FAKULTET ELEKTROTEHNIKE I RAČUNARSTVSA
Zavod za elektroničke sustave i obradu informacija

Sustavi za praćenje i vođenje procesa

Seminarski rad

# IPsec (IP security)

1. lipnja 2006.

Goran Živković
0036392772

# Sadržaj

# Uvod

IPsec (IP security) predstavlja skupinu protokola namijenjenih zaštićenoj komunikaciji preko Interneta. Ovi protokoli funkcioniraju na 3. sloju OSI modela i sastavni su dio IPv6 skupine protokola (a mogu se opcionalno uključiti i unutar IPv4 sustava). Zbog činjenice da funkcionira na 3. sloju OSI modela, IPsec pruža jednostavnu i efikasnu zaštitu i za TCP i za UDP protokole komunikacije preko računalne mreže.
U osnovi se IPsec dijeli na dvije podskupine protokola:

- kriptografski protokoli – **ESP protokol** (eng. Encapsulating Security Payload), **AH protokol** (eng. Authentication Header)
- protokoli za razmjenu ključeva – **IKE protokol** (eng. Internet Key Exchange)

Sam standard prvotno je definiran RFC-ovima 1825 – 1829, objavljenih 1995. godine. Od tada protokol je doživio popriličan broj izmjena, a zadnja revizija protokola datira iz prosinca 2005 te se može pronaći u RFC 4301 - 4309 dokumentima.

# Dizajn sustava

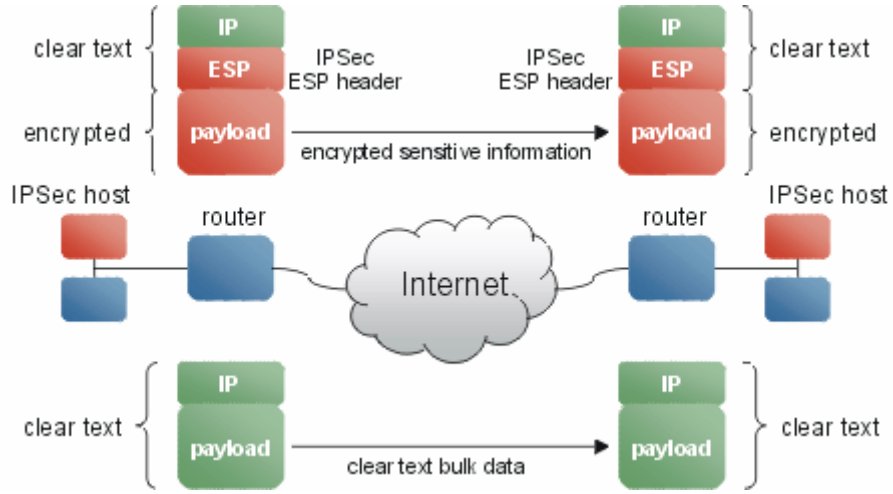
IPsec je dizajniran tako da zadovolji dvije osnovne zadaće:

- **tuneliranje paketa** i
- **transportni način rada.**

U prvom slučaju nekoliko računala (ili cijela jedna lokalna mreža) sakriva se iza jednog čvora te je kao takva nevidljiva ostatku mreže (a samim time i zaštićena od napada). U drugom slučaju paketi se šalju između dva krajnja računala na mreži, pri čemu računalo koje prima paket izvršava sigurnosne provjere prije isporučivanja paketa višim slojevima. U oba slučaja moguće je izgraditi Virtualne Privatne Mreže – VPN (eng. Virtual Private Network), što je i osnovna ideja zaštite IPsec protokolima.

Dodatno, kako IP protokol nije pružao nikakve elemente zaštite, pred IPsec postavljeni su i slijedeći zahtjevi:

1. kriptiranje podataka koje se prenose (eng. payload)
2. provjera integriteta podataka
3. autentificiranje čvorova kroz koje paket prolazi
4. omogućavanje tzv. 'Anti-Replay' opcije (zaštita od neovlaštenog odgovora za vrijeme aktivne sjednice)




Slika 1. Prikaz sustava baziranog na IPsec protokolu

# Osnovni protokoli

## *Authentication Header (AH) protokol*

Authentication Header (AH) protokol osigurava integritet bespojne veze te provjerava originalnost podataka koji se prenose IP datagramima. Opcionalno, ovaj protokol omogućava i zaštitu od tzv. 'replay' napada za što koristi tehniku odbacivanja starih paketa. Zaglavlje AH paketa prikazano je na slici 2.

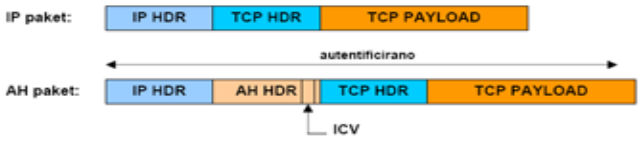
| 0 | 1 | 2 | 3 |
|---|---|---|---|
| 0 1 2 3 4 5 6 7 | 0 1 2 3 4 5 6 7 | 0 1 2 3 4 5 6 7 | 0 1 2 3 4 5 6 7 |
| Next Header | Payload Length | RESERVED | |
| Security Parameters Index (SPI) | | | |
| Sequence Number | | | |
| Authentication Data (variable) | | | |

Slika 2. Prikaz zaglavlja AH paketa

Značenje pojedinog polja:

- **Next Header –** označava protokol podataka koji se prenose (TCP ili UDP)
- **Payload Length –** duljina AH paket
- **RESERVED –** još se ne koristi (svi bitovi se postavljaju na nulu)
- **Security Parameters Index (SPI) -** kombinacija sigurnosnih parametara i IP adrese
- **Sequence Number** – redni broj paketa, koristi se za zaštitu od 'replay' napada
- **Authentication Data -** skup podataka koji se koristi za autentifikaciju paketa

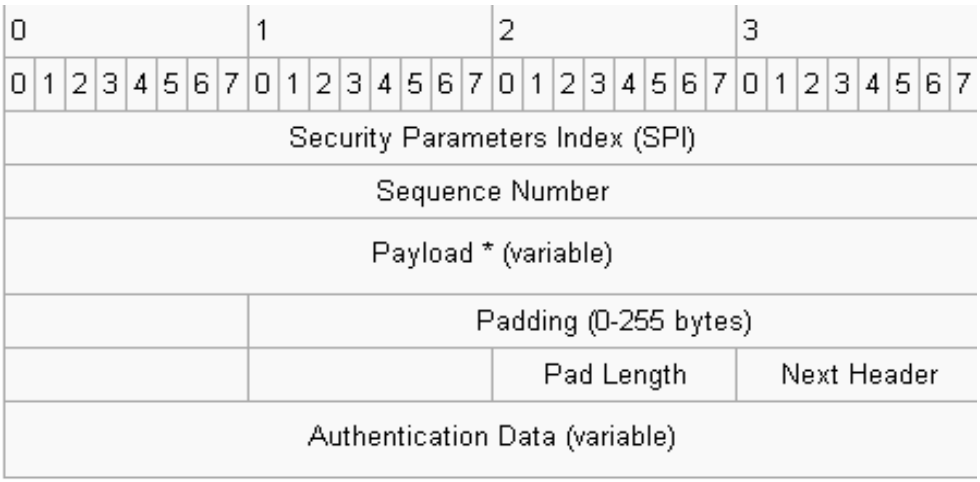
Usporedba IP i AH paketa dana je na slici 3.




Slika 3 Usporedba IP i AH paketa

## *Encapsulated Security Payload (ESP) protokol*

Encapsulating Security Payload (ESP) zaglavlje omogućava provjeru originalnosti paketa, integritet i tajnost podataka koji se prenose. Na slici 4 prikazan je izgled ESP zaglavlja.

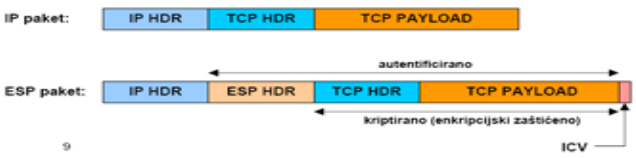



Slika 4. Prikaz zaglavlja ESP paketa

Značenje pojedinog polja:

- **Security Parameters Index (SPI)** - kombinacija sigurnosnih parametara i IP adrese
- **Sequence Number** - redni broj paketa, koristi se za zaštitu od 'replay' napada
- **Payload Data** - podaci koji se šalju
- **Padding** - koristi se za prijenos podataka koji popunjavaju cijeli blok
- **Pad Length** - duljina *Padding* polja
- **Next Header** – označava protokol podataka koji se prenose (TCP ili UDP)
- **Authentication Data** - skup podataka koji se koristi za autentifikaciju paketa

Usporedba IP i ESP paketa dana je na slici 5.

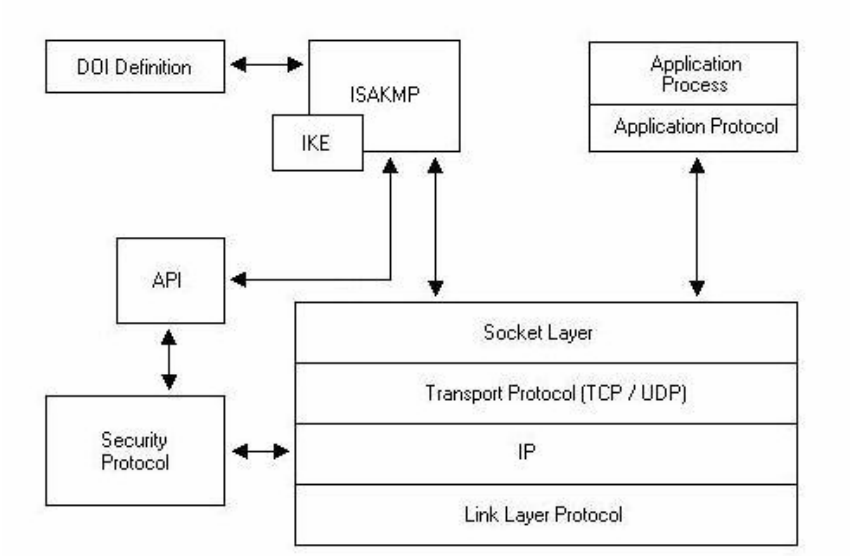



Slika 5. Usporedba IP i ESP paketa

## *IKE protokol*

IKE protokol obavlja obostranu autentifikaciju korisnika te uspostavlja SA (Security Association) vezu. Uspostava SA veze podrazumijeva izračunavanje *keying* materijala te dogovaranje oko skupa algoritama i drugih parametara koji će štititi SA.

Protokol radi tako da inicijator veze (eng. initiator) nudi prihvatljive parametre za zaštitu SA. Ako ih druga strana prihvati (eng. responder) ostvaruje se SA veza. Primjer ostvarivanja kriptiranja podataka za slanje preko mreže od strane API (eng. Application Programming Interface) aplikacije pomoću IKE protokola (IKEv2) prikazana je na slici 6.

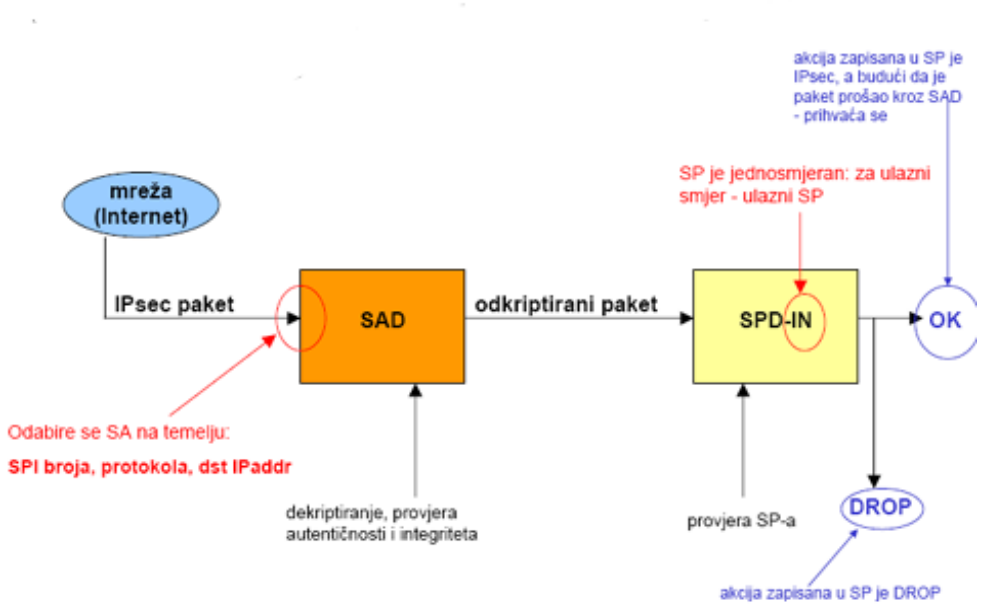



Slika 6. Prikaz rada IKE protokola

# Obrada paketa

## *Obrada ulaznih paketa*

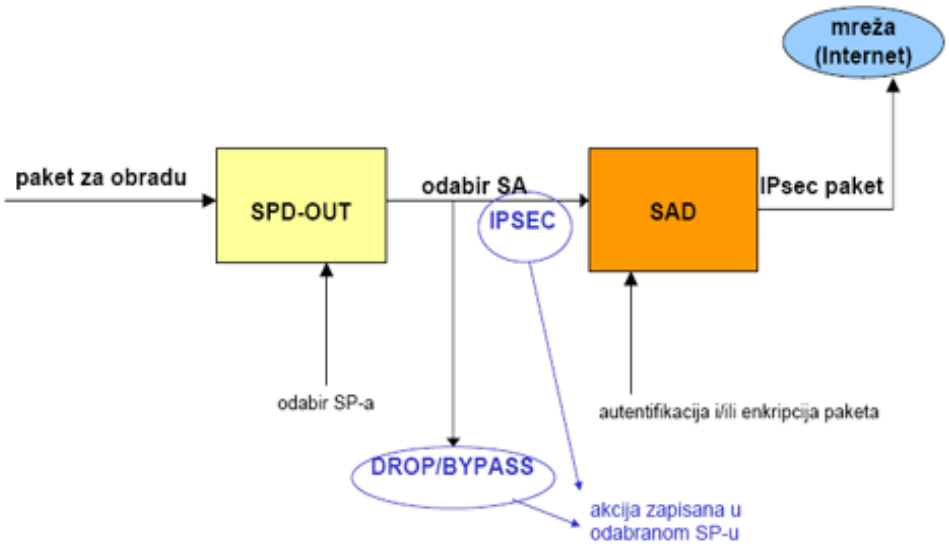
IPsec paket kojeg računalo prima s globalne računalne mreže (Interneta) prolazi kroz filtere definirane u SAD (Security Association Database) bazi. U ovom koraku podaci se dekriptiraju te se provjerava njihova autentičnost i integritet. Takvi podaci šalju se u SPD filter (Security Policy Database) gdje se u ovisnosti o tome da li paketi odgovaraju predefiniranim sigurnosnim politikama ili prihvaćaju ili odbijaju. Cijeli proces obrade ulaznih paketa prikazan je na slici 7.




Slika 7. Obrada ulaznih paketa

## *Obrada izlaznih paketa*

Paket koji se želi poslati na javnu računalnu mrežu prvo prolazi kroz SPD-OUT filter gdje se provjeravaju predefinirana pravila o tome koji se paketi smiju proslijediti na javnu mrežu. Zatim se bira odgovarajući SA algoritam za zaštitu podataka. I zadnji korak prije slanja paketa na javnu mrežu jest postavljanje elemenata autentifikacije paketa i po potrebi enkripcija podataka koji se šalju. To se obavlja u izlaznom SAD filteru.
Slika 8 prikazuje obradu izlaznih paketa:




Slika 8 Obrada izlaznih paketa

# Implementacije IPsec protokola

Na Linux/Unix operacijskim sustavima osnove IPsec protokola implementirane su u samu jezgru (eng. kernel), dok je rad s IKE ključevima realiziran kroz ISAKMP/IKE sustav.

Projekt grupe FreeS/WAN – **pluto** je prva *open source* implementacija cjelokupnog IPsec sustava za Linux/Unix operacijske sustave. Ovaj projekt sastoji se od posebnih dodataka za samu jezgru napisanih u obliku programskih skripti koje se koriste za podešavanje parametara kojima se definira da li se određeni paket propušta ili odbacuje. (parametri SAD i SPD filtera).

Za Winows operacijske sustave postoje alati namijenjeni Server 2000 i SERVER 2003 kojima se uređuje komunikacija IPsec protokolom na razini domene koju ti poslužitelji opslužuju (Microsoft Domain Isolation). Također, kod MS Windows XP operacijskog sustava s instaliranim SP2, korisnicima stoje na raspolaganju programi koji korisnicima omogućavaju transparentu komunikaciju IPsec protokolom.

Od ostalih sustava za implementaciju IPsec protokola važno je još napomenuti i Cisco-ve programske pakete pomoću kojih i mrežni uređaji ove firme mogu komunicirati navedenim protokolom.

# Zaključak

Sve veća potreba za sigurnošću računalnih mreža zahtjeva adekvatne elemente zaštite. Praksa je pokazala da zaštita na što nižem sloju OSI modela znatno poboljšava sigurnost prijenosa podataka preko nesigurne računalne mreže. Ako se dodatno uzme u obzir kako je najznačajniji nivo OSI modela **mrežni sloj** lako se može zaključiti da se fokus sigurnosti treba napraviti na tom (trećem) sloju OSI modela.

IPsec protokoli su jednostavni i efikasni, a zaštita koju pružaju vrlo visoka. Zbog toga, i prethodno navedenih tendencija razvoja sigurnosti računalnih mreža, za očekivati je kako će u budućnosti sva mrežna komunikacija biti bazirana na IPsec protokolima.

## Literatura:


1. Uvod u IPsec, Ana Kukec, FER-ZEMRIS
2. Network world security
   http://www.networkworld.com/details/721.html
3. Webopedia
   http://www.webopedia.com/TERM/I/IPsec.html
4. Wikipedia.org
   http://en.wikipedia.org/wiki/IP_Security
5. Cisco
   http://www.cisco.com/warp/public/105/IPSECpart1.html
6. Microsoft
   http://www.microsoft.com/windows2000/en/server/iis/default.asp?url=/WINDOWS2000/en/server/iis/htm/asp/apro2k11.htm
7. Pluto Project
   http://www.pluto.it/