vpliva tudi na odpoved celotnega sistema, vpliva pa na odpoved upravljanja z storitvijo. Povprečen čas odprave napake je 2 uri. Ekonomski stroški nastali z odpravo napake so nizki. Odpoved Ut vmesnika direktno ne vpliva na uveljavljanje finančnih kazni.

Verjetnost uresničitve grožnje (P)		N			S			V		
Stopnja ranljivosti		N	S	V	N	S	V	N	S	V
stroški zaradi (C) uresničitve grožnje	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	**6**
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

6 ZAKLJUČEK

Analiza ocene tveganj je pokazala pomembnosti posameznih vmesnikov v IMS arhitekturi. V nadaljevanju navajam najpomembnejše rezultate analize. Najpomembnejši dejavnik, ki vpliva na končen rezultat je tip vmesnika, torej ali je vmesnik notranji in neizpostavljen zunanjim zlorabam ali pa je vmesnik zunanji, kjer je izpostavljen vsem našim uporabnikom oz. v določenih primerih celo uporabnikom interneta. Pomemben dejavnik je tudi vpliv na odpovedi delovanja celotnega sistema. Odpoved delovanja posameznega vmesnika oz. posamezne storitve tudi vpliva na sam rezultat vendar nenv tolikšni meri kot odpoved celotnega sistema, ki ima za posledico veliko stroškov zaradi uresničitve groženj. Pomembno vpliva na analizo tudi podatek ali ima vmesnik tudi nalogo, ki je povezana z pravilnim zaračunavanje storitev, ker lahko ob izpadu vmesnika izgubimo podatke o uporabi storitev, lahko pa so podatki tudi napačni. Rezultati analize ocene tveganj so navedeni v tabeli 5.

Vmesnik	Ocena tveganja
Cr	3
Cx	4
Dh	3
Dx	2
Gm	7
Go	2
Gq	1
ISC	3
Ma	1
Mg	3
Mi	3
Mj	0
Mk	5
Mm	6
Mr	0
Mw	7
Rf	4
Ro	4
Rx	5
Sh	2

Sr	3
Ut	6

Tabela 5: Analiza ocene tveganj

Za zmanjšanje tveganja predlagam naslednje ukrepe, ki so tudi ekonomsko upravičeni, saj ne predstavljajo bistveno podražitev IMS arhitekture, prinesejo pa zmanjšanje uresničitve groženj.

Ukrep 1:
Za izboljšanje varnosti predlagam uporabo dodatnih naprav, kot so požarne pregrade in SBC naprave za zaščito pred DoS in DDoS napadi na zunanjih vmesnikih in na vmesnikih za medomrežne povezave. Za detekcijo in preprečevanje napadov na x-CSCF funkcije se lahko uporabijo dodatne naprave kot so IDS ali IPS naprave.

Ukrep 2:
Zaščito vmesnika Ut lahko izboljšamo z ustreno požarno pregrado, vsaj je le ta povezan tudi z javnim internetnim omrežjem. Preko Ut vmesnika je večina prometa s pomočjo http protokola, zaradi tega ne potrebujemo namesnkih SBC elementov ampak nam zadošča že bolj napredna požarna pregrada.

Ukrep 3:
Za vmesnike, ki so povezani z izpadom celotnega sistema bi predlagal redundančno vpetje posameznih vmesnikov med napravami. S tem bi povečali odpornost arhitekture.

Ukrep 4:
Pomembni vmesniki so tudi vmesniki preko katerih se prenašajo podatki o zaračunavanju. Izboljšanje zaščite bi bilo dvojno vpetje elementov in sistema za zaračunavanje.

Predlagani ukrepi so navedeni tudi po prioriteti. Z realizacijo ukrepov pa bi zelo zmanjšali tvaganje uresničitve grožnje.

LITERATURA IN SPLETNE STRANI

Moškon, S. in Brezavšček, A. (2009). Merjenje učinkovitosti sistema za upravljanje informacijske varnosti, 10. slovenski dnevi varstvoslovja, Ljubljana, 4. in 5. junij 2009. - Ljubljana : Fakulteta za varnostne vede. http://www.fvv.uni-mb.si/dv2009/Zbornik/clanki/moskon_brezavscek.pdf

E. Zwicky, S. Cooper, D. Chapman (2006): "Building Internet Firewalls", O'Reilly, 2nd Edition

Defeating Denial of Service Attacks which employ, IP Source Address Spoofing, IETF RFC 2827, maj 2000

Session Initiation Protocol (SIP), IETF RFC 3261, junij 2002

VoIP security, *http://www.voipsa.org*; dostop do vira februar 2010

WiKi enciklopedija, *http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem*; dostop od vira februar 2010

Insecure.org, *http://nmap.org/*; dostop do vira junij 2010

BackTrack Linux community, *http://www.backtrack-linux.org/*; dostop do vira april 2010

SANS, *http://www.sans.org/reading_room/?ref=3701*; dostop do vira junij 2010

Kratice:

AAA	Authentication, Authorisation & Accounting
AKA	Authentication and Key Agreement
AS	Application Server
B2BUA	Back To Back User Agent
BCF	Border Control Function
BG	Border Gateway
BGF	Border Gateway Function
BSF	Border Security Function
CLF	Connectivity Session Location and Repository Function
CK	Ciphering Key
CSCF	Call Session Control Function
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
ETSI	European Telecommunications Standards Institute
FMC	Fixed Mobile Convergence
FW	Firewall
HA	High Availability
HMAC	Hash function based Message Authentication Code
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IETF	Internet Engeniring Task Force
IK	Integrity Key
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IPS	Intrusion Prevention System
IPSec	IP Security Protocol
IPv4, IPv6	Internet Protocol Version 4, Internet Protocol Version 6
LDAP	Lightweight Directory Access Protocol
LI	Lawfull Intercept
MD5	Message Digest No. 5
MGW	Media Gateway
MIP	Mobile IP
MITM	Man In The Middle
MRF	Media Resource Function
MRFC	Media Resource Function Controller
NAPT	Network Address Port Translation
NAT	Network Address Translation
P2P	Peer To Peer
PDF	Policy Decision Function
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment

RTCP	Real-time Transport Control Protocol
RTP	Realtime Transport Protocol
SBC	Session Border Controller
SDP	Session Description Protocol; Service Delivery Platform
SHA1	Secure Hash Algorithm - Version 1.0
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SPDF	Service-based Policy Decision Function
SPIT	Spam over IP Telephony
SRTP	Secure Real-time Transport Protocol
SSO	Single Sign On
TFN	Tribe Flood Network
TFN2K	Tribe Flood Network 2K
TLS	Transport Level Security
UA	User Agent
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
VoIP	Voice over IP