UNIVERZA V LJUBLJANI
FAKULTETA ZA ELEKTROTEHNIKO
KRIPTOGRAFIJA IN RAČUNALNIŠKA VARNOST

# IPsec protokol v VPN omrežjih

SEMINARSKA NALOGA

Ljubljana, junij 2002 Franci Jereb

# KAZALO

# 1 UVOD

Zasebna omrežja so sestavljena iz komunikacijskih naprav, povezav med njimi in končnih sistemov, katerih lastništvo in upravljanje je v domeni ene same organizacije ali podjetja. Posamične lokacije v zasebnih omrežjih so povezane z najetimi ali klicnimi linijami, kar zagotavlja, da je komunikacija vedno zasebna.

Cilj navideznih zasebnih omrežij je uporabniku nuditi enako storitev kot v zasebnih omrežjih, vendar preko skupne infrastrukture ponudnika storitev. To je povezano z večjo izkoriščenostjo omrežja in zato z nižjimi stroški. Navidezna zasebna omrežja morajo izpolnjevati zahteve glede varnosti, zmogljivosti ter kvalitete storitve. Pri tem je treba dati poseben pomen kritičnim aplikacijam, ki se uporabljajo v danem poslovnem okolju.

Med varnostne mehanizme spadajo ločevanje prometa, tuneliranje, enkripcija, avtentikacija in kontrola dostopa.

Na tržišču lahko dobimo mnogo programske opreme, ki varuje komunikacijske povezave oz. aplikacije. Vendar so v teh primerih zaščitene le na aplikativnem nivoju. Ta programska oprema ravno tako uporablja moderne in močne šifrirne algoritme, ki nam zagotavljajo varnost. Tipična primera sta PGP za zaščito elektronske pošte ter SSL za avtentikacijo in šifriranje komunikacijske seje med Web strežnikom in odjemalcem. Te rešitve so sicer zelo učinkovite, vendar so uporabne le za specifične uporabnike in aplikacije.

Rešitev je v zaščiti podatkov že na tretjem ISO-OSI nivoju imenovanem tudi omrežni nivo.

# 2 IP PROTOKOL IN NAVIDEZNA ZASEBNA OMREŽJA

## 2.1 Prednosti IP omrežij

IP protokol je najbolj razširjen komunikacijski protokol v privatnih LAN/WAN omrežjih in je osnovni protokol Internet omrežja. Protokol je nepovezavno orientiran, kar pomeni, da se pred pričetkom prenosa ne vzpostavi povezava »točka-točka«. Zaradi svoje robustnosti je zelo primeren za klasični internet promet, kjer zahteve po kvaliteti storitve niso velike (prenos datotek, svetovni splet, elektronska pošta). Lahko rečemo, da je univerzalni medij modernih komunikacij prav zaradi svoje fleksibilnosti. Njegova moč je predvsem v enostavnem in hitrem usmerjanju paketov. Protokol je prisoten v komunikacijski tehnologiji že nekaj desetletij in prav zaradi svojih lastnosti bo ostal v uporabi še naprej. Dejstvo, ki govori v prid doloročnem obstoju IP protokola je bodoča nadgradnja trenutne različice protokola. Skupina IETF[1] že nekaj let načrtuje tako imenovan IP Next Generation oz. IP ver. 6. Nov tip protokola bo vpeljal 128 bitno naslavljanje in s tem odpravil pomanjkanje IP naslovnega prostora.

## 2.2 Slabosti IP omrežij

Kljub vsem ima protokol tudi nekaj slabih lastnosti, predvsem zaradi zgradbe samega IP paketa. Načrtovalci niso imeli razloga, da bi na IP nivoju zagotovili varnost. Za poslovno uporabo v osnovni obliki ni primeren, saj ima precej pomanjkljivosti v smislu varnosti, zanesljivosti in kvalitete storitev. Predvsem fleksibilnost IP protokola omogoča napadalcem izkoriščanje varnostnih lukenj in nepooblaščeno vdiranje v komunikacijske sisteme. Metoda IP usmerjanja paketov je ranljiva z naslednjimi tipi napadov [L 1]:

- Spoofing – napadalec spremeni svoj izvorni IP naslov in se napadeni napravi predstavi z naslovom, ki mu naprava zaupa.
- Sniffing – napadalec »prisluškuje«, komunikaciji med dvema napravama.
- Session hijacking – napadalec uporabi oba tipa napada in prevzame že vzpostavljeno komunikacijsko sejo med končnima napravama.
- Denial of Service – ta vrsta napada je sestavljena iz več različnih tipov napadov. Eden najbolj znanih je, da napadalec pošilje veliko količino prometa na IP naslov napadene naprave. Napadena naprava pa zaradi premajhnega definiranega obsega predpomnilnikov v programski kodi, ne more obdelati vseh zahtev. Posledica je neodzivanje naprave na določen tip storitve.

## 2.3 VPN omrežja in njihove prednosti

Navidezna zasebna omrežja (VPN[2]) so omrežja, ki so zgrajena na obstoječih javnih komunikacijskih omrežjih. Uporabljajo avtentikacijo in šifriranje podatkov za zagotavljanje varnih povezav. S prihodom novih IP standardov, ki omogočajo vpeljavo novih varnostnih postopkov in z dejstvom, da so IP omrežja povsod na voljo, so navidezna zasebna omrežja zelo močna alternativa obstoječim zasebnim omrežjem, zgrajenih preko najetih vodov in preko komutiranih vodov.

[1] Internet Engineering Task Force
[2] Virtual Private Networks

VPN omrežja imajo vso fleksibilnost obstoječih IP omrežij in poleg tega omogočajo vpeljavo novih funkcionalnosti, zmanjšanje stroškov povezanih s komunikacijsko opremo in seveda povečanje varnosti.

Kot prednosti uporabe VPN omrežij štejemo:

- Zmanjšanje stroškov – podjetje zmanjša stroške na večih področjih: stroške najetih vodov, stroške kupovanja in vzdrževanja opreme za odaljen dostop in stroške, ki izvirajo iz naslova zaposlenih, ki so zadolženi za upravljanje s komukacijsko opremo.
- Hitrejša vpeljava novih storitev – ni potrebno čakati več dni (včasih tednov), da vam ponudnik najetih vodov zagotovi prenosne kapacitete; navidezna zasebna omrežja lahko vpeljemo dejansko v nekaj desetih minutah.
- Varnost – VPN tehnologija zagotavlja uporabo najstrožjih varnostnih meril na osnovi šifriranja podatkov in avtentikacije uporabnikov.
- Razširljivost – VPN omrežja omogočajo podjetjem kakovostno uporabiti komunikacijsko infrastrukturo ponudnika Internetnih storitev. Torej podjetja lahko povečajo zmogljivosti brez velikih vložkov v infrastrukturo.
- Združljivost s širokopasovnimi tehnologijami – VPN tehnologija omogoča mobilnim uporabnikom uporabo širokopasovnih tehnologij, kot so xDSL, kabelski dostop do Interneta, za dostopanje do korporativnega omrežja.
- Zmanjšano izpostavljanje pri spremembi tehnologij – pri vpeljavi novih šifrirnih standardov, podjetje z majhnimi stroški nadgradi funkcionalnost in s tem upraviči vpeljavo VPN omrežij.

## 2.4 Dejavniki varnosti v VPN omrežjih

Za varnen prenos podatkov preko VPN omrežij, morajo biti izpolnjeni osnovni dejavniki varnosti [L 2]:

- Avtentikacija – dostop do VPN omrežja je dovoljen samo avtenticiranim uporabnikom. Poleg avtentikacije pa je mogoče tudi presojanje in obračunavanje (AAA[3]).
- Šifriranje podatkov – podatki, ki so prenašani preko javnih omrežij, morajo biti zaščiteni pred napadi tipa "man-in-the-middle" in nebereljivi za nepoblaščene organizacije in posameznike.
- Upravljanje s ključi – pri uporabi avtentikacije in šifriranja podatkov je neobhodna uporaba učinkovitega protokola za upravljanje s ključi, saj le s tem lahko zagotovimo, da varnost podatkov ni ogrožena.
- Podpora multiprotokolskim omrežjem – VPN omrežje mora transparentno prenašati tudi ostale komunikacijske protokole, ki so uporabljeni v sodobnih omrežjih (IPX/SPX, SNA, NetBEUI, in NetBIOS).

[3] Authentication, Auditing, Accounting

# 3 ARHITEKTURA IPSEC PROTOKOLA

## 3.1 Tunelski protokoli

Idejo o uporabi tunelskih protokolov je že zelo stara in sega nazaj v začetna leta obstoja Internet omrežja. Tako so skozi čas in različne potrebe uporabnikov nastali različni tipi tunelskih protokolov, vsak s svojimi prednostimi in slabostmi. Med najbolj znane tunelske protokole, ki se danes uporabljajo v VPN omrežjih, spadajo:

- Point-to-Point Tunneling Protocol (Microsoft, Ascend, 3Com, ...)
- Layer 2 Forwarding Protocol (Cisco Systems)
- Layer 2 Tunneling Protocol (IETF)
- IPSec Protocol (IETF)

Bistvena razlika med omenjenimi tunelskimi protokoli je ta, da se prvi trije protokoli nahajajo na drugem nivoju ISO-OSI modela (data link layer). IPsec pa je prvi in zaenkrat edini tunelski protokol tretjega nivoja (network layer). V času ko so nastajali tunelski protokoli drugega nivoja, še ni bila dodelana strategija varnega prenosa preko javnih omrežij.

### *3.1.1 Prednosti IPsec protokola pred ostalimi tunelskimi protokoli*

IPsec protokol je sestavljen iz več delov, ki definirajo arhitekturo IPsec protokola, enkripcije, avtentikacije in upravljanja s ključi. Značilnost IPsec tehnologije je varen prenos, ki je zagotovljen z močnim šifriranjem in avtentikacijo.

Poleg tega je IPsec protokol standardiziran, kar omogoča interoperabilnost med različnimi proizvajalci aktivne opreme. IPsec omogoča prenos različnih tipov komunikacijskih protokolov, ki se danes uporabljajo v LAN omrežjih (IPX/SPX, SNA, NetBEUI, in NetBIOS). Drugonivojski protokoli so imeli veliko pomanjkljivost prav zaradi nepodpiranja različnih tipov protokolov [L 3].

Poglavitna prednost IPsec protokola pred ostalimi tipi tunelskih protokolov je v implementaciji močnih varnostnih mehanizmov, ki zagotavljajo varne komunikacije. Ostali tunelski protokoli nimajo implemenitiranih močnih šifrirnih algoritmov za preverjanje avtentikacije, integritete in zaupnosti podatkov. Integriteta podatkov je pri drugonivojskih tunelskih protokolih odvisna le od dolžine in zapletenosti uporabniškega imena in gesla. Prav tako se med samo tunelsko sejo, ki jo vzpostavijo drugonivojski protokoli ne spreminjajo šifrirni ključi, kar za IPsec ne velja. Čas trajanja veljavnosti ključa se lahko pri IPsec protokolu nastavlja glede na čas trajanja povezave oz. na količino prenešenih informacij preko tunela.

Tunelski protokoli drugega ISO-OSI nivoja so sicer še vedno uporabi, vendar jih IPsec zaradi svoje robustnosti in fleksibilnosti počasi, a zagotovo izpodriva.

## 3.2 Gradniki IPsec protokola

IPsec sestavlja skupek večih varnostnih tehnologij za zagotavljanje zaupnosti, integritete podatkov in avtentikacije. IPsec protokol je podrobno definiran v RFC standardih: RFC 2401-2411 in RFC – 2451. IPsec standardi definirajo vpeljavo novih naborov glav, ki so dodani IP datagramom. Te glave paketov so vstavljene za klasično glavo IP datagrama in pred začetkom glave TCP ali UDP datagrama [L 4].

Poznamo dva različna tipa glav:
- Authentication header (AH)
- Encapsulation Security Payload (ESP)

Za varno izmenjavo ključev med končnima entitetama pa skrbi IKE protokol.

Poleg omenjenih osnovnih gradnikov IPsec protokola moram omeniti še Security Association (SA), ki je ključnega pomena za vsak omenjen gradnik.

### *3.2.1 Security Association (SA)*

Ko se vzpostavlja IPsec tunel med dvema končnima entitetama, se entiteti dogovorita za vse tipe algoritmov, ki se bodo uporabljali v času trajanja povezave (tip šifrirnega algoritma, tip integritetnega algoritma, čas veljavnosti ključev). Po končanem dogovarjanju si morata entiteti izmenjati ključe. Za sledenje vseh informacij glede določene IPsec povezave, IPsec protokol uporablja takoimenovan Security Association. SA je odnos med dvema entitetama, ki opisuje katere varnostne algoritme uporabljata za varno komunikacijo. Vsaka SA je unikatno določena z naključno izbranim številom, ki ga imenujemo Security Parameter Index (SPI), in s ciljnim IP naslovom. Preden se paket pošlje preko IPsec tunela, se v Ipsec glavo doda SPI številko. Ciljna naprava sprejme Ipsec paket, prebere SPI številko in ciljni IP naslov, ter glede na svoj vpis v SA bazi sprocesira paket.

### *3.2.2 Internet Key Exchange (IKE)*

Za izmenjavo SA in ključev med končnima entitetama je IETF forum standardiziral protokol imenovan IKE. Protokol vzpostavi avtenticiran varen tunel med entitetama, preko katerega se izvrši izmenjava SA. Z metodo pogajanja uskladita skupen protokol za avtentikacijo [L 5].

IPsec standard podpira naslednje avtentikacijske metode:

- Pre-shared keys – isti ključ (v bistvu je to niz znakov, kot nekakšno geslo) je ob inštalaciji aktivne opreme vpisan v obe napravi. Entiteti avtenticirata ena drugo, tako da opravita zgoščevalno funkcijo nad podatki, kateri vsebujejo "Pre-shared key". Če lahko sprejemna entiteta neodvisno kreira isti rezultat s pomočjo zgoščevalne funkcije in "Pre-shared key"-ja potem imata napravi isto "Pre-shared key" in se avtenticirata.
- Šifriranje z javnimi ključi – obe entiteti generirata pseudo-naključno število in ga zašifrirata z javnim ključem nasprotne entitete. Če je entiteta sposobna dešifrirati prispele podatke s svojim privatnim ključem in je psevdo-naključno število isto, potem se entiteti avtenticirata.

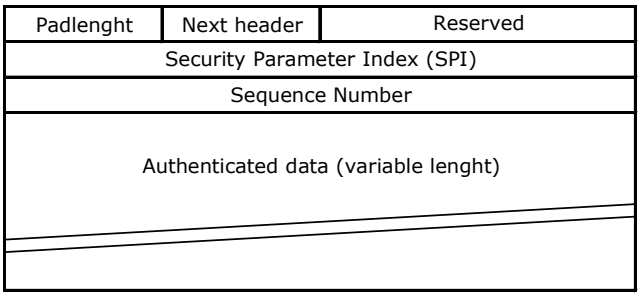
- Digitalni podpisi – vsaka entiteta digitalno podpiše niz podatkov in jih pošlje nasprotni entiteti. V bistvu je metoda zelo podobna prejšnji.

Trenutno sta v IPsec standardu implementirani tako RSA šifriranje z javnimi ključi, kot tudi Digital Signature Standard (DSS).

Po opravljeni avtentikaciji se vzpostavi varen IKE tunel in izmenjata se SA. Na osnovi izmenjanih SA-jev, pa se nato vzpostavi Ipsec tunel, preko katerega se varno pošilja uporabniške podatke.

### *3.2.3 Authentication header (AH)*

IP Authentication Header (AH) je uporabljen za zagotavljanje integritete podatkov in avtentičnosti pošiljatelja. IPsec AH zagotavlja avtentičnost tako koristnih podatkov (podatkov, ki izvirajo iz višjih ISO-OSI nivojev), kot tudi za same glavo IP datagrama. Treba je poudariti, da AH ne varuje vseh polj IP glave datagrama, ker se nekatere vrednosti polj spreminjajo po komunikacijski poti. Sama koristna vsebina ni šifrirana, zato se sam AH načeloma uporablja samo v primerih, ko ne rabimo šifriranja. Uporabimo ga takrat ko želimo biti prepričani, da se nam IP glava na prenosni poti ni spremenila [L 6].




Slika 1: Struktura AH paketa

Sestavni deli AH paketa:

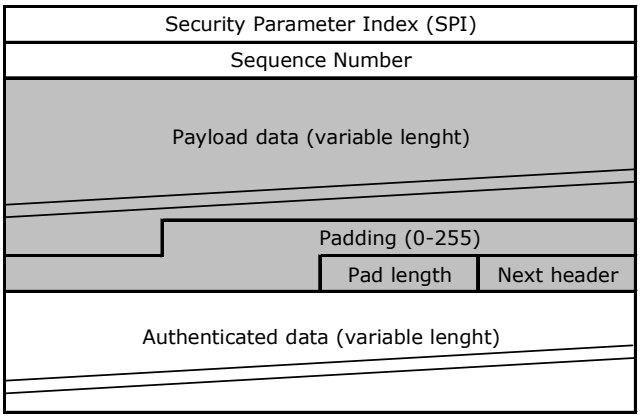
- Polje Next header pove kateri višje nivojski protokol sledi AH glavi (lahko je ESP ali TCP).
- Polje Reserved je rezervirano za prihodnost.
- Polje SPI opisuje nabor varnostnih parametrov.
- Polje Sequence Number, se povečuje z vsakim poslanim paketom za določen SA.
- Polje Authenticated Data vsebuje rezultat zgoščevalne funkcije oz. lahko mu rečemo tudi digitalni podpis.

AH uporablja dva tipa zgoščevalnih funkcij in sicer SHA-1 in MD5.

AH je lahko uporabljen tudi kot samostojna funkcionalnost ali pa skupaj z ESP glavo.

### *3.2.4 Encapsulation Security Payload (ESP)*

IPsec protokol opravlja šifriranje podatkov na paketnem nivoju. Protokol za šifriranje se imenuje ESP in podpira simetričen tip šifriranja. Standard za ESP je 56 bitno DES šifriranje, ki je nadgrajen na 3DES z 168 bitnim ključem. Načeloma se lahko uporabi vsakršen šifrirni algoritem v ESP paketu, le da je simetričen. Vendar sam IPsec standard predpisuje uporabo DES-CBC načina. Z izbiro DES-CBC načina delovanja je zagotovljena interoperabilnost med različnimi proizvajalci opreme [L 7].




Slika 2: Struktura ESP paketa (siva barva - šifrirano)

Sestavni deli ESP paketa:

- Polje SPI opisuje nabor varnostnih parametrov.
- Polje Sequence Number, se povečuje z vsakim poslanim paketom za določen SA.
- Polje Payload Data vsebuje šifrirano prenašano koristno vsebino.
- Polje Padding uporabljajo nekateri šifrirni algoritmi za navidezno povečanje prenešene koristene vsebine, s tem se potencialne napadalce zavede o resnični uporabni količini informacij.
- Polje Padlenght pove razmerje med navidezno in pravo velikostjo koristne vsebine.
- Next header pove kateri višjenivojski protokol sledi ESP glavi (ponavadi TCP oz. UDP).
- Polje Authenticated Data vsebuje rezultat zgoščevalne funkcije oz. lahko mu rečemo tudi digitalni podpis.

Kot vidimo tako AH kot ESP protokol omogočata overjanje paketov. Razlog, da se funkcionalnosti prekrivata izvira iz časov, ko je bila uvedena izvozna omejitev na šifrirne algoritme. Medtem, ko za algoritme za overjanje te omejitve niso veljale.

## 3.3 Transportni in tunelski način IPsec tunela

Obstojata dva načina delovanja in sicer transportni in tunelski način. Transportni način se uporablja za zaščito protokolov višjih nivojev oziroma aplikacij. V transportnem načinu se šifrirajo samo podatki, ne pa glava IP paketa. Transportni način se uporablja pri komunikaciji dveh gostiteljev (klientov).

Pri komunikaciji dveh IPsec komunikacijskih naprav pa se uporablja tunelski način. Na IPsec VPN napravo se priključi LAN segment, kjer se lahko uporabljajo zasebne IP številke. Pri uporabi ESP VPN naprava celotni IP paket, ki ga dobi iz LAN omrežja, zašifrira in vključi v ESP paket, ki mu doda novo IP glavo. V novi IP glavi je vpisan njegov javni IP naslov. Ciljni IP naslov postaje v oddaljenem LAN omrežju pa zamenja z javnim IP naslovom oddaljene VPN naprave. Obe VPN napravi vsebujeta usmerjevalne tabele, na osnovi katerih usmerita IP datagram na ciljni naslov v LAN omrežju.

# 4 ZAGOTAVLJANJE VARNOSTI V IPSEC PROTOKOLU

Varnost v IPsec VPN omrežju se zagotavlja na osnovi močnih šifrirnih in avtentikacijskih algoritmov. IPsec protokol uporablja naslednje varnostne algoritme:

- Zgoščevalne funkcije za zagotavljanje avtentikacije.
- Šifrirne algoritme za šifriranje podatkov.
- Uporaba digitalnih certifikatov za avtenticiranje uporabnikov.

## 4.1 Zgoščevalne funkcije

Zgoščevalne funkcije preslikajo poljubno dolg niz znakov v blok konstantne dolžine, ki je kot nekakšen prstni odtis oziroma povzetek vhodnega niza. Od zgostitvenega algoritma pričakujemo:

- Nemogoče je najti dve različni sporočili, ki bi ju preslikal v isti blok.
- Isto sporočilo vedno preslika v enak blok.
- Iz zgostitvenega bloka ni mogoče restavrirati sporočila (od tu ime one-way hash function).
- Vsaka sprememba v sporočilu povzroči spremembo zgostitvenega bloka.

### *4.1.1 Message Digest - MD5*

Sporočilu v binarni obliki doda toliko bitov, da je skupno število deljivo s 512 in sicer je zadnjih 64 bitov rezerviranih za zapis dolžine sporočila. Prostor med koncem sporočila in temi 64 biti pa napolni tako, da najprej doda 1, potem pa same 0. Potem zaporedoma obdeluje bloke po 512 bitov. Blok razdeli na 16 besed po 32 bitov, ki jih obdeluje v štirih 32-bitnih registrih. Postopek ima štiri različne zanke. Povzetek je tisto, kar na koncu dobimo v registrih, torej je dolg 128 bitov [L 8].

### *4.1.2 Secure Hash Algorithm - SHA-1*

Razvili sta ga organizaciji NIST in NSA. Ravno tako kot MD5 obdeluje bloke po 512 bitov. Obdeluje jih v petih registrih po 32 bitov, kar da 160-bitni rezultat. Zenkrat velja za najboljši zgostitveni algoritem, čeprav je bolj počasen kot MD5 [L 9].

## 4.2 Šifrirni algoritmi

### *4.2.1 DES*

Šifrirajo se 64 bitov dolgi bloki z uporabo 56 bitov dolgega ključa, uporablja transpozicije in substitucije. 64 bitov na začetku permutiramo, potem jih preuredimo s pomočjo posebnih tabel (S-boxes) in ključa. Ta del postopka se 16-krat ponovi - vsakokrat z drugače preurejenim ključem. Algoritem učinkuje tako, da sprememba enega samega vhodnega bita bloka spremeni skoraj vse bite v rezultatu bloka. Dešifriramo z istim ključem in skoraj enakim postopkom [L 10].

### *4.2.2 3DES*

Ker je DES šifriranje precej enostavno za razbijanje, sedaj priporočajo trojno enkripcijo z DES na takle način: zašifriramo s ključem 1, dešifriramo s ključem 2, zašifriramo s ključem 3. Pri dešifriranju gremo po istih stopinjah v obratnem redu: dešifriramo s ključem 3, šifriramo s ključem 2 in dešifriramo s ključem 1. Ocenjujejo, da je tako uporabljen algoritem tako varen, kot da bi imel 112 bitov dolg ključ. Kot že omenjeno se uporablja DES-CBC tip simetričnega šifriranja [L 10].

## 4.3 Digitalni certifikat

Digitalni certifikat je digitalni dokument, ki potrjuje povezavo med javnim ključem in osebo oz. strežnikom. Z njim lahko preverimo, komu pripada javni ključ. Potrdilo vsebuje javni ključ in informacijo o njegovem imetniku, ki ju podpiše oseba ali institucija, ki ji zaupamo. Središčni del predstavlja overitelj javnih ključev (Certification Authority -CA). Vsak overitelj objavi svoj javni ključ in dokument (Certification Policy), ki opisuje postopek, kako in komu podeljuje potrdila ter na kakšen način varuje svoj zasebni ključ.

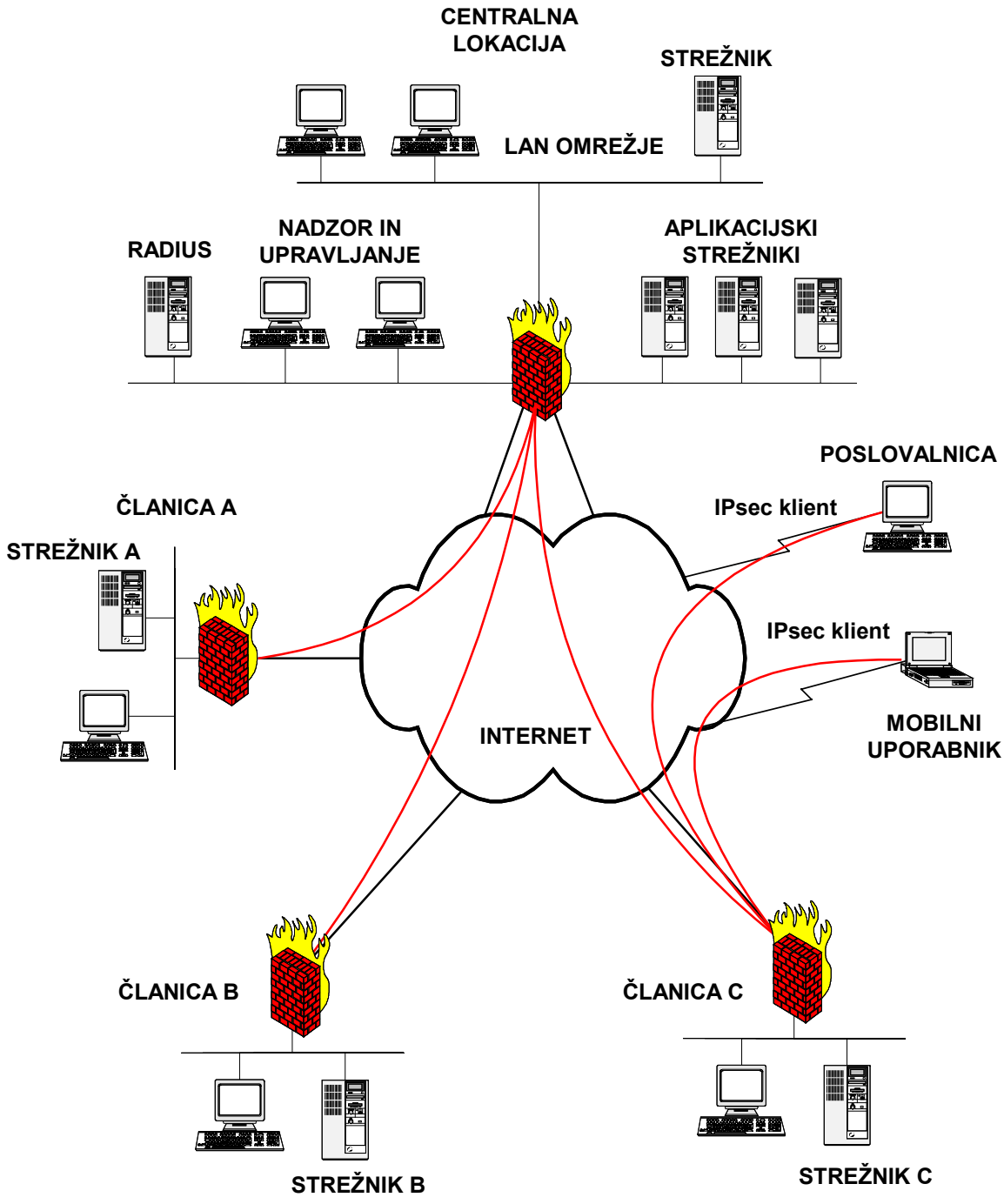
IPsec standard podpira uporabo digitalnih certifikatov za preverjanje avtentičnosti uporabnika. Proizvajalci programske opreme PKI, ki imajo omogočeno podporo IPsec standardu so: Verisign, Entrust, Thawte.

# 5 IMPLEMENTACIJA VPN - IPSEC OMREŽJA

V nadaljevanju bom predstavil pilotski projekt VPN omrežja podjetja Iskra Holding d.d. Holding kot krovna družba združuje 20 podjetij, ki jih vežejo podobni poslovni interesi. Vodstvo holdinga se je odločilo za postavitev lastnega IPsec VPN omrežja. Z vpeljavo novih tehnologij bodo lažje sledili spremembam, do katerih prihaja na globalnem trgu. Poleg tega pa bodo zmanjšali operativne fiksne stroške in povečali produktivnost zaposlenih.

Vsaka izmed članic holdinga bo na svoji lokaciji imela postavljeno aktivno opremo Lucent Brick. Oprema bo služila obenem kot požarni zid, ki varuje LAN omrežja članic, in kot VPN stikalo. Na centralni lokaciji bo postavljen nadzor in upravljanje VPN omrežja, kjer bo omogočen nadzor in po potrebi spreminjanje varnostne politike oddaljenih lokacij. Na varovanem delu omrežja na centralni lokaciji bodo postavljeni centralni aplikacijski strežniki, na katerih bodo tekle

skupne aplikacije holdinga. V RADIUS strežniku bodo vpisana uporabniška imena mobilnih uporabnikov in uporabnikov, ki bodo uporabljali klicni dostop do VPN omrežja.




Slika 3: Pilotno IPsec VPN omrežje

Zaradi zagotavljanje varnosti in redundance bo centralna lokacija imela dostop do Interneta preko dveh ponudnikov Interneta, članice pa preko enega. Med lokacijami bodo vzpostavljeni VPN tuneli do centralne lokacije z zvezdasto topologijo, to se pravi, da bo vsaka izmed članic imela VPN tunel le proti

centralni lokaciji. Ker imajo nekatere izmed članic veliko število majhnih poslovalnic in trgovskih potnikov, bo omogočen tudi njim dostop do korporativnega omrežja preko komutiranih linij. Ti uporabniki bodo najprej vzpostavili klicno povezavo do Interneta preko lokalnega ponudnika Interneta, nato pa preko IPsec programske opreme, inštalirane na njihovem osebnem računalniku, vzpostavili IPsec tunel do njihovega matičnega podjetja. Tako bodo lahko dostopali do strežnika v matičnem podjetju. Če pa bodo želeli dostopati do aplikacijskih strežnikov na centralni lokaciji, bo VPN stikalo preusmerilo njihove pakete po Ipsec tunelu proti centralni lokaciji.

Na vseh lokacijah se bo uporabila tako imenovana »split tunneling« metoda, tako da se bo šifriral samo promet namenjem proti aplikacijskim strežnikom na centralni lokaciji. S tem se omogočilo posameznim članicam hitrejši in kvalitetnejši dostop do Interneta, centralne lokacije pa ne bodo obremenjevale s svojim prometom namenjenim na Internet.

# 6 ZAKLJUČEK

Glede na samo implementacijo IPsec protokola, njegovo veliko skalabilnost in popularnost se bo standard obdržal kot varen in zanesljiv komunikacijski protokol tudi v prihodnosti. Večjih sprememb v sami osnovni zgradbi protokola ni pričakovati, seveda pa je zaradi svoje modularne zgradbe pripravljen za nadgradnjo z novimi varnostnimi algoritmi. Arhitekti IETF IPsec foruma že pripravljajo standard za nadgradnjo z novimi šifrirnim in avtentikacijskimi algoritmi. Kot opisujejo na svoji internetni strani bo v prihodnje IPsec standard podpiral naslednje algoritme AES-CBC, AES-MAC, SHA-2 in hitri AES način za strojne šifrirne naprave [L 11]. Proizvajalci aktivne opreme so se obvezali, da bodo po objavljenih standardih implementirali nove algoritme in tako omogočili svojim kupcem nove varnostne rešitve.

# 7 LITERATURA

[L 1] IPsec - white paper, www.cisco.com, 2000

[L 2] T. Fortenberry - Windows 2000 Virtual Private Networking, New Riders, 2001

[L 3] Understanding the IPsec Protocol Suite, www.alcatel.com, 2000

[L 4] Security Architecture for the Internet Protocol, RFC 2401, www.rfc-editor.org

[L 5] The Internet Key Exchange (IKE), RFC 2409, www.rfc-editor.org

[L 6] IP Authentication Header, RFC 2402, www.rfc-editor.org

[L 7] IP Encapsulating Security Payload (ESP), RFC 2406, www.rfc-editor.org

[L 8] The MD5 Message-Digest Algorithm, RFC 1321, www.rfc-editor.org

[L 9] Secure Hash Standard, http://csrc.nist.gov/encryption/tkhash.html

[L 10] Encryption, http://csrc.nist.gov/encryption/tkencryption.html

[L 11] IP Security Protocol, http://www.ietf.org/html.charters/ipsec-charter.html