HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

IPSec

CCERT-PUBDOC-2004-01-58

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. Uvod

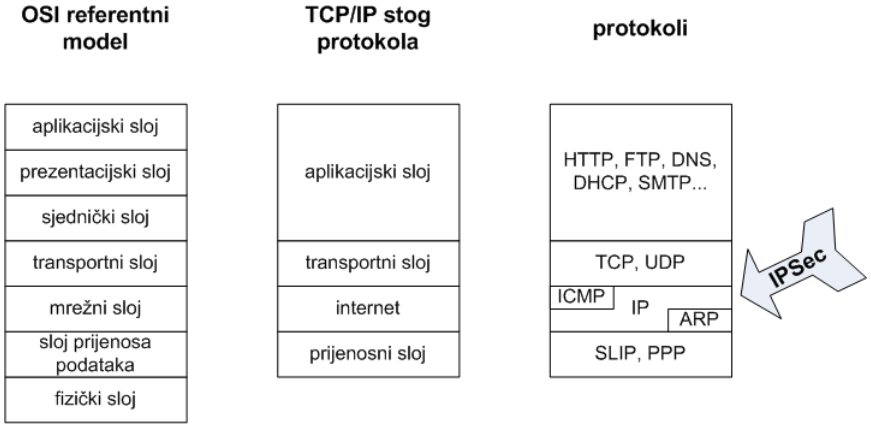
TCP/IP je skup protokola koji je *de facto* prihvaćen kao standard za mrežnu komunikaciju u većini današnjih računalnih mreža. Internet, kao "mreža svih mreža", također koristi TCP/IP stog protokola.
Trenutno se TCP/IP stog protokola bazira na IPv4 (IP protokol inačice 4) protokolu, iako već dulje vrijeme postoji i IPv6 (IP protokol inačice 6), koji bi trebao ispraviti neke inherentne nedostatke u IP protokolu i unaprijediti mrežnu komunikaciju.
Jedan od osnovnih nedostataka TCP/IP stoga protokola u svom izvornom obliku jest nepostojanje nikakvih mehanizama kojima bi se osigurala zaštita i integritet podataka u prijenosu i izvršila autentikacija strana u komunikaciji.
Ovaj dokument bavi se IPSec-om (eng. *IP Security*), skupom proširenja IPv4 protokola kojim se osiguravaju osnovni sigurnosni aspekti mrežne komunikacije, a to su:

- tajnost,
- integritet,
- autentikacija i
- neporecivost.

S tim da valja napomenuti da IPSec, osim što proširuje IPv4 koji se trenutno koristi, dolazi i kao integralni dio IPv6 protokola.
Obzirom da se integrira s IP protokolom, IPSec implementira sigurnu mrežnu komunikaciju na trećem, odnosno mrežnom sloju (eng. *network layer*) ISO OSI stoga protokola, tj. u internet sloju, ukoliko se promatra TCP/IP stog (Slika 1). Naravno, sigurnost je moguće implementirati i u drugim slojevima, od fizičkog do aplikacijskog sloja (SSH, SSL/TLS). Svaka od implementacija ima svoje prednosti i nedostatke, no detaljnija usporedba izlazi iz okvira ovog dokumenta.

2. Položaj IPSec-a unutar stoga protokola

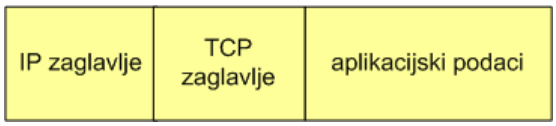
Kako je već spomenuto, IPSec funkcionira unutar mrežnog sloja te osigurava tajnost, integritet, autentikaciju i neporecivost. Pošto IP protokol osigurava uslugu komunikacijskog kanala od kraja do kraja (eng. *end-to-end*), zaštita kanala na istoj razini korištenjem IPSec-a omogućava mu neovisnost obzirom na niže slojeve. To znači da komunikacijski uređaji na putu između dvaju entiteta ne moraju podržavati IPSec, što omogućava korištenje IPSec-a bez obzira na način implementacije fizičkog sloja (eng. *physical layer*) i sloja prijenosa podataka (eng. *data link layer*).
S druge strane, ukoliko dva krajnja entiteta podržavaju IPSec, njegova uporaba je transparentna obzirom na više slojeve protokolnog stoga. Aplikacije mogu koristiti sigurnu komunikaciju koju pruža IPSec, bez obzira na vlastitu funkcionalnost. Isto se odnosi i na protokole koji su implementirani u transportnom sloju (eng. *transport layer*), što znači da svi podaci koji se prenose korištenjem TCP i UDP protokola, isto kao i ICMP poruke, mogu koristiti sigurni komunikacijski kanal koji pruža IPSec.



Slika 1:*Položaj IPSec-a u odnosu na TCP/IP stog protokola, odnosno OSI referentni model*

3. IPSec protokoli

IPSec se implementira korištenjem dvaju međusobno neovisnih protokola koji osiguravaju različite aspekte sigurnosti. AH (eng. *authentication header*) osigurava integritet, autentikaciju i neporecivost, dok ESP (eng. *encapsulated security payload*) osim toga može osigurati i tajnost podataka koji se prenose. Oba protokola, AH i ESP, modificiraju standardni oblik IP datagrama (Slika 2). U nastavku poglavlja biti će detaljno opisana oba protokola i njihova funkcionalnost.

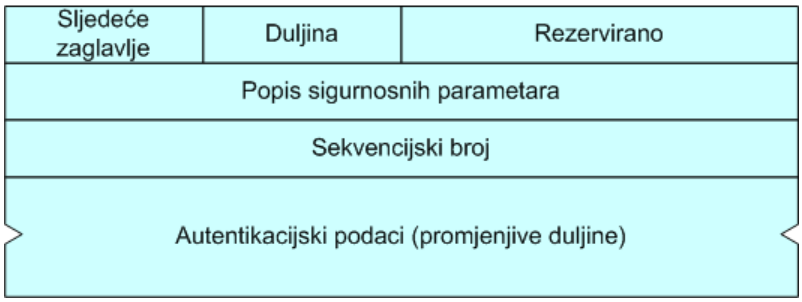


Slika 2: *Standardni oblik IP datagrama*

3.1. AH

AH protokol (IP protokol 51) definiran je u RFC 2402 dokumentu i osigurava autentikaciju, integritet i neporecivost IP datagrama, ali ne može osigurati i tajnost. Protokolom je definirano vlastito (AH) zaglavlje koje se umeće između IP zaglavlja i IP podataka koji slijede (Slika 5). Specifičnost AH jest u tome što on, za razliku od ostalih protokola TCP/IP stoga, ne enkapsulira podatke protokola kojima pruža uslugu.

Slika 3 prikazuje AH zaglavlje, zajedno s pripadajućim poljima. Sva prikazana polja su obvezna, odnosno uvijek su prisutna u AH zaglavlju. U nastavku su opisane njihove funkcije.



Slika 3: *AH zaglavlje*

Sljedeće zaglavlje (eng. *next header*) – Sljedeće zaglavlje je 8-bitno polje koje identificira tip podataka koji slijedi nakon AH zaglavlja. Polje može poprimiti vrijednost iz definiranog skupa brojeva koji označavaju IP protokole (npr. 6 – TCP, 17 – UDP, 51 – ESP). U dokumentu RFC 3232, odnosno *online* bazi podataka (http://www.iana.org), dan je trenutno važeći skup brojeva, odnosno protokola.

Duljina (eng. *payload length*) – Duljina je polje koje specificira duljinu AH zaglavlja. Duljina se računa kao duljina u 32-bitnim riječima umanjena za vrijednost 2.

Rezervirano (eng. *reserverd*) – Ovo polje duljine 16 bita je rezervirano za buduće potrebe. Ono mora biti postavljeno na vrijednost "0".

Popis sigurnosnih parametara (eng. *security parameters index*) – Ovo polje duljine 32 bita sadrži proizvoljnu vrijednost, koja uz IP adresu i sigurnosni protokol (u ovom slučaju AH) definira jedinstveni skup sigurnosnih parametara (eng. *security association – SA*) koji se koristi u sigurnoj komunikaciji između dvaju entiteta. SA skup sigurnosnih parametara definira se prilikom uspostave IPSec spoja. Vrijednosti od 1 do 255 rezervirane su od IANA-e za buduću uporabu.

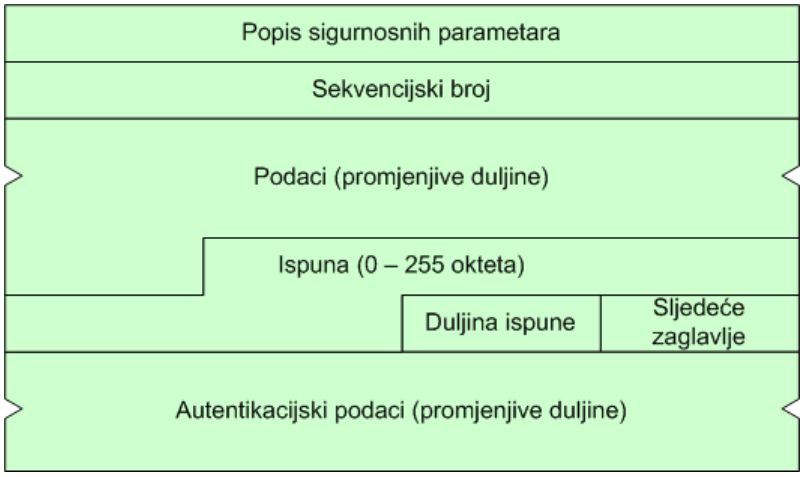
Sekvencijski broj (eng. *sequence number*) – Ovo polje duljine 32 bita služi za osiguranje od napada ponavljanjem paketa, a povećava se prilikom svakog slanja paketa koji ima identični SA skup sigurnosnih parametara. Pošiljatelj mora nužno generirati ovo polje, dok ga primatelj može ili ne mora interpretirati. Prilikom inicijacije komunikacije ovo polje se postavlja na vrijednost "1".

Autentikacijski podaci (eng. *authentication data*) – Polje koje sadrži autentikacijske podatke je varijabilne duljine. U njemu je sadržana ICV (eng. *integrity check value*) vrijednost na temelju koje se provjerava integritet i autentičnost poruke. Duljina polja za autentikacijske podatke mora biti cjelobrojni višekratnih 32-bitne riječi. Ukoliko polje samo po sebi ne ispunjava taj uvjet, dodaje se (proizvoljna) ispuna kojom se nadopunjava odgovarajući broj bitova.

Vrijednost ICV-a se računa na temelju svih polja IP zaglavlja koja se ne mijenjaju prilikom prijenosa, čitavog AH zaglavlja (koje je za tu potrebu postavljeno na vrijednost "0"), te svih podataka protokola višeg sloja. Algoritam koji se upotrebljava za računanje ICV-a, koji može biti autentikacijski kod poruke (eng. *message authentication code*) izračunat korištenjem simetričnih algoritama za šifriranje (npr. DES) ili rezultat *hash* funkcija (npr. MD5 ili SHA-1), definira se prilikom uspostave komunikacije i dio je SA skupa sigurnosnih parametara.

3.2. ESP

ESP protokol (IP protokol 50) definiran je u RFC 2406 dokumentu, a može osigurati autentikaciju, integritet, neporecivost i tajnost podataka. Protokol također definira vlastito zaglavlje koje se umeće iza IP zaglavlja, te enkapsulira sve podatke protokola višeg sloja, dodajući pri tom završni slog u kojem mogu biti sadržani autentikacijski podaci. Slika 4 prikazuje ESP datagram zajedno s pripadajućim poljima. U nastavku su opisane funkcije tih polja.



Slika 4: *ESP datagram*

Popis sigurnosnih parametara (eng. *security parameters index*) – Popis sigurnosnih parametara je 32-bitno polje u kojem se, isto kao i kod AH, definira jedinstveni SA skup sigurnosnih parametara (određen prilikom uspostave komunikacije) koji se koristi u komunikaciji između dvaju entiteta. Kao i kod AH, vrijednosti od 1 do 255 su rezervirane za buduću uporabu.

Sekvencijski broj (eng. *sequence number*) – Ovo polje duljine 32 bita, isto kao i kod AH, služi za osiguranje od napada ponavljanjem paketa, a povećava se prilikom svakog slanja paketa koji ima identični SA skup sigurnosnih parametara. Pošiljatelj mora nužno generirati ovo polje, dok ga primatelj može ili ne mora interpretirati. Prilikom inicijacije komunikacije ovo polje se postavlja na vrijednost "0", za razliku od AH gdje je inicijalna vrijednost tog polja "1".

Podaci i ispuna (eng. *payload data*) – Ovo polje proizvoljne duljine sadrži podatkovni dio IP paketa i ispunu. Vrsta podataka koja se nalazi u podatkovnom dijelu definirana je poljem "sljedeće zaglavlje". Osim samih podataka, u tom polju mogu biti i eksplicitno sadržani podaci koji su nužni za kriptografsku sinkronizaciju (npr. inicijalizacijski vektor – IV), ukoliko to kriptografski algoritam koji se koristi zahtijeva (npr. DES u CBC načinu rada). Ovisno o načinima rada kriptografskih protokola koji koriste IV inicijalizacijskih vektor, on može biti sadržan na samom početku šifriranog bloka podataka ili zasebno od šifriranih podataka, što ovisi o konkretnim implementacijama algoritama.

Ispuna se koristi iz dva razloga:

- neki kriptografski algoritmi za šifriranje koriste blokove fiksne duljine, te je podatkovni dio paketa potrebno dopuniti do odgovarajuće duljine,
- zbog implementacijskih razloga nužno je da duljina podataka ispune, te dva sljedeća polja ("duljina ispune" i "sljedeće zaglavlje") zajedno daju cjelobrojni višekratnik 32-bitne riječi, odnosno da je ta duljina poravnata na 4-okteta.

Duljina ispune (eng. *payload length*) – Ovo 8-bitno polje definira duljinu prethodno korištene ispune u oktetima. Dozvoljene vrijednosti su od 0 do 255, s time da vrijednost 0 označava da ispuna ne postoji.

Sljedeće zaglavlje (eng. *next header*) – Sljedeće zaglavlje, ponovno kao i kod AH, je 8-bitno polje koje identificira tip podataka koji slijedi nakon ESP zaglavlja. Polje može poprimiti vrijednost iz definiranog skupa brojeva koji označavaju IP protokole.
Autentikacijski podaci (eng. *authentication data*) – Ovo polje proizvoljne duljine nije obvezno, a koristi se samo u slučaju da je u SA skupu sigurnosnih parametara specificirana usluga autentikacije. U tom slučaju ovo polje sadrži ICV koji se računa za cijeli ESP datagram (ESP zaglavlje, podatkovni dio i ispuna), ne uključujući pri tom samo polje namijenjeno autentikacijskim podacima, a njegova duljina ovisi o autentikacijskom algoritmu koji se koristi.

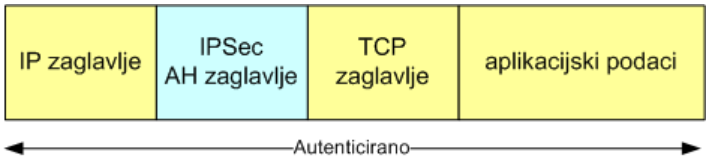
4. Načini rada

IPSec definira dva osnovna načina rada. To su transportni način rada te tuneliranje. Oba protokola, AH i ESP, mogu se koristiti u transportnom načinu rada ili za tuneliranje. Također, moguće je, u slučaju potrebe za dodatnim podizanjem razine sigurnosti, koristiti i kombinaciju oba protokola.
U nastavku poglavlja biti će opisana oba načina rada, te mogućnosti korištenja AH i ESP protokola.

4.1. Transportni način rada

Transportni način rada namijenjen je prvenstveno za uspostavu sigurne komunikacije između entiteta, odnosno tzv. *host-to-host* komunikacije u privatnim LAN ili WAN računalnim mrežama. Za transportni način rada nužno je da obje krajnje točke (izvor i odredište) podržavaju IPSec. Korištenjem AH i ESP protokola moguće je postići različite aspekte sigurne komunikacije.

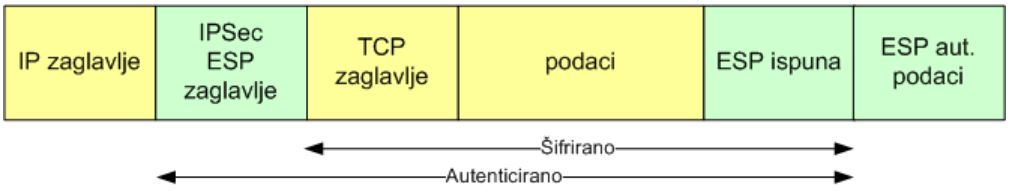
AH – Ukoliko se u transportnom načinu rada koristi AH protokol, moguće je osigurati integritet, autentikaciju i neporecivost, a AH zaglavlje se dodaje odmah iza IP zaglavlja (Slika 5). U tom slučaju polje *protokol* u IP zaglavlju sadrži vrijednost 51 (AH), dok polje *sljedeće zaglavlje* u AH zaglavlju sadrži vrijednost koja odgovara enkapsuliranom datagramu iz višeg sloja (npr. 6 za TCP datagram).



Slika 5: *AH u transportnom načinu rada*

Kako se iz slike može vidjeti, AH u transportnom načinu rada provodi autentikaciju, te osigurava integritet i neporecivost čitavog IP datagrama.

ESP – U transportnom načinu rada ESP osigurava integritet, autentikaciju, neporecivost i tajnost podataka koji se prenose. Ukoliko se za IPSec koristi ESP, polje *protokol* u IP zaglavlju sadržavat će vrijednost 50 (ESP), a polje *sljedeće zaglavlje* u ESP zaglavlju sadržat će vrijednost koja odgovara enkapsuliranim podacima iz višeg sloja, isto kao i kod AH. Iza enkapsuliranih podataka ESP također dodaje ispunu, te opcionalno (ukoliko je u SA skupu sigurnosnih parametara specificirana i autentikacija) polje *autentikacijski podaci*. Slika 6 Prikazuje ESP u transportnom načinu rada.

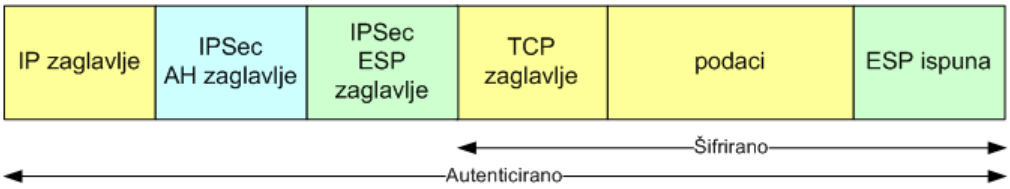


Slika 6: *ESP u transportnom načinu rada*

Kako se iz slike može vidjeti, svi podaci višeg sloja, zajedno s ESP ispunom, su šifrirani. Također je uočljivo da, za razliku o AH koji autenticira čitav IP datagram, uključujući i IP zaglavlje, ESP autenticira vlastito zaglavlje i podatkovni dio datagrama, čime je teoretski ostavljena mogućnost neovlaštene modifikacije IP zaglavlja.

ESP + AH – Iz prethodnih razmatranja vidljivo je da AH osigurava integritet, autentikaciju i neporecivost čitavog IP datagrama. Istovremeno, ESP može osigurati tajnost podatkovnog dijela datagrama, te opcionalno integritet, autentikaciju i neporecivost za taj dio datagrama (uključujući i ESP zaglavlje) ali ne i za pripadajuće IP zaglavlje. Ukoliko se želi postići maksimalna razina zaštite, odnosno osigurati tajnost podataka i autentikacija, integritet i neporecivost čitavog IP datagrama, moguće je koristiti ESP i AH zajedno. U tom slučaju polje *protokol* u IP zaglavlju sadržat će vrijednost 51 (AH), nakon toga slijedit će AH zaglavlje, čije će polje *sljedeće zaglavlje* sadržati vrijednost 50 (ESP), nakon kojeg će slijediti ESP zaglavlje u čijem će polju *sljedeće zaglavlje* biti sadržana vrijednost koja će označavati protokol višeg sloja čiji podaci su enkapsulirani u tako formiranom datagramu. Slika 7 prikazuje IPSec u transportnom načinu rada ukoliko se istovremeno koriste ESP i AH.

Ovdje valja napomenuti da se prvo formira ESP dio paketa, odnosno šifrira se datagram transportnog sloja, te se formira pripadajuće ESP zaglavlje. Nakon toga se računa vrijednost pripadajućeg AH zaglavlja i formira isto. U ovom slučaju ESP dio paketa ne sadrži opcionalno polje *autentikacijski podaci*, pošto autentikaciju, integritet i neporecivost osigurava AH.

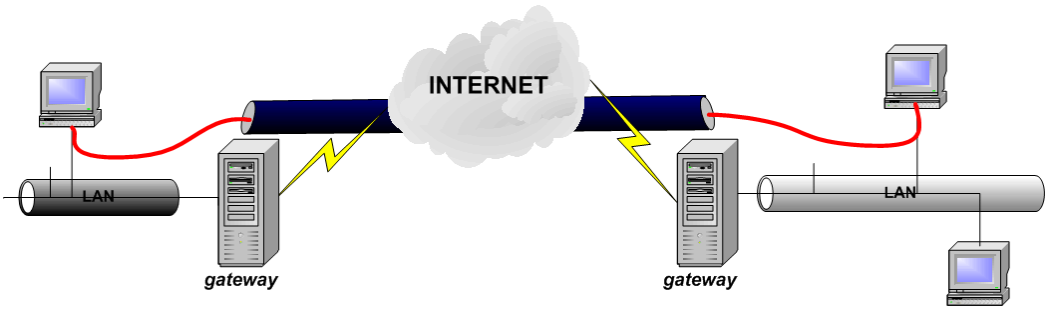


Slika 7: *ESP + AH u transportnom načinu rada*

4.2. Tuneliranje

Tuneliranje je drugi način rada ili druga funkcionalnost IPSec protokola. U tom načinu rada IPSec služi za uspostavu sigurne komunikacije između *gateway* uređaja na udaljenim mrežama (eng. *gateway-to-gateway*), osiguravajući tako virtualnu privatnu komunikaciju, odnosno uspostavljajući VPN (eng. *Virtual Private Network*) spoj između udaljenih lokacija. U ovom slučaju krajnji entiteti u komunikaciji ne moraju podržavati IPSec; čitava komunikacija za njih je potpuno transparentna jer sve operacije nužne za sigurnu komunikaciju korištenjem IPSec-a obavljaju *gateway* uređaji. *Gateway* uređaji na udaljenim mrežama predstavljaju ulaznu, odnosno izlaznu točku sigurnog komunikacijskog kanala. Oni preko nesigurnog medija (Internet) formiraju sigurni tunel, zbog čega se ovaj način rada i zove tuneliranje (Slika 8).

Korištenje tunelskog načina rada također je moguće i u *host-to-host* ili *host-to-gateway* komunikaciji, no tada ponovno krajnji entiteti ili entitet moraju podržavati IPSec.



Slika 8: *Tuneliranje*

Za razliku od transportnog načina rada gdje se AH odnosno ESP zaglavlja dodaju unutar postojećeg IP datagrama, kod tuneliranja se formira potpuno novi IP datagram koji enkapsulira kompletni originalni IP datagram.

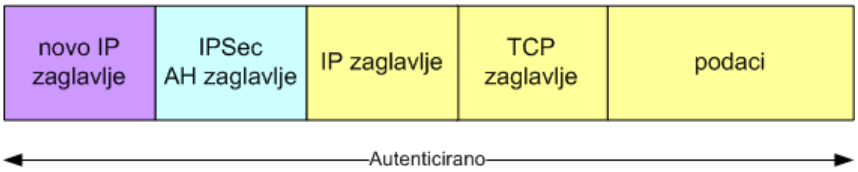
U načelu komunikacija između dva entiteta funkcionira na sljedeći način:

1. Izvorno računalo formira IP datagram i šalje ga preko lokalne mreže lokalnom *gateway* uređaju.
2. *Gateway* uređaj enkapsulira čitav originalni IP datagram u novi datagram (IP enkapsulacija – RFC dokument 2003), te formira odgovarajuća AH odnosno ESP zaglavlja.

3. Tako formirani datagram se šalje preko uspostavljenog tunela do *gateway* uređaja na udaljenoj mreži koji uklanja dodatna zaglavlja, te po potrebi vrši dešifriranje i provjeru integriteta paketa.
4. Nakon toga originalni IP datagram se isporučuje ciljnom računalu.

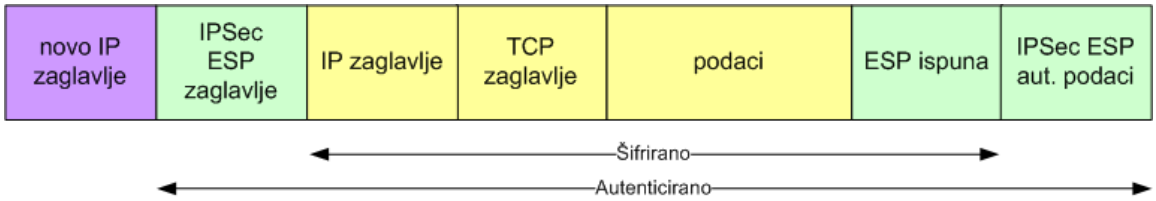
Isto kao i u transportnom načinu rada, moguća je implementacija korištenjem AH i ESP.

AH – Ukoliko se želi osigurati samo integritet, autentikacija i neporecivost poruka, a tajnost nije nužna, moguće je koristiti AH protokol. U tom slučaju originalni IP datagram, koji sadrži adresu krajnjeg odredišta, se enkapsulira u novi IP datagram kojem se dodaje odgovarajuće AH zaglavlje (Slika 9). U ovom slučaju polje *protokol* novog IP zaglavlja koje sadrži adresu krajnje točke IPSec tunela ima vrijednost 51 (AH), dok polje *sljedeće zaglavlje* unutar AH zaglavlja ima vrijednost 4 (enkapsulirani IP).



Slika 9: *Tuneliranje korištenjem AH*

ESP – Ukoliko se osim autentikacije, integriteta i neporecivosti želi osigurati i tajnost komunikacije, nužna je uporaba ESP protokola. Korištenjem ESP u tunelskom načinu rada, za razliku od transportnog načina, vrši se šifriranje čitavog originalnog IP datagrama, a također je osigurana autentikacija, integritet i neporecivost čitavog datagrama, pošto je sam datagram enkapsuliran u novi IP paket. U ovom slučaju polje *protokol* novog IP zaglavlja koje, isto kao i kod AH, sadrži adresu krajnje točke IPSec tunela ima vrijednost 50 (ESP), dok polje *sljedeće zaglavlje* unutar ESP zaglavlja ima vrijednost 4 (enkapsulirani IP).



Slika 10: *Tuneliranje korištenjem ESP*

Kombinacija AH i ESP u tunelskom načinu rada nije predviđena (RFC dokument 2401).

5. Uspostava IPSec komunikacije

Korištenjem IPSec-a, odnosno AH i/ili ESP protokola, osigurava se integritet, autentikacija, neporecivost i povjerljivost, no unutar IPSec-a nije implementiran nikakav mehanizam koji bi služio za uspostavu komunikacije, odnosno specifikaciju kriptografskih algoritama i funkcija koje će se koristiti u IPSec komunikaciji.

Za korištenje bilo kakvih kriptografskih metoda nužno je da entiteti u komunikaciji dogovore skup sigurnosnih parametara komunikacije (eng. *Security Association – SA*). Taj skup sigurnosnih parametara uključuju dogovor kriptografskih metoda koje će se koristiti, način autentikacije strana u komunikaciji, te razmjenu kriptografskih ključeva nužnih za tako dogovorenu komunikaciju.

Postoji nekoliko načina na koje je moguće uspostaviti IPSec komunikaciju. Na prvom mjestu, teoretski je moguće ručno podešavanje skupa sigurnosnih parametara, no to za bilo kakvu ozbiljniju primjenu nije prihvatljivo.

Osim toga, postoji nekoliko formalnih metoda koje se koriste ili su predlagane za uspostavu IPSec komunikacije. Photuris i SKIP (eng. *Simple Key management for Internet Protocols*), protokoli bazirani na Diffie-Hellman razmjeni ključeva mogu se koristiti za tu svrhu, no u širokoj primjeni prihvaćen je ISAKMP (eng. *Internet Security Association and Key Management Protocol*), odnosno IKE (eng. *Internet Key Exchange*).

5.1. IKE

IKE je standardni protokol za uspostavu sigurne IPSec komunikacije, a definiran je u RFC 2409 dokumentu. Protokol je implementiran kombiniranjem nekoliko postojećih protokola; na prvom mjestu ISAKMP, te Oakley i SKEME protokola.
ISAKMP protokol, definiran u RFC 2408 dokumentu, specificira infrastrukturu za autentikaciju i razmjenu ključeva. Protokol je oblikovan tako da je neovisan o načinu razmjene ključeva, odnosno može podržati razne metode za razmjenu ključeva.
Oakley protokol opisuje načine razmjene ključeva (eng. *modes*), te detalje i usluge koje svaki od tih načina pruža. SKEME je također protokol koji opisuje način razmjene ključeva i koji osigurava anonimnost, a baziran je na starijem Photuris protokolu.
Uspostava IPSec komunikacije korištenjem IKE protokola sastoji se od dvije osnovne faze:
- uspostave IKE (ISAKMP) SA skupa sigurnosnih parametara i
- uspostave IPSec SA skupa sigurnosnih parametara korištenjem IKE SA.

Uobičajeno je da se za IKE komunikaciju koristi UDP port 500.

5.2. Uspostava IKE SA

Osnovna funkcija IKE SA skupa sigurnosnih parametara jest osigurati autentikaciju i sigurnost IKE prometa, a unutar tako uspostavljene komunikacije mogu se definirati višestruki IPSec SA.
Atributi koje uspostavljeni IKE SA mora sadržavati su:
- algoritam za šifriranje,
- *hash* funkcija,
- metoda autentikacije i
- Oakley grupa koja definira Diffie-Hellman razmjenu ključeva (RSA, eliptičke krivulje).

Metoda autentikacije označava način na koji će se entiteti autenticirati u nadolazećoj komunikaciji. IKE podržava sljedeće metode autentikacije:
- korištenje digitalnih potpisa (RSA ili DSS),
- korištenje tajnog ključa (eng. *preshared key*) i
- korištenje kriptografije temeljene na javnim ključevima (osnovna i modificirana metoda).

Uspostava IKE SA može se provesti na dva načina:
- glavni način (eng. *main mode*) i
- agresivni način (eng. *aggressive mode*).

Glavni način se koristi kada je nužna zaštita identiteta entiteta u komunikaciji. U glavnom načinu rada entiteti moraju razmijeniti 6 poruka da bi uspostavili IKE SA. Agresivni način se može koristiti kada zaštita identiteta nije nužna, već je poželjna što veća brzina uspostave komunikacije. Kod ovog načina potrebna je razmjena svega 3 poruke između entiteta. Valja napomenuti da će, ukoliko se kod agresivnog načina koristi kriptografija temeljena na javnim ključevima, zaštita identiteta također biti osigurana.
Za održavanje IKE komunikacije potrebno je generirati četiri različita sjednička ključa:
- `SKEYID` – glavni ključ koji se koristi za generiranje ostalih ključeva,
- `SKEYID_d` – ključ koji IKE SA koristi za šifriranje poruka,
- `SKEYID_a` – ključ koji IKE SA koristi za osiguranje integriteta i autentikaciju poruka,
- `SKEYID_e` – ključ koji služi za generiranje IPSec SA.

Pri generiranju ključeva koriste se i kolačići koje generiraju entiteti u komunikaciji i koji predstavljaju *hash* vrijednosti izračunate od identifikatora (IP adresa entiteta, port, protokol), vremenske značke i tajne vrijednosti poznate samo entitetu koji je generirao kolačić.
Detaljni opis protokola izlazi iz okvira ovog dokumenta, no zbog pojašnjenja kao primjer će biti pokazana uspostava IKE sa korištenjem tajnog ključa. Oznake u nastavku imaju značenja kako je navedeno:
- `prf()` – pseudoslučajna funkcija (*hash* funkcija),
- `HDR` – ISAKMP zaglavlje (označava način),
- `HDR*` – ISAKMP zaglavlje koje enkapsulira šifrirane podatke,
- `SA` – predloženi (ili prihvaćeni) skup sigurnosnih parametara,
- `Ni`, `Nr` – slučajne vrijednosti (eng. *nonce*) generirane od strane pojedinog entiteta,

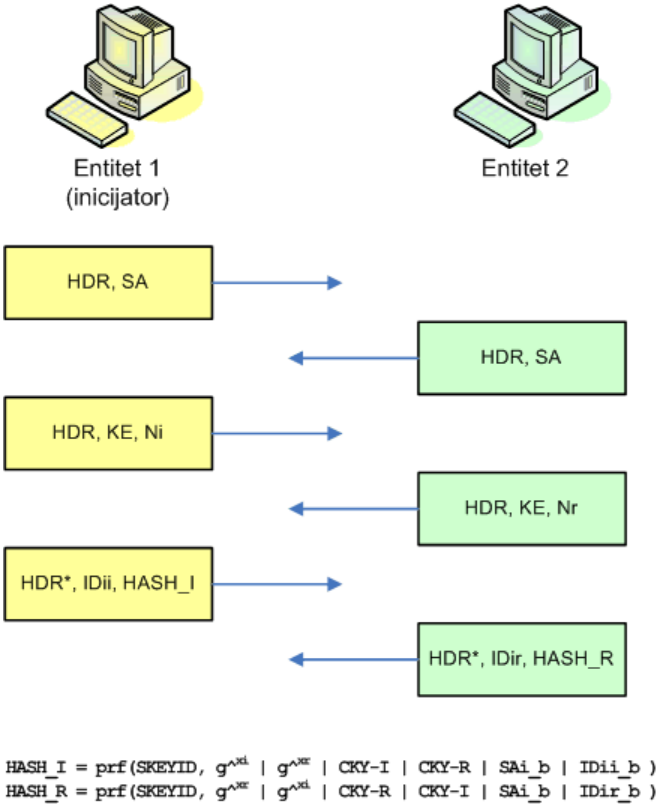
- KE – informacije koje se koriste u Diffie-Hellman razmjeni ključeva,
- HASH – *hash* vrijednost parametara koji služe za autentikaciju,
- IDii, IDir, IDci, IDcr – identiteti entiteta u komunikaciji,
- g^{xy} – Diffie-Hellman zajednički tajni ključ,
- g^{xi}, g^{xr} – javne Diffie-Hellman vrijednosti za entitete u komunikaciji,
- CKY-I, CKY-R – kolačići generirani od strane entiteta,
- | – oznaka za konkatenaciju.

Slika 11 prikazuje uspostavu IKE SA na glavni način uz autentikaciju korištenjem tajnog ključa. Kod takve autentikacije glavni sjednički ključ se generira na sljedeći način:

```
SKEYID = prf(tajni ključ, Ni_b | Nr_b)
```

Dok se preostali sjednički ključevi generiraju na temelju tog ključa, neovisno o metodi autentikacije:

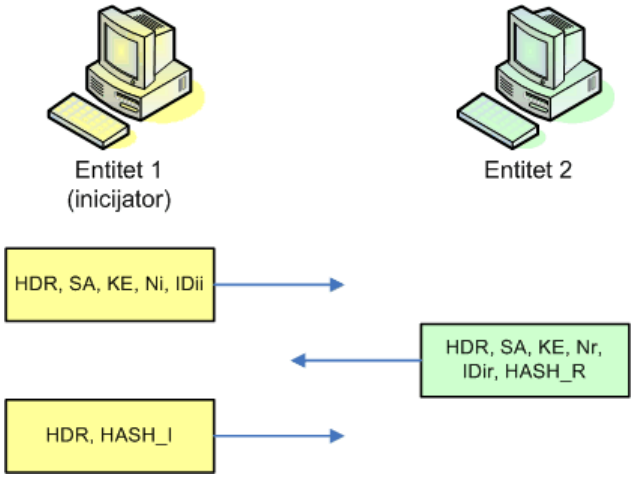
```
SKEYID_d = prf(SKEYID, g^xy | CKY-I | CKY-R | 0)
SKEYID_a = prf(SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
SKEYID_e = prf(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)
```



Slika 11: *Uspostava IKE SA na glavni način uz autentikaciju korištenjem tajnog ključeva*

Metoda autentikacije korištenjem tajnog ključa ranjiva je na tzv. *man-in-the-middle* napade, što je inherentno svojstvo Diffie-Hellman algoritma za razmjenu ključeva, tako da se za sigurnu autentikaciju preporuča korištenje kriptografije temeljene na javnim ključevima, odnosno PKI.

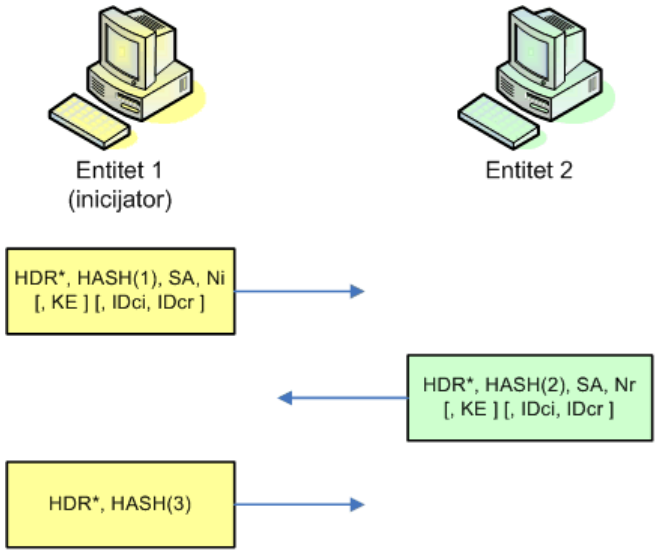
Kod agresivnog načina (Slika 12), broj poruka koje je potrebno razmijeniti je reduciran, no kod ovog načina, osim što nije osigurana zaštita identiteta, moguće je izvođenje napada primjenom sile (eng. *brute force*) jer se HASH vrijednosti u ovom načinu prenose kao otvoreni tekst, a ne šifrirano kao kod normalnog načina.



Slika 12: *Agresivni način uspostave IKE SA uz autentikaciju korištenjem tajnog ključa*

5.3. Uspostava IPSec SA

Druga faza IKE protokola služi za uspostavu IPSec SA skupa sigurnosnih parametara. Ova faza provodi se u tzv. brzom načinu (eng. *quick mode*). Cijela komunikacija koja se odvija kroz drugu fazu zaštićena je korištenjem prethodno uspostavljenog IKE SA skupa sigurnosnih parametara.
Ova faza ustvari nije zasebna faza, već se koristi samo za generiranje IPSec SA na temelju ranije uspostavljenog IKE SA. Slika 13 prikazuje komunikaciju između entiteta prilikom uspostave IPSec SA.




```
HASH(1)=prf(SKEYID_a, M-ID | SA | Ni [| KE] [| IDci | IDcr])
HASH(2)=prf(SKEYID_a, M-ID | Ni_b | SA | Nr [| KE] [| IDci | IDcr])
HASH(3)=prf(SKEYID_a, 0 | M-ID | Ni_b | Nr_b)
```

Slika 13: *Uspostava IPSec SA*

Nakon što se okonča druga faza IKE protokola, dva entiteta u komunikaciji su definirala IPSec SA skup sigurnosnih parametara, te mogu uspostaviti siguran kanal za razmjenu poruka.

6. IPSec redundancija

Jedno od pitanja koje se često postavlja jesu dodatni resursi koje IPSec zahtijeva. Zbog kriptografskih operacija koje su matematički zahtjevne, korištenje IPSec-a zahtijeva dodatne procesorske resurse, no detaljna analiza tih zahtjeva izlazi iz okvira ovog dokumenta.

Osim zahtijeva za procesorskim resursima, IPSec također povećava ukupan mrežni promet, što je samo po sebi razumljivo ukoliko se IPSec datagrami promatraju u odnosu na standardne IP datagrame. Povećanje mrežnog prometa, odnosno redundancija (eng. *overhead*) koju IPSec unosi, a što može rezultirati degradacijom mrežnih performansi, proizlazi iz dva funkcionalna razloga:

– zbog dodatnih zaglavlja koja se mogu pojaviti u različitim načinima IPSec rada,
– zbog kriptografskih algoritama koji se koriste, odnosno ispune (eng. *padding*) koja je nužna za njihovo ispravno funkcioniranje.

6.1. Redundancija zaglavlja

Redundancija zaglavlja ovisi o načinu rada IPSec-a, kao i o IPSec protokolima koji se koriste. Korištenje AH protokola (ukoliko se koriste propisane *hash* funkcije MD5 ili SHA-1) unosi redundanciju od 24 okteta od čega 12 okteta otpada na zaglavlje bez polja *autentikacijski podaci*, dok preostalih 12 okteta (96 bita) otpada na to polje koje sadrži ICV vrijednost generiranu od strane *hash* funkcija. Ovdje valja napomenuti da, iako MD5 daje izlazni rezultat duljine 128 bita, a SHA-1 160 bita, se te vrijednosti za potrebe IPSec-a svode na 96-bitni duljinu.

Ukoliko se koristi ESP protokol, redundancija ovisi o tome da li se ESP koristi samo za osiguravanje tajnosti, ili služi također za osiguranje integriteta, neporecivosti i autentikacije poruke. Također, redundancija ovisi i o kriptografskom protokolu koji se koristi. ESP zaglavlje samo po sebi dodaje 8 okteta. Nadalje, ukoliko se kriptografski algoritmi koriste u CBC načinu rada, zahtijevati će korištenje IV, inicijalizacijskog vektora, čija duljina može biti do 16 okteta (8 okteta za DES i 3DES ili 16 okteta za AES). Tu su još četiri okteta koji se odnose na polja duljina ispune i sljedeće zaglavlje (dva okteta za polja i dva nužna okteta za poravnanje do 32-bitne riječi), a ukoliko se ESP koristi za osiguranje integriteta, neporecivosti i autentikacije, potrebno je dodati i 12 oktetnu ICV vrijednost koja je u tom slučaju sadržana u polju *autentikacijski podaci* na kraju ESP datagrama.

Konačno, ukoliko se IPSec koristi u tunelskom načinu rada valja dodati i 20 okteta, kolika je duljina novog IP zaglavlja. Tablica 1 prikazuje redundanciju koju unosi IPSec, ovisno o načinu rada, protokolu i kriptografskim algoritmima koji se koriste.

		Transportni način	Tuneliranje
AH	MD5, SHA-1	24 okteta	44 okteta
ESP	DES, 3DES, AES + MD5, SHA-1	24 okteta	44 okteta
	DES-CBC, 3DES CBC + MD5, SHA-1	32 okteta	52 okteta
	AES-CBC + MD5, SHA-1	40 okteta	60 okteta
AH+ESP	DES, 3DES, AES+ MD5, SHA-1	36 okteta	-
	DES-CBC, 3DES CBC + MD5, SHA-1	44 okteta	-
	AES-CBC + MD5, SHA-1	52 okteta	-

Tablica 1: *Redundancija IPSec zaglavlja*

Tablica 2 prikazuje prosječnu redundanciju koju IPSec zaglavlja dodaju u odnosu na standardni IP datagram. Iz tablice se lako može uočiti da je ta redundancija općenito nešto veća u tunelskom načinu rada, te da je značajna za kratke datagrame, dok kod većih datagrama postaje zanemariva.

Duljina paketa	**Transportni način**			**Tuneliranje**		
	ESP 3DES CBC + SHA-1, MD5	**ESP** AES CBC + SHA-1, MD5	**AH** SHA-1, MD5	**ESP** 3DES CBC + SHA-1, MD5	**ESP** AES CBC + SHA-1, MD5	**AH** SHA-1, MD5
46	70%	87%	52%	113%	130%	96%
512	6,3%	7,8%	4,7%	10,2%	11,7%	8,6%
1500	2,1%	2,7%	1,6%	3,5%	4%	2,9%

Tablica 2: *Prosječna redundancija IPSec zaglavlja u odnosu na duljinu datagrama*

6.2. Redundancija ispune

Redundancija ispune ovisi o IPSec protokolima koji se koriste, odnosno direktno o kriptografskim algoritmima i *hash* funkcijama koje su odabrane u SA skupu sigurnosnih parametara. Ta ispuna je

nužna iz razloga što kriptografski algoritmi i *hash* funkcije kao ulaz koriste blokove fiksne duljine, čija duljina ovisi o specifičnom algoritmu koji će se koristiti (Tablica 3).

Kriptografski algoritam/*hash* funkcija	Duljina bloka
DES, 3DES	64 bita
AES	128 bita
MD5, SHA-1	512 bita

Tablica 3: *Duljine ulaznih blokova podataka za uobičajene kriptografske algoritme i hash funkcije*

Kod kriptografskih algoritama (DES, 3DES, AES) to konkretno znači da će svaki datagram imati ispunu takvu da IP datagram bude poravnat na 64 bitni odnosno 128 bitni blok. Kod *hash* funkcija (MD5 i SHA-1), zbog implementacijske specifičnosti, datagram će biti poravnat na 448 bitni blok. Razlog tome je što oba algoritma ulaznim podacima implicitno dodaju 64-bitni blok podataka, što skraćuje duljinu ulaznog bloka koji može biti procesuiran u *hash* funkciji.
Tablica 4 prikazuje redundanciju ispune u najgorim slučajevima (kada je potrebna duljina ispune maksimalna). Uočljivo je da je redundancija kod manjih paketa značajna, dok kod većih paketa ta redundancija u relativnom udjelu značajno opada.

Algoritam/ funkcija	Duljina bloka	Mali paketi (~50 okteta)	Prosječni paketi (~350 okteta)	Veliki paketi (~1500 okteta)	Duljina paketa je višekratnik bloka
DES, 3DES	64 bita	~15%	~2%	~0,5%	0%
AES	128 bita	~30%	~4%	~1%	0%
SHA-1, MD5	512 bita	~100%	~18%	~4%	0%

Tablica 4: *Redundancija ispune u najgorim slučajevima*

7. Implementacijski problemi

IPSec protokol, sam po sebi donosi neke probleme koje je ponekad, u specifičnim mrežnim okruženjima teško ili nemoguće riješiti. To se prvenstveno odnosi na korištenje NAT-a, te IP fragmentaciju koja se može pojaviti prilikom IPSec komunikacije.

7.1. NAT

Obzirom na poznata ograničenja adresiranja kod IPv4 protokola, velik broj lokalnih mreža koristi privatno adresiranje, a pristup Internetu, odnosno udaljenim lokacijama, implementira se korištenjem NAT-a (eng. *Network Address Translation*) koji može biti statički ili dinamički, odnosno NAPT-a (eng. *Network Address Port Translation*).
Ukoliko se bilo gdje između entiteta koji žele uspostaviti IPSec komunikaciju provodi NAT, korištenje AH bilo u transportnom, bilo u tunelskom načinu rada, za TCP/UDP komunikaciju nije moguće pošto će provođenje NAT-a rezultirati narušavanjem integriteta IP datagrama i uzrokovati njegovo odbacivanje na strani primatelja.
Ukoliko se za IPSec koristi samo ESP, stvar je donekle drugačija. U transportnom načinu rada provođenje NAT-a također rezultira nemogućnošću IPSec komunikacije, no u tunelskom načinu ESP može funkcionirati.
Pri korištenju NAT-a pažnju valja obratiti i na IKE/ISAKMP, jer autentikacija temeljena na tajnom ključu koristi i kolačiće koji se generiraju ovisno o IP adresi entiteta, što također rezultira gubitkom integriteta, te nemogućnošću uspostave komunikacije. Ovaj nedostatak, za razliku od problema s AH i ESP, može se riješiti korištenjem drugih IKE autentikacijskih metoda (korištenje digitalnih potpisa ili kriptografije temeljene na javnim ključevima).

7.2. Fragmentacija

Pri korištenju IPSec komunikacije, prvenstveno u tunelskom načinu rada, a isto tako i IKE/ISAKMP komunikacije, može doći do IP fragmentacije. U tom slučaju mogu se pojaviti dodatni problemi. Naime, neki vatrozidi ili usmjerivači mogu biti konfigurirani tako da odbacuju IP fragmentirane datagrame, jer na taj način osiguravaju mreže od nekih oblika DoS napada (npr. *Teardrop*). Očiti

problem kod toga jest da će u tom slučaju i legitimni IPSec ili IKE paketi isto biti odbačeni, što će onemogućiti uspostavu sigurnog kanala među udaljenim entitetima.

8. Zaključak

IPSec je protokol kojem je cilj osigurati tajnost, integritet, autentikaciju i neporecivost poruka koje razmjenjuju entiteti u komunikaciji. Kako je u iz dokumenta vidljivo, sam protokol je prilično složen, a uspostava komunikacije odvija se u više koraka. Dodatni zahtjev je taj da je za uspostavu IPSec kanala prethodno nužno uspostaviti IKE/ISAKMP komunikaciju.
Osim toga, zbog same implementacije mogu se pojaviti problemi vezani uz NAT i fragmentaciju, što može onemogućiti uspostavu IPSec kanala.
Postoje i neki sigurnosni problemi vezani uz korištenje tajnih ključeva koji omogućavaju pojedine napade, no u realnim situacijama oni su prilično nevjerojatni. Osim toga, ti problemi mogu se efikasno otkloniti korištenjem kriptografije temeljene na javnim ključevima, odnosno uporabom digitalnih certifikata i PKI.
U realnim situacijama, često se dešava da se ne može osigurati interoperabilnost različitih IPSec implementacija, odnosno da je proizvode različitih proizvođača teško konfigurirati da međusobno komuniciraju.
Bez obzira na sve te nedostatke, u većini situacija, pažljivim planiranjem i adekvatnom implementacijom, IPSec služi kao vrlo efikasno i robusno rješenje za uspostavu sigurne *host-to-host* komunikacije ili uspostavu VPN kanala između udaljenih lokacija.

9. Reference

The MD5 Message-Digest Algorithm, http://www.ietf.org/rfc/rfc1321.txt,

US Secure Hash Algorithm 1 (SHA1), http://www.ietf.org/rfc/rfc3174.txt,

IP Encapsulation within IP, http://www.ietf.org/rfc/rfc2003.txt,

Security Architecture for the Internet Protocol, http://www.ietf.org/rfc/rfc2401.txt,

IP Authentication Header, RFC 2402, http://www.ietf.org/rfc/rfc2402.txt,

IP Encapsulating Security Payload (ESP), RFC2406, http://www.ietf.org/rfc/rfc2406.txt,

The Internet Security Association and Key Management Protocol, RFC 2408, http://www.ietf.org/rfc/rfc2408.txt,

The Internet Key Exchange, http://www.ietf.org/rfc/rfc2409.txt, RFC 2409, http://www.ietf.org/rfc/rfc2409.txt,

The OAKLEY Key Determination Protocol, RFC 2412, http://www.ietf.org/rfc/rfc2412.txt,

Explaining the Gap between Specification and Actual Performance for IPsec VPN Systems, http://www.tisc2001.com/newsletters/39.html.

Dodatak A: Popis RFC dokumenata vezanih iz IPSec

The ESP DES-CBC Transform (RFC 1829)
IP Encapsulating Security Payload (ESP) (RFC 1827) obsoleted by RFC 2406
IP Authentication using Keyed MD5 (RFC 1828)
IP Authentication Header (RFC 1826) obsoleted by RFC 2402
Security Architecture for the Internet Protocol (RFC 1825) obsoleted by RFC 2401
HMAC: Keyed-Hashing for Message Authentication (RFC 2104)
HMAC-MD5 IP Authentication with Replay Prevention (RFC 2085)
Security Architecture for the Internet Protocol (RFC 2401)
The NULL Encryption Algorithm and Its Use With IPsec (RFC 2410)
IP Security Document Roadmap (RFC 2411)
IP Authentication Header (RFC 2402)
The OAKLEY Key Determination Protocol (RFC 2412)
The ESP CBC-Mode Cipher Algorithms (RFC 2451)
The Use of HMAC-MD5-96 within ESP and AH (RFC 2403)
The Use of HMAC-SHA-1-96 within ESP and AH (RFC 2404)
The ESP DES-CBC Cipher Algorithm With Explicit IV (RFC 2405)
IP Encapsulating Security Payload (ESP) (RFC 2406)
The Internet IP Security Domain of Interpretation for ISAKMP (RFC 2407)
Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408)
The Internet Key Exchange (IKE) (RFC 2409)
The Use of HMAC-RIPEMD-160-96 within ESP and AH (RFC 2857)
More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) (RFC 3526)
On the Use of Stream Control Transmission Protocol (SCTP) with IPsec (RFC 3554)
The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec (RFC 3566)
The AES-CBC Cipher Algorithm and Its Use with IPsec (RFC 3602)
The AES-XCBC-PRF-128 algorithm for IKE (RFC 3664)
Using AES Counter Mode With IPsec ESP (RFC 3686)
A Traffic-Based Method of Detecting Dead IKE Peers (RFC 3706)

Službena IETF Web stranica vezana us IPSec protokol je sljedeća:
http://www.ietf.org/html.charters/ipsec-charter.html