ZAVOD ZA ELEKTRONIKU, MIKROELEKTRONIKU, RAČUNALNE I INTELIGENTNE SUSTAVE
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
SVEUČILIŠTE U ZAGREBU

DIPLOMSKI RAD br. 1800

Upravljanje IPsec podsustavom u Linux okruženju uz pomoć NETLINK sučelja

Dalibor Dukić

Zagreb, srpanj 2009.

Zahvaljujem svima koji su mi pomogli u izradi ovog diplomskog rada, posebno dr.sc. Stjepanu Grošu i Doc.dr.sc. Leonardu Jelenkoviću na stručnom vodstvu i brojnim savjetima. Također veliko hvala mojoj obitelji i djevojci Morani na beskrajnom strpljenju i potpori, bez Vas ovo ne bih nikad postigao.

Sažetak

U operacijskom sustavu Linux implementirano je mnoštvo različitih mrežnih protokola. Kako bi aplikacije mogle upravljati postavkama tih protokola definirano je jedinstveno sučelje pod nazivom NETLINK. U okviru diplomskog rada proučeno je i opisano NETLINK sučelje s posebnim naglaskom na podskup tog sučelja pod nazivom XFRM. Na temelju načinjene analize ostvareno je upravljanje IPsec sigurnosnim poveznicama i politikama u implementaciji IKEv2 protokola za razmjenu ključeva. Opisana je arhitektura i detalji implementacije. Radu je priložen izvorni tekst programa i rezultati istraživanja uz potrebna objašnjenja i dokumentaciju. Citirana je korištena literatura.

Abstract

The Linux operating system incorporates variety of network protocols. Management of protocol settings is handled by unified interface called NETLINK. Diploma thesis describes NETLINK interface with emphasis on interface subset called XFRM. Based on the carried out analysis managing of IPsec security associations and policies within IKEv2 protocol for key exchange has been implemented. The architecture and details of implementation have been described. Source code of program and survey results have been enclosed along with documentation. Referenced literature was cited.

Sadržaj

Popis oznaka i kratica

OSI	Open Systems Interconnection
IETF	Internet Engineering Task Force
RFC	Request For Comment
NE	Network Element
CP	Control Plane
FP	Forwarding Plane
BSD	Berkeley Software Distribution
IP	Internet Protocol
API	Application Programming Interface
QoS	Quality of Service
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
BGP	Border Gateway Protocol
TC	Traffic Control
DiffServ	Differentiated Services
RSVP	Resource Reservation Protocol
NAT	Network Address Translation
UDP	User Datagram Protocol
IPC	Inter Process Communication
NLA	Netlink Attribute
TLV	Type Length Value
IOCTL	Input/Output Control
PROCFS	Process File System
INET	Internet socket
IPsec	Internet Protocol Security
SELinux	Security Enhanced Linux
iSCSI	Internet Small Computer System Interface
DECNet	Digital Equipment Corporation Network
TPM	Trusted Platform Module
ESP	Encapsulating Security Payload
AH	Authentication Header
IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
SAD	Security Association Database
SPD	Security Policy Database
SPI	Security Parameter Index
IPcomp	IP Protocol Compression
MOBIKE	IKEv2 Mobility and Multihoming Protocol

Popis slika

Ispis

1. Uvod

Problem sigurne komunikacije na Internetu već dulje vrijeme predstavlja veliki izazov na području računarskih znanosti. Izgrađeni i predstavljeni sigurnosni principi zahtijevaju visoki stupanj funkcionalnosti i fleksibilnosti prilikom njihove upotrebe. U današnjem svijetu, sigurnost na Internetu ostvarena je upotrebom IPsec arhitekture koja predstavlja *de-facto* standard. IPsec arhitektura omogućava zaštitu dijeljene informacije između sudionika na mrežnom sloju OSI modela. Sigurnosni mehanizmi koje pruža IPsec arhitektura u potpunosti su implementirani u jezgri operativnog sustava (eng. *kernel space*) na razini mrežnog sloja OSI modela. Navedeni mehanizmi osiguravaju zaštitu protokolima višeg sloja TCP (eng. *Transmision Control Protocol*) i UDP (eng. *User Datagram Protocol*) koje IP (eng. *Internet Protocol*) protokol prenosi.

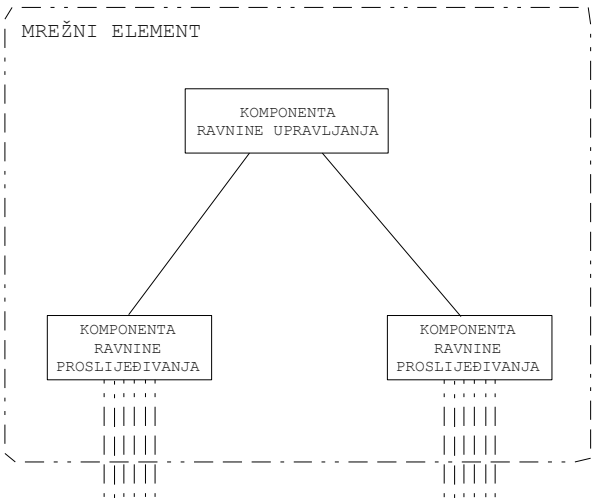
Upotreba protokola za razmjenu ključeva u sprezi s IPsec arhitekturom, podiže razinu sigurnosti i osigurava jednostavnost upotrebe. Implementacija protokola za razmjenu ključeva kao upravljački mehanizam IPsec arhitekture nalazi se smješten u korisničkoj okolini (eng. *user space*).

Prenosivost i međusobna inteoperabilnost implementacija protokola za razmjenu ključeva i IPsec arhitektura u različitim operacijskim sustavima predstavlja ključnu stvar za široku upotrebu IPsec protokola. IETF (*Internet Engineering Task Force*) standardizacijsko tijelo kroz niz napisanih RFC dokumenata pokušava unificirati i standardizirati protokole povezivanja u različitim sigurnosnim domenama. U Linux okruženju povezivanje entiteta domene upravljanja s modulima u jezgri operativnog sustava ostvareno je upotrebom Netlink sustava i pripadajućeg protokola.

Predmet promatranja ovog diplomskog rada je područje Netlink protokola i njegova primjena u okruženju implementacije protokola za razmjenu ključeva. U radu se teorijski razmatra Netlink protokol i usluga za zaštitu IP protokola. Praktičan dio sastoji se od implementacije Netlink sustava za pristup sigurnosnim bazama unutar jezgre operativnog sustava Linux.

2. Odvajanje ravnina upravljanja i proslijeđivanja

Računalna komunikacijska mreža sastavljena je od više međusobno povezanih mrežnih elemenata. Pojedini mrežni elementi (eng. *network element*) sastoje se od više odvojenih logičkih entiteta. Dva osnovna entiteta koji čine mrežni element su komponente ravnine upravljanja (eng. *control plane*) i komponente ravnine proslijeđivanja (eng. *forwarding plane*). Navedeni entiteti međusobno usko surađuju radi ostvarenja određene usluge. Suradnja tih entiteta ostvarena je upotrebom protokola kojim komponente međusobno komuniciraju. Slika 2.1. prikazuje pojednostavljeni prikaz arhitekture mrežnog elementa s komponentama ravnine upravljanja i proslijeđivanja.



Slika 2.1. Odvajanje ravnine upravljanja i proslijeđivanja

IETF radna grupa pod nazivom *Forces* (eng. *Forwarding and Control Element Separation*) obavlja radnje za standardizaciju protokola kojim navedene ravnine komuniciraju. Standardizacija protokola omogućava povećanu skalabilnost te međusobnu neovisnost ravnina između različitih mrežnih elemenata. Koncept odvajanja ravnine upravljanja i ravnine proslijeđivanja originalno nazvan "*IP Service control-forwarding separation*" [1] ranih 90-tih predstavila je *Computer Systems Research* grupa s sveučilišta *Berkeley* u sklopu implementacije BSD (*Berkeley Software Distribution*) 4.4 *socket* sučelja.

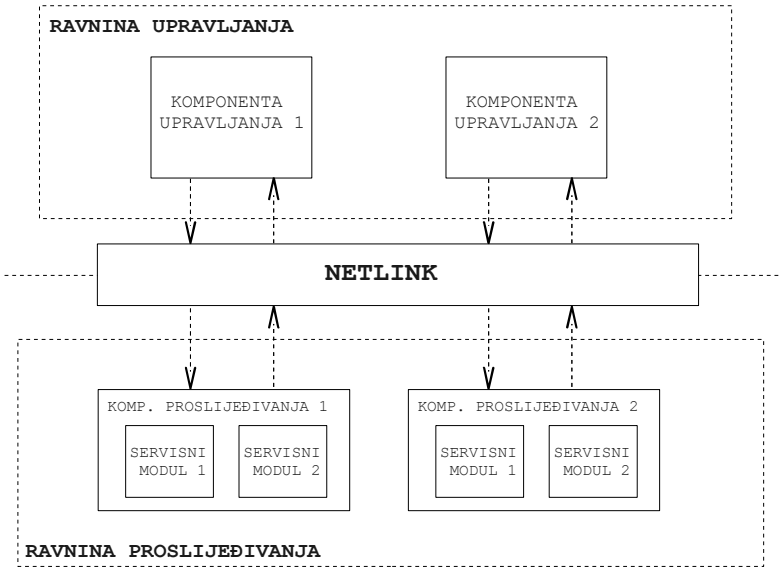
Osnovna zamisao koncepta odnosila se na odvajanje ravnine upravljanja i ravnine proslijeđivanja u IPv4 usmjeravanju opisanog u [2]. Prilikom proslijeđivanja mrežnih paketa, usmjernici konzultiraju tablicu proslijeđivanja (eng. *forwarding table*) koja je smještena u jezgrenoj domeni. Administrator upotrebom alata iz korisničke domene obavlja statičko ili dinamičko namještanje zapisa u tablicu proslijeđivanja. Navedeni entiteti nalaze se u dvije različite sigurnosne domene, korisničkoj i jezgrenoj. Upotrebom protokola koji povezuje navedene entitete omogućena je međusobna efikasna i sigurna

komunikacija. Komunikacija između komponenata ravnine upravljanja i ravnine proslijeđivanja definira IP uslugu (eng. *IP service*).

2.1. Arhitektura

Linux operacijski sustav od svojih ranih početaka u potpunosti se oslanja na predstavljeni koncept. U svrhu povezivanja ravnine upravljanja i proslijeđivanja, definiran je i implementiran Netlink sustav opisan u [3]. Netlink sustav sastoji se od protokola za komunikaciju između komponenata te programskog sučelja (eng. *Application Programming Interface – API*) za korištenje Netlink usluga.

Elementi koji čine arhitekturu Netlink sustava su ravnina upravljanja (eng. *Control Plane – CP*) i ravnina proslijeđivanja (eng. *Forwarding Engine – FE*). Svaka od ravnina može sadržavati više različitih komponenata koje obavljaju specifične operacije. Interakcija između komponenata ravnine upravljanja i modula proslijeđivanja definira Netlink IP uslugu. IP usluga opisuje način na koji se tretiraju mrežni paketi prilikom prolaska kroz različite podsustave mrežnog stoga (sigurnosna stijena, QoS modul, IPsec modul). Svaki od navedenih podsustava u Netlink okruženju, opisujemo kao mrežni element (eng. *Network Element – NE*). Slika 2.2. prikazuje arhitekturu Netlink sustava u Linux operacijskom sustavu.



Slika 2.2. Arhitektura Netlink sustava

Osnovni elementi koji čine arhitekturu Netlink sustava su:

- ravnina upravljanja

  Ravnina upravljanja pozicionirana je u korisničkoj domeni i njezina je temeljna funkcija upravljanje i nadzor određene Netlink IP usluge. Sastoji se od više različitih komponenata upravljanja (eng. *Control Plane Component – CPC*), od

kojih svaka predstavlja mehanizam upravljanja za različitu IP uslugu koju obavlja jedna ili više komponenti ravnine proslijeđivanja. Komponente ravnine upravljanja obuhvaćaju signalizacijske protokole, protokole upravljanja i nadzora.

- ravnina proslijeđivanja

  Ravnina proslijeđivanja smještena je u jezgrenoj domeni operacijskog sustava i obuhvaća pakete koji dolaze s mreže. Osnovna funkcija ravnine proslijeđivanja predstavlja obavljanje upravljačkih naredbi dobivenih od ravnine upravljanja. Upravljačke naredbe predstavljaju specifične transformacije koje ravnine proslijeđivanja obavlja nad paketima. Ravnine proslijeđivanja sastoji se od više različitih komponenti proslijeđivanja (eng. *Forwarding Engine Component – FEC*). Različite usluge koriste različite komponente proslijeđivanja. Unutar pojedine komponente nalazi se jedan ili više servisnih modula (eng. *service module*) koji obavljaju potrebno procesiranje nad mrežnim paketima. U slučaju da komponenta sadrži više servisnih modula, svaki od njih obavlja specifične operacije. Metoda ulančavanja više servisnih modula predstavlja složeniju IP uslugu. Ovakav princip specifičan je za Linux model ravnine proslijeđivanja.

Svrha ravnine upravljanja je osiguranje okruženja za prethodno navedene aktivnosti s krajnjim ciljem upravljanja i konfiguracije druge komponente mrežnog elementa, odnosno komponente modula proslijeđivanja. Rezultat konfiguracije definira način procesiranja paketa koji prolaze određenu komponentu ravnine proslijeđivanja. Interakcija između ravnine upravljanja i proslijeđivanja u Netlink kontekstu definira IP uslugu. Protokol upravljanja komponenata ravnine proslijeđivanja definiran je upotrebom predložaka (eng. *templates*) specifičnih za IP uslugu.

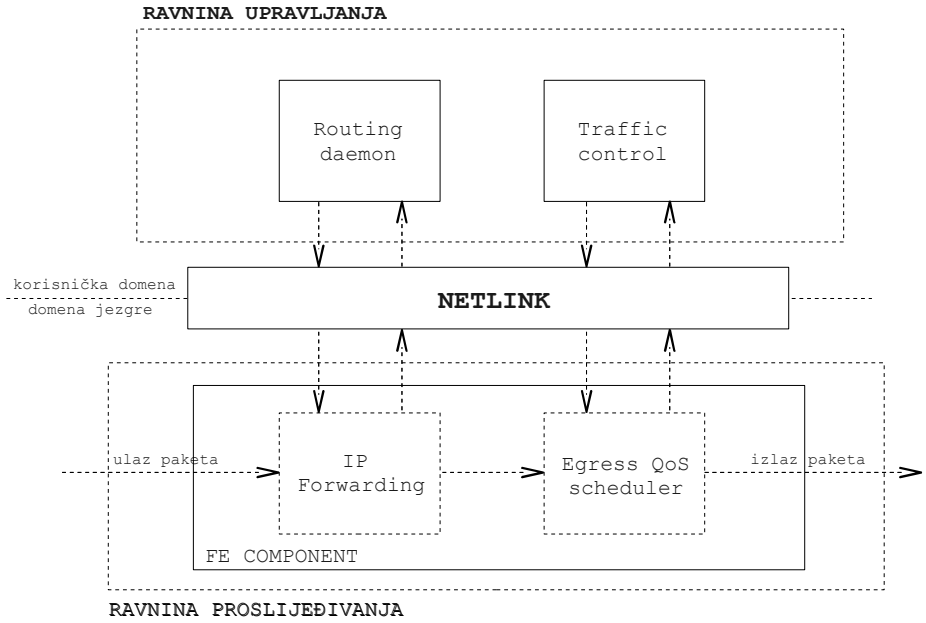
Sa sigurnosnog stajališta, ovakav dizajn mrežnog elemenata dodatno povećava sigurnost i dostupnost elementa budući eventualne kompromitacije komponenata ravnine upravljanja ne narušavaju ispravan rad komponenta ravnine proslijeđivanja. Upravo su komponente ravnine upravljanja te koje su izložene te predstavljaju potencijalne sigurnosne probleme za mrežne elemente.

Od prvih početaka implementacije Netlink sustava, Linux podiže originalni BSD koncept na višu razinu te dozvoljava apstrakciju koncepta IP usluge. Pod apstrakcijom IP usluge razmatra se upotreba Netlink protokola za potrebe komunikacije između komponenata koje ne obavljaju usluge specifične za računalnu mrežu. U nastavku je opisana usluga IP proslijeđivanja.

2.2. Usluga IP proslijeđivanja

Najzastupljeniji mrežni element specifične namjene na Internetu je usmjernik (eng. *router*). Temeljna funkcija usmjernika je proslijeđivanje mrežnih paketa na mrežnom sloju OSI modela.

Primjer na slici 2.3. definira Netlink IP uslugu klasičnog IP proslijeđivanja paketa s primjenom jednostavnih QoS (eng. *Quality of Service*) pravila na izlazu paketa iz mrežnog elementa. Opisani entiteti i funkcije mrežnog elementa zajedno predstavljaju osnovni usmjernik.



Slika 2.3. Primjer Netlink usluge IP proslijeđivanja

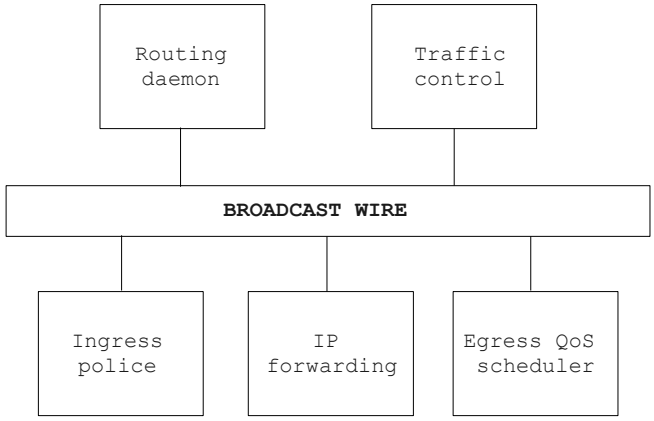
Ravnina upravljanja sastoji se od dvije komponente, koje predstavljaju implementaciju protokola usmjeravanja i kontrolni alat za definiciju QoS pravila. Ravnina proslijeđivanja sadrži jednu komponentu sastavljenu od dva servisna modula, modula IP proslijeđivanja i QoS raspoređivača (eng. *QoS scheduler*) paketa. Komponenta upravljanja koju predstavlja implementacija protokola usmjeravanja, obavlja potrebne modifikacije u tablici proslijeđivanja. Obično se radi o specifičnoj implementaciji algoritama usmjeravanja (eng. *routing algorithms*) kao što su OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*) ili BGP (*Border Gateway Protocol*) protokoli. Komponenta TC (*Traffic Control*) ravnine upravljanja definira i upravlja QoS pravilima koja se primjenjuju prilikom izlaza paketa iz mrežnog elementa. Ovakav dizajn predstavlja ulančavanje servisnih modula komponente ravnine proslijeđivanja za ostvarenje složene IP usluge.

U slučaju ispada pojedinih veza usmjernika, ravnina proslijeđivanja asinkronim događajem obavještava ravninu upravljanja o navedenim promjenama. Takvi slučajevi uzrokuju promjenu mrežne topologije. Komponente ravnine upravljanja koje implementiraju algoritme usmjeravanja obavljaju potrebne operacije i izračune pogodnog puta (eng. *best path*) te spremaju trenutno stanje o mreži u tablicu usmjeravanja (eng. *routing information base*). Tablica usmjeravanja nalazi se u domeni ravnine upravljanja te se pomoću nje gradi tablica proslijeđivanja. Nužno je da komponenta koja implementira algoritam usmjeravanja obavijesti ravninu proslijeđivanja o navedenim promjenama.

U današnje vrijeme tehnologija mreže je uvelike napredovala, pa je neophodno dodati nove IP usluge u usmjerivače kako bi se zadovoljili trenutni zahtjevi tržišta. Netlink sustav posjeduje složenije usluge koje proširuju standardnu uslugu IP prosljeđivanja. Navedene usluge razmatraju pakete i njihova zaglavlja na mrežnom i višim slojevima ISO/OSI modela.

2.2.1. Logički prikaz IP usluge

Komponente ravnine upravljanja i prosljeđivanja logički su modelirane kao više računala spojenih na mrežni segment. Mrežni segment jedinstven je za IP uslugu. Komponente međusobno razmjenjuju poruke upotrebom Netlink protokola koji omogućava isporuku Netlink poruka *unicast-om* (eng. *unicast*), difuzijom (eng. *broadcast*) i difuzijom u grupi (eng. *multicast*). Slika 2.4. prikazuje logički model usluge IP prosljeđivanja.



Slika 2.4. Logički prikaz Netlink IP usluge

Za ostvarenje komunikacije, komponente ravnine upravljanja obavljaju registraciju za specifičnu IP uslugu. Nakon registracije na IP uslugu komponente mogu slati upravljačke naredbe te primati asinkrone događaje od komponenata ravnine prosljeđivanja. Nije nužno da sve komponente šalju poruke prema ravnini prosljeđivanja. U tom slučaju specifična komponenta ravnine upravljanja obavlja registraciju na način da samo osluškuje poruke koje se odašilju na segmentu za navedenu uslugu. Takva komponenta predstavlja nadzorni element IP usluge. Prilikom komunikacije, poruke koje se razmjenjuju moraju biti ispravne, u protivnom, Netlink sustav takve poruke odbacuje te šalje poruku o grešci komponenti koja je neispravnu poruku odaslala. Ostalim komponentama koje osluškuju na segmentu odbačene poruke nisu vidljive.

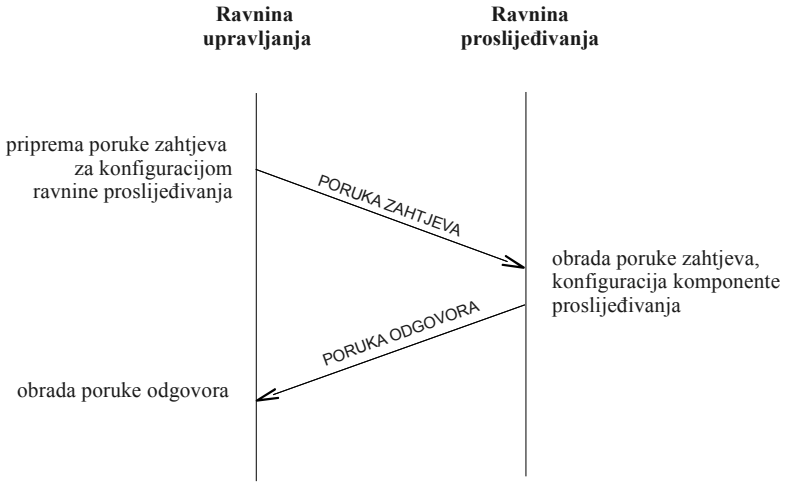
Navedeni primjer predstavlja uslugu IP prosljeđivanja s jednostavnom ravninom upravljanja. U kompleksnijim slučajevima određene komponente ravnine upravljanja mogu obaviti registraciju na više različitih segmenata te tako upravljati komponentama prosljeđivanja za više različitih IP usluga. Jednako tako, više različitih komponenata ravnine upravljanja može upravljati istom IP uslugom. U tom slučaju, ravnina

proslijeđivanja šalje obavijesti svim komponentama koje su registrirane za dotičnu IP uslugu. Na ovaj način održava se konzistentno stanje ravnine proslijeđivanja.

2.3. Netlink protokol

Netlink sustav u Linux operacijskom sustavu upotrebom Netlink protokola nudi fleksibilnu i robusnu okolinu za komunikaciju između komponenata ravnine upravljanja i ravnine proslijeđivanja.

Komunikacija između ravnine upravljanja i proslijeđivanja omogućena je u oba smjera. Razmjenu poruka obično započinje komponenta ravnine upravljanja koja odašilje zahtjev za konfiguracijom (eng. *NEW request*) ravnine proslijeđivanja ili zahtjev za dohvaćanjem postojeće konfiguracije (eng. *GET request*) komponente ravnine proslijeđivanja. Jednako tako, razmjenu poruka može započeti komponenta ravnine proslijeđivanja slanjem asinkronih događaja (eng. *asynchronous events*) s ciljem obavještavanja ravnine upravljanja o promjenama stanja pojedine komponente ravnine proslijeđivanja. Slika 2.5. prikazuje razmjenu poruka prilikom zahtijeva za konfiguracijom ravnine proslijeđivanja.



Slika 2.5. Razmjena poruka u Netlink protokolu

Netlink protokol po svom je radu vrlo sličan UDP (eng. *User Datagram Protocol*) protokolu te spada u bespojni (eng. *connectionless*) tip usluge. Osnovna karakteristika bespojnog tipa usluge je negarantirana isporuka poruka i ne sačuvan redoslijed isporuke.

Netlink protokol nudi vrlo jednostavan, ali učinkovit mehanizam potvrde primitka poruke (eng. *message acknowledge*) pomoću kojeg komponente ravnine upravljanja mogu ustanoviti je li isporuka obavljena uspješno. Slijedni brojevi (eng. *sequence numbers*) iz poruka potvrde mogu poslužiti za praćenje redoslijeda isporuke poruka. Upotrebom navedenih mehanizama Netlink sustav programeru daje mogućnost izrade spojnog tipa usluge kombinacijom slijednih brojeva, poruka potvrde te upotrebom internih *retransmit timere* jezgre operativnog sustava. Upotrebom specijalnih poruka programer može ostvariti protokol za praćenje stanja (eng. *Heartbeat protocol*) pojedinih komponenata ravnine

prosljeđivanja. Netlink protokol može se upotrijebiti i za komunikaciju između više različitih komponenata ravnine upravljanja te tako poslužiti kao vrlo moćan mehanizam za međuprocesnu komunikaciju (eng. *Inter Process Communication – IPC*).

Ravnina upravljanja i prosljeđivanja obično se nalaze u sklopu istog mrežnog elementa što ne mora biti pravilo. Ravnina upravljanja jednog mrežnog elementa može upravljati komponentama ravnine prosljeđivanja sasvim drugog mrežnog elementa. U tom smislu potrebno je obaviti enkapsulaciju Netlink poruka u neki od transportnih protokola. Transportnim protokolom omogućava se adresiranje drugog mrežnog elementa i prijenos poruka upravljanja na ravninu prosljeđivanja drugog mrežnog elementa.

U nastavku su prikazani formati Netlink poruka te su opisana polja poruka koja se razmjenjuju u Netlink protokolu.

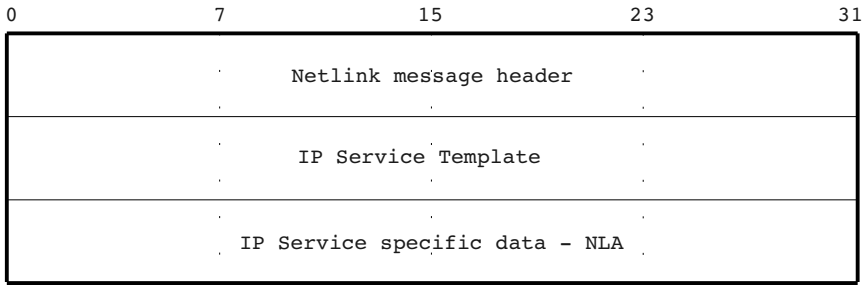
2.3.1. Format Netlink poruke

Netlink protokol definira poruke koje se sastoje od Netlink zaglavlja te pridruženim teretom. Ukoliko je teret veći od raspoloživog mjesta u jednoj poruci teret se može razdijeliti na više Netlink poruka.

U Netlink protokolu razlikujemo tri različite vrste poruka:

- poruke upravljanja (eng. *control messages*) iz smjera ravnine upravljanja prema ravnini prosljeđivanja. Poruke predstavljaju zahtjev za konfiguracijom ili zahtjev za dohvaćanjem konfiguracije ravnine prosljeđivanja.
- poruke obavijesti o asinkronim događajima (eng. *asynchronous event messages*) iz smjera ravnine prosljeđivanja prema ravnini upravljanja.
- poruke obavijesti o greškama (eng. *error messages*) iz smjera ravnine prosljeđivanja prema ravnini upravljanja

Ispravno formatirana Netlink poruka sadrži jedinstveno zaglavlje i teret specifičan za IP uslugu. Teret poruke definiran je poljima *IP Service template* i *IP Service specific data*. Slika 2.6. prikazuje format Netlink poruke.



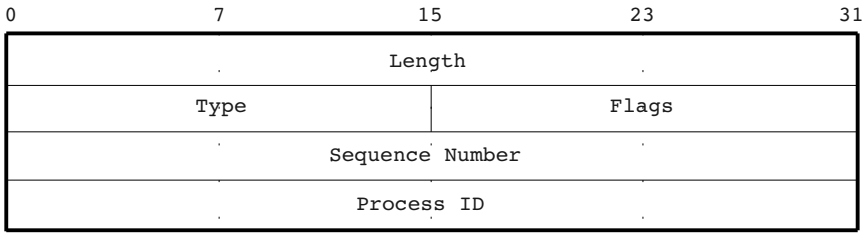
Slika 2.6. Format Netlink poruke

U slijedećim poglavljima detaljno je objašnjeno svako polje Netlink poruke te ostali tipovi poruka.

2.3.2. Zaglavlje poruke

Zaglavlje Netlink poruke nalazi se ispred tereta koji se prenosi između sugovornika. Od programera se očekuje da eksplicitno postavi zaglavlje prilikom kreiranja Netlink poruke, što nije nužno ukoliko se koriste usluge ostalih mrežnih protokola.

Slika 2.7. prikazuje format zaglavlja Netlink poruke. Netlink zaglavlje sadrži informaciju o veličini Netlink poruke u oktetima. Upotrebom informacije u polju `Type` komponente ravnine proslijeđivanja, razlikuju dolazne poruke i obavljaju demultipleksiranje poruka prema određenim servisnim modulima. Pojedina IP usluga definira i opisuje raspoložive tipove poruka. Polje `Flags`, informira ravninu proslijeđivanja o načinu na koji je potrebno obraditi poruku. Komponenta ravnine upravljanja prilikom slanja poruka zahtjeva, mora postaviti `Process ID` član na vrijednost proces identifikatora. Vrijednost proces identifikatora, komponente ravnine upravljanja dobivaju *`getpid()`* pozivom. Upotreba `Process ID` člana od velikog je značaja prilikom difuzije u grupi kada je član neophodan za korelaciju poruka.

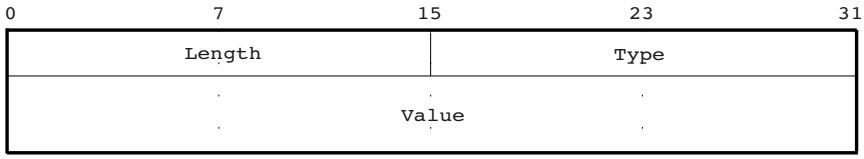


Slika 2.7. Format zaglavlja Netlink poruke

Ukoliko je teret veći od raspoloživog prostora u Netlink poruci, teret se postavlja u dijelovima (eng. *fragments*) u više uzastopnih Netlink poruka (eng. *multipart messages*). Rezultat takve podjele je niz Netlink poruka od kojih svaka sadrži zasebno Netlink zaglavlje. Prva i sve slijedeće poruke, u Netlink zaglavlju imaju postavljenu NLM_F_MULTI zastavicu koja predstavlja *multipart* poruku. Zadnja poruka u Netlink zaglavlju za tip poruke ima postavljenu vrijednost NLMSG_DONE pomoću koje se označava kraj *multipart* poruke.

2.3.3. Teret poruke

Polja *IP Service Template i IP service specific data* prikazani na slici 2.6. predstavljaju teret Netlink poruke. *IP Service Template* polje je obvezatno i predstavlja predložak poruke zahtjeva. IP usluga koja koristi Netlink protokol, točno opisuje format ovog polja. Detaljnije objašnjenje formata polja *IP Service Template* nalazi se u nastavku teksta za Netlink uslugu zaštite IP protokola. *IP service specific data* polje predstavlja dodatni teret (eng. *parametrization data*). Dodatni teret unosi se u obliku Netlink atributa (eng. *Netlink Attribute – NLA*). Slika 2.8. prikazuje format polja poruke koji predstavlja Netlink atribut.



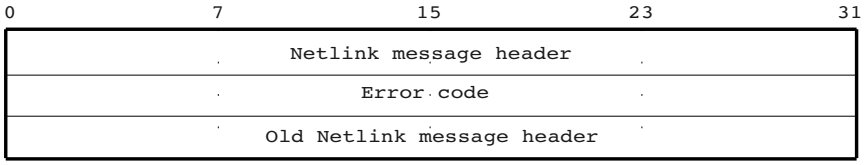
Slika 2.8. Format zaglavlja Netlink atributa

Netlink atribut predstavlja dodatni teret za pojedine poruke IP usluge. Netlink atribut predstavljen je TLV (*Type Length Value*) zapisom. Svaki zapis sadrži tip `Type` i duljinu tereta `Length` i proizvoljnu duljinu tereta `Value`. Ukoliko Netlink poruka zahtijeva više Netlink atributa, postavlja se više TLV zapisa u TLV polje.

2.3.4. Poruka greške

Neispravan format Netlink poruka u komunikaciji između komponenata upravljanja i prosljeđivanja uzrokuju grešku. Upotrebom poruke greške ravnina prosljeđivanja obavještava komponente upravljanja.

Tip poruke greške također sadrži prethodno objašnjeno Netlink zaglavlje uz postavljeno polje `Type` na NLMSG_ERROR vrijednost. Slika 2.9. prikazuje format poruke koja predstavlja NLMSG_ERROR tip poruke.



Slika 2.9. Format Netlink poruke greške

Navedeni tip poruke ne predstavlja samo poruku greške nego se tip poruke greške koristi i prilikom poruka potvrde primitka. Poruka sadrži `Error code` polje pomoću kojeg komponenta upravljanja može razlučiti o kojem tipu poruke se radi, poruci greške ili poruci potvrde primitka.

Ukoliko je vrijednost `Error code` polja različito od nule, poruka predstavlja poruku greške ili negativnu potvrdu (eng. *negative acknowledge message*). Takvom porukom, ravnina prosljeđivanja signalizira komponenti ravnine upravljanja pogrešku u komunikaciji. Zaglavlje originalne neispravne poruke sadržano je kao teret poruke greške.

U slučaju da je `Error code` polje postavljeno na vrijednost nula, poruka predstavlja poruku potvrde primitka (eng. *acknowledge message*) ispravne Netlink poruke. Komponenta ravnine upravljanja upotrebom slijednih brojeva iz zaglavlja poruke potvrde primitka može obaviti usporedbu s već odaslanim porukama, te potvrditi primitak poruke. Dodatno, poruka potvrde sadrži i originalno Netlink zaglavlje.

3. Linux Netlink sučelje

Linux Netlink sučelje omogućava programeru korištenje usluga Netlink sustava. Temeljna operacija Netlink protokola je povezivanje ravnine upravljanja s ravninom proslijeđivanja. Koristeći Netlink sučelje, komponente ravnine upravljanja obavljaju razmjenu podataka s različitim modulima u jezgri operativnog sustava, koji implementiraju komponente ravnine proslijeđivanja.

Razmjena podataka između navedenih ravnina u Linux okruženju omogućena je na više različitih načina. Upotrebom sistemskih poziva (eng. *system calls*), `ioctl` (eng. *input/output control*) poziva ili koristeći `procfs` (eng. *process file system*) pseudo datotečni sustav, moguće je ostvariti razmjenu podataka s modulima u jezgri. Navedeni mehanizmi nisu jednostavni za korištenje i implementaciju te imaju niz nedostataka u usporedbi s Netlink sustavom i pripadajućim protokolom.

Prednost Netlink sustava pred predstavljenim mehanizmima je ostvarenje vrlo fleksibilnog protokola za komunikaciju s ravninom proslijeđivanja upotrebom standardnog BSD *socket* sučelja. U radu s Netlink pristupnom točkom koriste se standardni i dobro poznati sistemski pozivi za slanje i primitak poruka što olakšava razvoj i povećava samu produktivnost programera. Dodatno, implementacija Netlink sustava zahtjeva minimalne modifikacije na programskoj podršci za pristup postojećoj Netlink usluzi.

Netlink sustav u potpunosti nudi upravljački pristup mrežnom dijelu Linux jezgre. Upotrebom Netlink sustava omogućava pristup različitim podsustavima Linux jezgre koji ne pripadaju mrežnim protokolima. Ovime Netlink sustav proširuje originalni koncept te uvodi pojam apstrakcije IP usluge.

Raspoložive porodice protokola Netlink sustava u trenutno stabilnoj verziji Linux 2.6.30.1 jezgre definirane su u zaglavnoj datoteci `</usr/include/linux/netlink.h>`:

- NETLINK_ROUTE – porodica omogućava pristup i modifikaciju IPv4 i IPv6 tablica proslijeđivanja, adresa i parametara mrežnog sučelja, QoS sustava i raspoređivača mrežnih paketa
- NETLINK_UNUSED – porodica nema upotrebu
- NETLINK_USERSOCK – porodica omogućava pristup korisničkom *socket* sučelju
- NETLINK_FIREWALL – porodica omogućava prijenos IP paketa s Linux Netfilter podsustava u korisničku okolinu
- NETLINK_INET_DIAG – porodica omogućava nadzor INET socket sučelja
- NETLINK_NFLOG – porodica omogućava prijenos bilježenje i prijenos zapisa Linux Netfilter podsustava u korisničku okolinu za ULOG sustav

- NETLINK_XFRM – porodica omogućava pristup sigurnosnim bazama IPsec podsustava
- NETLINK_SELINUX – porodica omogućava prijenos SELinux događaja u korisničku okolinu
- NETLINK_ISCSI – porodica omogućava upravljački pristup Open-ISCSI podsustavu
- NETLINK_AUDIT – porodica omogućava bilježenje i prijenos događaja unutar jezgre u korisničku okolinu
- NETLINK_FIB_LOOKUP – porodica omogućava pregled tablice proslijeđivanja
- NETLINK_CONNECTOR – porodica omogućava povezivanje različitih agenata
- NETLINK_NETFILTER – porodica omogućava upravljački pristup Linux Netfilter podsustavu
- NETLINK_IP6_FW – porodica omogućava prijenos IPv6 paketa s Linux Netfilter podsustava u korisničku okolinu
- NETLINK_DNRTMSG – porodica omogućava primitak događaja od DECNet podsustava za proslijeđivanje mrežnih paketa
- NETLINK_KOBJECT_UEVENT – porodica omogućava prijenos i bilježenje događaja jezgre operativnog sustava
- NETLINK_GENERIC – porodica nudi općenito Netlink sučelje upotrebom kojeg korisnik može definirati specifičan protokol za povezivanje ravnine upravljanja i proslijeđivanja
- NETLINK_SCSITRANSPORT – porodica omogućava primitak asinkronih događaja od SCSI transport modula
- NETLINK_ENCRYPTFS – porodica omogućava TPM (eng. *Trusted Platform Module*) komponenti upravljanja pristup na kriptografski sloj datotečnog sustava (eng. *cryptographic filesystem*)

Implementacija Netlink sučelja sastoji se od dva osnovna dijela; standardnog BSD *socket* sučelja za korisničku okolinu i internog sučelja u jezgri. Implementacija koji se odnosi na korisničku okolinu opisana je unutar zaglavne datoteke `<linux/netlink.h>` s pripadajućim podatkovnim strukturama i pomoćnim funkcijama. Interno sučelje u jezgri koriste različiti moduli u jezgri operativnog sustava koji predstavljaju komponente ravnine proslijeđivanja. Implementacija internog sučelja nalazi se u izvornom kôdu jezgre u datoteci `<net/af_netlink.c>` dok se deklaracija i pomoćne funkcije nalaze u zaglavnoj datoteci `<include/net/netlink.h>`.

Implementacija modernih mrežnih alata Linux operativnog sustava u ravnini upravljanja uglavnom koristi usluge Netlink sučelja za pristup mrežnim komponentama ravnine proslijeđivanja. Jedan od poznatijih mrežnih alata koji upravo koristi Netlink sučelje za manipulaciju mrežnih postavki je `iproute` alat. Upotreba `iproute` alata administratoru daje mogućnost obavljanja konfiguracije mrežnih sučelja, održavanja stanja tablice proslijeđivanja, kreiranje i održavanje logičkih tunel sučelja te manipulaciju zapisa u IPsec sigurnosnim bazama.

U sklopu diplomskog rada razmatra se Netlink sustav i protokol za komunikaciju između ravnina mrežnog elementa. Netlink sučelje za pristup Netlink uslugama razmatra se s gledišta ravnine upravljanja. Sukladno tome u nastavku se razmatraju podatkovne strukture i operacije potrebne za rad s Netlink sučeljem iz ravnine upravljanja.

3.1. Podatkovne strukture

Korištenje Netlink sučelja od strane programera podrazumijeva ispravno shvaćanje osnovnih podatkovnih struktura Netlink sučelja. Navedene strukture opisuju različite objekte Netlink sustava. U nastavku slijedi pregled podatkovnih struktura koje se upotrebljavaju prilikom rada s Netlink sučeljem zajedno s detaljnim objašnjenjima članova struktura.

3.1.1. Adresna podatkovna struktura

Podatkovna struktura `sockaddr_nl` jedinstveno opisuje Netlink klijenta kojem se šalju poruke. Netlink klijent može biti komponenta ravnine upravljanja ili ravnine proslijeđivanja.

```
struct sockaddr_nl
{
        sa_family_t     nl_family;
        unsigned short  nl_pad;
        __u32           nl_pid;
        __u32           nl_groups;
};
```

Ispis 1. Podatkovna struktura sockaddr_nl

Podatkovna struktura `sockaddr_nl` sadrži slijedeće članove:

- `nl_family`

  Član strukture označava grupu komunikacijskih usluga koju odašiljemo putem Netlink spojne točke. Obavezno je postaviti član na vrijednost `AF_NETLINK`.

- `nl_pad`

  Član strukture nema posebno značenje, te se u pravilu ne koristi. Obično se postavlja na vrijednost nule.

- `nl_pid`

  Član strukture predstavlja adresu Netlink pristupne točke. Ukoliko je primatelj poruke pristupne točke u jezgri tada je vrijednost potrebno postaviti na nulu. Od komponenata upravljanja očekuje se postavljanje jedinstvene vrijednosti ovog člana iako komponente interno mogu sadržavati više različitih pristupnih točaka.

- `nl_groups`

  Član strukture opisuje grupe prema kojima se odašilju poruke. Svaka IP usluga raspolaže s 32 grupe koje služe za difuziju poruka u grupi (eng. *multicast*). U slučaju primitka poruka potrebno je postaviti član na vrijednosti grupa za koje želimo primiti poruke. U slučaju da je vrijednost postavljena nulu tada se poruka šalje isključivo jednom primatelju (eng. *unicast*).

Tip `sockaddr_nl` podatkovne strukture mijenja se na standardnu adresnu strukturu `sockaddr` te se navedena struktura prosljeđuje prilikom svakog poziva funkcije primanja ili slanja na Netlink spojnoj točci.

3.1.2. Podatkovna struktura zaglavlja Netlink poruke

Podatkovna struktura `nlmsghdr` predstavlja zaglavlje Netlink poruke. Ispravan format Netlink poruke zahtijeva postavljanje Netlink zaglavlja. Podatkovnu strukturu potrebno je postaviti na početak memorijskog prostora koje predstavlja poruku zahtjeva.

```
struct nlmsghdr
{
        __u32           nlmsg_len;
        __u16           nlmsg_type;
        __u16           nlmsg_flags;
        __u32           nlmsg_seq;
        __u32           nlmsg_pid;
};
```

Ispis 2. Podatkovna struktura nlmsgdhr

Podatkovna struktura `nlmsghdr` ima slijedeće članove:

- `nlmsg_len`

  Član strukture označava veličinu Netlink poruke u oktetima. Veličina se odnosi na teret Netlink poruke zajedno s zaglavljem.

- `nlmsg_type`

  Član strukture označava tip Netlink poruke. Tip poruke posebno je opisan za svaku Netlink IP uslugu. U posebnim slučajevima neovisno o IP usluzi član može poprimiti i slijedeće vrijednosti:

  - NLMSG_NOOP – ovaj tip poruke je potrebno ignorirati

- NLMSG_ERROR – ovaj tip poruke signalizira ravnini upravljanja da je došlo do pogreške. Tip poruke predstavlja negativnu potvrdu (eng. *negative acknowledge*) prilikom konfiguracije ravnine proslijeđivanja. teret poruke sadrži `nlmsgerr` podatkovnu strukturu iz koje se može detaljnije saznati uzrok pogreške. Dodatno se navedeni tip upotrebljava za pozitivnu potvrdu primitka poruke.
- NLMSG_DONE – ovaj tip poruke terminira više uzastopnih *multipart* poruka.

• `nlmsg_flags`

Član strukture predstavlja Netlink zastavice koje definiraju način na koji su poruke procesirane i interpretirane od strane primatelja. Standardne Netlink zastavice su:

- NLM_F_REQUEST – potrebno postaviti na svim porukama zahtjeva
- NLM_F_MULTI – zastavica govori da je poruka dio *multipart* Netlink poruke i da će biti *multipart* poruka biti završena porukom koja ima postavljenu zastavicu NLMSG_DONE
- NLM_F_ACK – zastavicom ravnina upravljanja traži potvrdu primitka za sve odaslane poruke prema komponentama ravnine proslijeđivanja
- NLM_F_ECHO – zastavicom ravnina upravljanja traži da se sve odaslane poruke prema komponentama ravnine proslijeđivanja vrate prema ravnini upravljanja u originalnom obliku

Dodatne i opcionalne zastavice za sve poruke zahtjeva za dohvaćanjem konfiguracije ravnine proslijeđivanja od strane ravnine upravljanja su:

- NLM_F_ROOT – ravnina upravljanja izričito zahtjeva odgovor u obliku polja podataka, a ne jednostruki odgovor.
- NLM_F_MATCH – vratiti sve objekte koji zadovoljavaju navedeni kriterij
- NLM_F_ATOMIC – obaviti *atomic* operaciju vraćanja svih objekata koji zadovoljavaju navedeni kriterij uz upotrebu *lock-a*

Dodatne zastavice za sve poruke zahtjeva za konfiguraciju ravnine proslijeđivanja tj. za dodavanje novog objekta prema ravnini proslijeđivanja su:

- NLM_F_REPLACE – obaviti zamjenu postojećeg objekta ako postoji s trenutno primljenim
- NLM_F_EXCL – ne obaviti zamjenu postojećeg objekta s trenutno primljenim
- NLM_F_CREATE – potrebno alocirati prostor za novi objekt ukoliko identičan objekt ne postoji

- NLM_F_APPEND – dodati trenutno primljeni objekt na kraj liste prisutnih objekata

- `nlmsg_seq`

  Član strukture predstavlja slijedni broj poruke i upotrebljava se za korelaciju primljenih poruka odgovora s poslanim porukama zahtjeva od strane ravnine upravljanja.

- `nlmsg_pid`

  Član strukture predstavlja proces identifikator. Upotreba člana je vrlo slična kao i prethodnog.

3.1.3. Podatkovna struktura zaglavlja Netlink atributa

Podatkovna struktura `nlattr` predstavlja zaglavlje Netlink atributa. Ispravan format Netlink atributa zahtijeva postavljanje `nlattr` zaglavlja. Podatkovnu strukturu potrebno je postaviti na početak memorijskog prostora koje predstavlja Netlink TLV atribut.

```
struct nlattr
{
        __u16           nla_len;
        __u16           nla_type;
};
```

Ispis 3. Podatkovna struktura nlattr

Podatkovna struktura ima slijedeće članove:

- `nla_len`

  Član strukture predstavlja duljinu teret koji se prenosi u zapisu Netlink atributa.

- `nla_type`

  Član strukture predstavlja tip atributa koji se prenosi. Tipovi atributa su specifični za IP uslugu.

3.1.4. Podatkovna struktura zaglavlja poruke greške

Podatkovna struktura `nlmsgerr` predstavlja teret poruke greške ili poruke potvrde primitka.

```
struct nlmsgerr
{
        int             error;
        struct nlmsghdr msg;
};
```

Ispis 4. Podatkovna struktura nlmsgerr

Podatkovna struktura `nlmsgerr` ima slijedeće članove:

- `error`

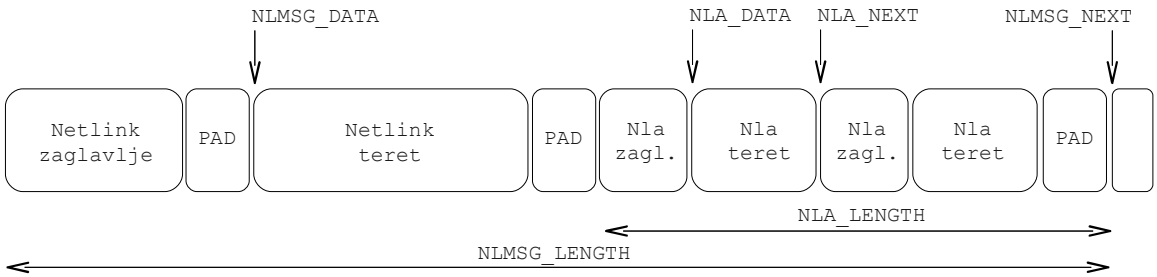
  Član strukture predstavlja *errno* vrijednost upotrebom koje je moguće detaljnije saznati opis greške. U slučaju da je vrijednosti člana jednaka nuli tada poruka predstavlja poruku potvrde primitka poruke.

- `msg`

  Član strukture predstavlja zaglavlje originalne poruke koja je odaslana prema komponenti ravnine proslijeđivanja.

3.2. Logički prikaz Netlink poruke

Slika 3.1. prikazuje logički prikaz potpune Netlink poruke u memoriji. Netlink poruka predstavljena je tokom okteta s koji se sastoji od zaglavlja Netlink poruke te pripadajućeg tereta. Polja PAD u Netlink poruci predstavljaju prostor koji osigurava da je poruka ispravno prezentirana u memoriji računala (eng. *data structure padding*). Teret poruke opisan je poljima `Netlink teret` te poljem Netlink atributa u obliku TLV unosa. Polje atributa sadrži dva TLV unosa s pripadajućim zaglavljem i vrijednosti u polju `Nla teret`.



Slika 3.1. Logički prikaz Netlink poruke

Netlink sučelje definira niz pomoćnih makro funkcija koje olakšavaju kreiranje i manipulaciju Netlink porukama. Na slici je slikovito prikazana upotreba pomoćnih makro funkcija koje je obvezatno koristiti prilikom kreiranja i manipulacije Netlink porukama. Njihova upotreba osigurava da su kreirane poruke ispravno formatirane i prezentirane u memoriji različitih arhitektura računala. Sve makro funkcije definirane su u zaglavnoj datoteci `<linux/netlink.h>`.

Objašnjenje pomoćnih funkcija:

- `int NLMSG_ALIGN(size_t len)`

  Funkcija prima duljinu poruke te zaokružuje duljinu na prvi veći višekratnik `NLMSG_ALIGNTO`. Vrijednost `NLMSG_ALIGNTO` postavljena je na 4 okteta. Navedena funkcija ne upotrebljava se direktno prilikom rada s Netlink sučeljem već funkciju interno koriste ostale definirane makro funkcije.

- `int NLMSG_LENGTH(size_t len)`

  Funkcija prima duljinu tereta (eng. *payload*) koji se isporučuje u Netlink poruci i vraća veličinu tereta poruke zajedno s Netlink zaglavljem. Vraćena vrijednost zaokružena je na prvi veći višekratnik `NLMSG ALIGNTO` vrijednosti. Makro funkcija se obično koristi prilikom popunjavanja `nlmsg_len` vrijednosti podatkovne strukture `nlmsghdr`.

- `int NLMSG_SPACE(size_t len)`

  Funkcija vraća namještenu vrijednost veličine Netlink poruke zajedno `len` duljinom tereta poruke.

- `void *NLMSG_DATA(struct nlmsghdr *nlh)`

  Funkcija vraća pokazivač na teret Netlink poruke za zadano `nlh` zaglavlje.

- `struct nlmsghdr *NLMSG_NEXT(struct nlmsghdr *nlh, int len)`

  U slučaju da odgovor na upit od komponente ravnine upravljanja ne stane u jednu Netlink poruku, poruke se isporučuju u obliku više uzastopnih Netlink poruka. Funkcija služi za pozicioniranje na slijedeću Netlink poruku unutar memorijskog polja. Parametar `len` je lijeva strane (eng. *lvalue*) operacije i predstavlja duljinu ostatka memorijskog polja.

- `int NLMSG_OK(struct nlmsghdr *nlh, int len)`

  Funkcija provjerava je li Netlink poruka ispravna, tj. je li teret poruke u cijelosti dohvatljiv ili je odrezan (eng. *truncated*). U slučaju da je funkcija vratila pozitivnu vrijednost moguće je ispravno koristiti ostale pomoćne makro funkcije.

- `int NLMSG_PAYLOAD(nlmsghdr *nlh, int len)`

  Funkcija vraća vrijednost duljine tereta za `nlh` Netlink poruku.

3.3. Komunikacija između ravnine upravljanja i proslijeđivanja

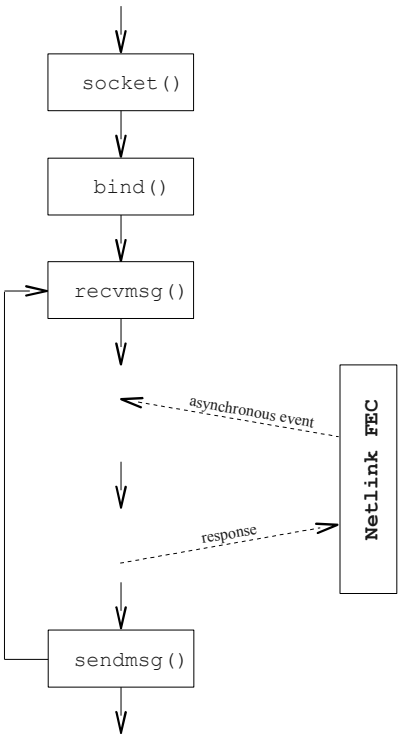
Komunikacija između komponenata upravljanja i proslijeđivanja omogućena je u oba smjera. Komponente mogu neovisno o stanju drugih komponenata započeti komunikaciju. Nakon registracije komponenata ravnine upravljanja za određenu IP uslugu Netlink protokol ne opisuje tko je od sudionika zaslužan za početak komunikacije.

U nastavku slijedi opis i redoslijed poziva funkcija prilikom povezivanja komponenata ravnine upravljanja za specifičnu IP uslugu. Razmatraju se dva različita slučaja koji se odnose na ostvarenje konekcije od strane ravnine upravljanja te slučaj za primitak asinkronih događaja od komponenata ravnine proslijeđivanja.

Ukoliko komponente upravljanja samo odašilju upravljačke naredbe prema ravnini proslijeđivanja potrebno je obaviti slijedeće:

- povezivanje na određenu IP uslugu pozivom `socket` funkcije za kreiranje pristupne Netlink točke. Prilikom poziva prosljeđuje se parametar funkciji koji opisuje tip Netlink IP usluge koja se koristi
- upotrebom standardnih funkcija za slanje i primanje na bespojnoj usluzi, *sendmsg* i *recvmsg* obavlja se slanje i primanje poruka od komponenata ravnine proslijeđivanja

Slika 3.2. prikazuje redoslijed poziva funkcija prilikom odašiljanja poruka zahtjeva za konfiguraciju ili dohvaćanja konfiguracije prema ravnini proslijeđivanja.

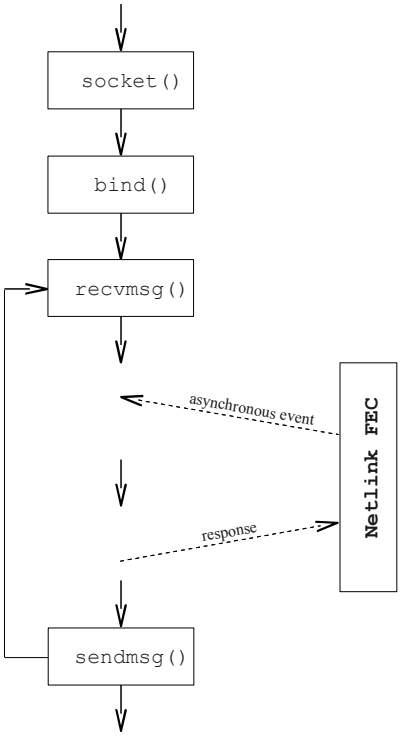


Slika 3.2. Redoslijed poziva funkcija prilikom prihvaćanja Netlink događaja

U slučaju da komponente ravnine upravljanja samo zaprimaju asinkrone događaje od ravnine proslijeđivanja potrebno je obaviti slijedeće:

- povezivanje na određenu IP uslugu pozivom `socket` funkcije za kreiranje pristupne Netlink točke. Prilikom poziva prosljeđuje se parametar funkciji koji opisuje tip Netlink IP usluge koja se koristi
- povezivanje na pristupnu Netlink točku upotrebom funkcije `bind` za primanje asinkronih događaja od komponenata ravnine proslijeđivanja
- povezivanje na pristupnu Netlink točku za osluškivanje asinkronih događaja za IP uslugu. Ukoliko više komponenata obavlja upravljanje za istu IP uslugu tada Netlink sustav šalje obavijesti ostalim komponentama o obavljenim promjenama.

Slika 3.3. prikazuje redoslijed poziva funkcija pristupne točke za prihvat asinkronih Netlink događaja.



Slika 3.3. Redoslijed poziva funkcija prilikom prihvaćanja Netlink događaja

Detaljnije upute za korištenje gore navedenih funkcija nalazi se u slijedećem poglavlju.

3.3.1. Kreiranje Netlink spojne točke i povezivanje

Pristup upravljačkoj ravini Linux jezgre upotrebom Netlink sučelja obavlja se upotrebom standardnog BSD *socket* sučelja uz korištenje AF_NETLINK grupe komunikacijskih usluga.

Prototip funkcije za kreiranje spojne točke ima slijedeći oblik:

```
#include <sys/types.h>
#include <sys/socket.h>

int socket(int domain, int type, int protocol);
```

Ispis 5. Funkcija za kreiranje spojne točke

dok argumenti imaju slijedeća značenja:

- `domain`

Argument funkcije određuje grupu komunikacijskih usluga koja se koristi. Ukoliko se koristiti Netlink programsko sučelje prema jezgri operativnog sustava potrebno je odabrati **AF_NETLINK**. Popis raspoloživih komunikacijskih usluga moguće je naći u `<sys/socket.h>` zaglavnoj datoteci.

- `type`

  Argument funkcije dodatno specificira karakteristiku usluge koja se koristi. Ukoliko upotrebljavamo `AF_NETLINK` tada je potrebno postaviti vrijednost na `SOCK_RAW`.

- `protocol`

  Argument funkcije bira protokol koji se koristi za implementaciju željene vrste komunikacije u danoj grupi komunikacijskih usluga. U slučaju Netlink protokola član strukture sadrži vrijednost koja definira protokol između ravnine upravljanja i proslijeđivanja za specifičnu IP uslugu. Za `AF_NETLINK` grupu popis raspoloživih protokola nalazi se u `<linux/netlink.h>` zaglavnoj datoteci

Prototip funkcije za povezivanje na Netlink spojnu točku ima slijedeći oblik:

```
#include <sys/types.h>
#include <sys/socket.h>

int bind(int sockfd, const struct sockaddr *addr,
                        socklen_t addrlen);
```

Ispis 6. Funkcija za povezivanje na spojnu točku

dok argumenti imaju slijedeća značenja:

- `sockfd`

  Argument predstavlja Netlink spojnu točku na koju se povezuje.

- `addr`

  Argument predstavlja adresnu podatkovnu strukturu koja opisuje Netlink sudionika u komunikaciji.

- `addrlen`

  Argument predstavlja veličinu adresne podatkovne strukture.

4. Netlink usluga zaštite IP protokola

Usluga zaštite IP protokola omogućena je upotrebom IPsec arhitekture (eng. *Internet Protocol Security – IPsec*). IPsec arhitektura predstavlja skup protokola razvijen od strane IETF standardizacijske udruge koji obuhvaćaju mehanizme zaštite toka na mrežnom sloju OSI (*Open Systems Interconnection*) modela. Osnovna zadaća IPsec arhitekture je ispunjenje osnovnih zahtijeva sigurnosti informacijskog sustava prilikom zaštite dijeljene informacije:

- tajnost (eng. *confidentiality)* – isključivo ovlaštena osoba može pristupiti dijeljenoj informaciji
- integritet ili besprijekornost (eng. *integrity)* – zaštita informacije od oštećenja ili izmjene od strane neovlaštene osobe
- autentičnost (eng. *authentication)* – provjera identiteta izvora informacije

Osnovne zahtjeve zaštite dijeljene informacije IPsec arhitektura pruža upotrebom slijedećih protokola:

- ESP (*Encapsulating Security Payload*) – protokol osigurava integritet, provjeru vjerodostojnosti pošiljatelja IP paketa, tajnost paketa i zaštitu od napada reprodukcijom. ESP protokol opisan je u [].
- AH (*Authentication Header*) – protokol osigurava integritet i provjeru vjerodostojnosti IP paketa. AH protokol opisan je u [].
- protokol za uspostavu i razmjenu ključeva – protokol se upotrebljava za uspostavu sigurnosnih poveznica, dogovor sigurnosnih algoritama i za razmjenu enkripcijskih i ovjernih ključeva, predstavnici – IKE (*Internet Key Exchange*), ISAKMP (*Internet Security Association and Key Management Protocol*)

IPsec arhitektura upotrebljava koncept sigurnosne politike i poveznice kao temeljne elemente pri osiguranju zaštite IP protokola između IPsec sudionika.

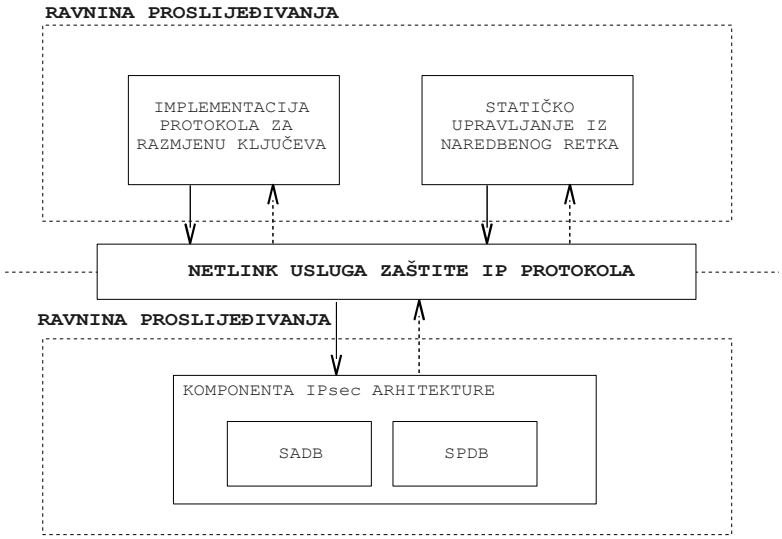
Sigurnosna politika opisuje promet koji je potrebno zaštititi. Promet u IPsec sustavu definiran je izvorišnom i odredišnom IP adresom, protokolom višeg sloja, smjerom prometa, tipom sigurnosnog protokola i dr. Sigurnosna poveznica predstavlja jednosmjernu logičku vezu koja pruža sigurnosne mehanizme IP prometu kojeg prenosi. Sigurnosna poveznica predstavlja poveznicu između sudionika u IPsec sustavu te sadrži dijeljenu informaciju i skup kriptografskih algoritama koji se primjenjuju na pakete toka prometa koji se štiti. Za uspostavu tipične dvosmjerne veze IPsec arhitektura zahtijeva upotrebu dvije instance sigurnosne poveznice, koristeći svaku u jednom smjeru.

Netlink grupa komunikacijskih usluga s pripadajućim protokolom omogućava povezivanje ravnine upravljanja s IPsec podsustavom Linux jezgre. Cilj povezivanja je osigurati komponentama upravljačke ravnine upravljanje bazama sigurnosnih poveznica i politika.

Sigurnosne baze nalaze se unutar jezgre operacijskog sustava te predstavljaju sastavni dio IPsec arhitekture.

4.1. Arhitektura

IPsec arhitektura u Netlink okruženju razmatra se kao komponenta ravnine proslijeđivanja. Slika 4.1. prikazuje arhitekturu Netlink usluge zaštite IP protokola. IPsec komponenta ravnine proslijeđivanja sastoji se od dva servisna elementa, implementacije baze sigurnosnih poveznica i politika te pripadajuće operacije za obavljanje transformacija nad paketima.



Slika 4.1. Netlink usluga zaštite IP protokola

Ravnina upravljanja odnosi se na komponente koje obavljaju statičko ili dinamičko upravljanje IPsec komponenti proslijeđivanja. Predstavnici statičkog upravljanja su alati naredbenog retka dok se dinamičko upravljanje odnosi na komponente koje implementiraju IKE protokol za razmjenu i dogovor ključeva. Navedene komponente nalaze se u korisničkom okruženju jer imaju direktan pristup konfiguracijskim parametrima IPsec sudionika te informacijama potrebnim za ovjeru (*pre-shared keys, certificates*).

U slučaju da je potrebno zaštiti određeni tok podataka IPsec komponenta ravnine proslijeđivanja obavlja transformacije nad paketima toka. Detalji oko transformacija su zapisani u sigurnosnim bazama te se odnose na primjenu enkripcijskih i ovjernih operacija nad paketima. Pri tome se transformacije obavljaju efikasno bez unosa dodatnog kašnjenja kako bi isporuka bila obavljena što brže. Ravnina upravljanja obavlja upravljačke mehanizme nad sigurnosnim bazama te se ujedno i brine o njihovom stanju. Dodatno IPsec komponenta proslijeđivanja obavještava komponente upravljanja o trenutnom stanju sigurnosnih baza. Opisani mrežni element predstavljaju sigurnosni prilaz (eng. *security gateway*).

U svrhu podizanja sigurnosti i jednostavnosti u sprezi s IPsec arhitekturom preporuka je koristiti dinamičko upravljanje sigurnosnih baza. Upotrebom IKE protokola uspostavlja se siguran tunel između komponente ravnine upravljanja sudionika u IPsec sustavu u svrhu dogovora sigurnosnih algoritama i uspostave enkripcijskih ključeva. Implementacija protokola za razmjenu ključeva danas predstavlja standard za manipulaciju sigurnosnih baza.

5. Netlink XFRM sučelje

Upravljanje IPsec sigurnosnim bazama koristeći Netlink uslugu zaštite IP protokola omogućena je upotrebom Netlink XFRM sučelja. Netlink XFRM sučelje omogućava programeru ostvarenje komponenti upravljanja IPsec sigurnosnim bazama unutar IPsec komponente proslijeđivanja.

Implementacija koja se odnosi na ravninu proslijeđivanja nalazi se u izvornom kôdu Linux jezgre u kazalu `<net/xfrm/>` a sučelje prema Netlink protokolu nalazi se unutar datoteke `<net/xfrm/xfrm_user.c>`. Dio implementacije koji se odnosi na Netlink XFRM sučelje u ravnini upravljanja opisano je unutar zaglavne datoteke `<linux/xfrm.h>` s pripadajućim podatkovnim strukturama. Upravo ovo sučelje programer koristi prilikom izrade komponente ravnine upravljanja.

U nastavku slijedi pregled podatkovnih struktura s detaljnim objašnjenjima koje se upotrebljavaju prilikom rada s Netlink XFRM sučeljem. Detaljno su objašnjene Netlink poruke koje se razmjenjuju između ravnine upravljanja i proslijeđivanja.

5.1. Podatkovne strukture

Sigurnosni protokoli su sastavni i obvezni dio mrežnog sloja IPv6 protokola, a opcionalni u IPv4 protokolu. IPsec arhitektura u Linux operacijskom sustavu u potpunosti je omogućena za IPv4 i IPv6 protokol. Unija podataka `xfrm_address_t` predstavlja tip podatka kojim se opisuje adresa u XFRM protokolu. Adresa može biti IPv4 ili IPv6 tipa.

```
typedef union
{
        __be32                  a4;
        __be32                  a6[4];
} xfrm_address_t;
```

Ispis 7. Tip podatka xfrm_address_t

Sigurnosna poveznica ili kraće SA (eng. *Security Association*) pojam objašnjavamo kao jednosmjerna veza (eng. *simplex*) koja pruža sigurnosne mehanizme prometu koristeći IPsec sigurnosne protokole. Za uspostavu tipične dvosmjerne veze zahtijeva upotrebu dvije instance sigurnosne poveznice, koristeći svaku u jednom smjeru. Sigurnosna poveznica opisana je podatkovnom strukturom `xfrm_usersa_info` koja je detaljnije opisana u nastavku.

Ispravna i jednoznačna identifikacija instance sigurnosne poveznice u bazi zahtjeva poznavanje SPI (*Security Payload Identificator*) identifikatora, odredišnu IP adresu paketa i tip sigurnosnog protokola. U slučaju dolaznog toka, kombinacijom SPI parametra i IP adrese, IPsec arhitektura odabire zapis iz baze sigurnosnih poveznica u kojem se nalaze algoritmi enkripcije i ovjere te potrebni ključevi za ispravno dekriptiranje dolaznog paketa.

Podatkovna struktura `xfrm_id` predstavlja identifikator pomoću kojeg se jedinstveno opisuje sigurnosna poveznica.

```
struct xfrm_id
{
        xfrm_address_t              daddr;
        __be32                      spi;
        __u8                        proto;
};
```

Ispis 8. Podatkovna struktura xfrm_id

Podatkovna struktura `xfrm_id` ima slijedeće članove:

- `daddr`

  Član strukture predstavlja odredišnu adresu sigurnosne poveznice.

- `spi`

  Član strukture predstavlja jedinstvenu vrijednost SPI parametra sigurnosne poveznice.

- `proto`

  Član strukture predstavlja IPsec protokol sigurnosne poveznice, ESP ili AH protokol.

Prilikom prolazak paketa IPsec komponentom ravnine proslijeđivanja potrebno je obaviti povezivanje trenutnog toka paketa s pripadajućom sigurnosnom politikom. Povezivanje se obavlja upotrebom selektora prometa (eng. *traffic selector*). Podatkovna struktura `xfrm_selector` predstavlja selektor prometa koji je sastavni dio svake sigurnosne politike.

```
struct xfrm_selector
{
        xfrm_address_t              daddr;
        xfrm_address_t              saddr;
        __be16                      dport;
        __be16                      dport_mask;
        __be16                      sport;
        __be16                      sport_mask;
        __u16                       family;
        __u8                        prefixlen_d;
        __u8                        prefixlen_s;
        __u8                        proto;
        int                         ifindex;
        uid_t                       user;
};
```

Ispis 9. Podatkovna struktura xfrm_selector

Članovi podatkovne strukture `xfrm_selector` predstavljaju parametre pomoću kojih se obavlja usporedba s pripadajućim tokom. Usporedba se obavlja na temelju izvorišne i

odredišne adrese toka, porodicom protokola višeg sloja, pristupnim vratima te indeksom mrežnog sučelja.

5.2. Tip poruka

U Netlink sučelju zaštite IP protokola razlikujemo više različitih vrsta poruka:

- asinkroni događaji od ravnine proslijeđivanja
- poruke za upravljanje i manipulaciju zapisa u bazi sigurnosnih poveznica
- poruke za upravljanje i manipulaciju zapisa u bazi sigurnosnih politika
- poruke za upravljanje sigurnosnim bazama u okruženju s pokretnim agentima
- poruke za upravljanje sigurnosnim bazama u HA okruženju
- dohvaćanje informacija o sigurnosnim bazama

5.3. Asinkroni događaji ravnine proslijeđivanja

Uslijed promjene stanja određenih objekata ravnine proslijeđivanja, upotrebom asinkronih događaja (eng. *asynchronous events*) komponente proslijeđivanja o promjenama obavještavaju ravninu upravljanja. Upotrebom poruka asinkronih događaja nema potrebe za nepotrebnim kontinuiranim upitima ravnine upravljanja o stanju pojedinog objekta ravnine proslijeđivanja. Na taj način se održava konzistentno stanje ravnine upravljanja bez dodatnog i nepotrebnog opterećenja na ravninu proslijeđivanja.

Razlikuje se više tipova obavijesti ravnine proslijeđivanja i to obavijesti o:

- nedostatku sigurnosne poveznice u bazi sigurnosnih poveznica
- istek ograničenja postojeće sigurnosne poveznice ili politike
- stanju promjenjivih parametara sigurnosne poveznice

5.3.1. Nedostatak poveznice u bazi sigurnosnih poveznica

U slučaju nedostatak pripadajuće sigurnosne poveznice u bazi sigurnosnih poveznica prilikom prolaska prometa kroz ravninu proslijeđivanja IPsec komponenta o tome obavještava komponente ravnine upravljanja. Upotrebom `XFRM_MSG_ACQUIRE` tipa poruke ravnina proslijeđivanja signalizira ravnini upravljanja nedostatak sigurnosne poveznice za

određeni tok podataka. Teret poruke predstavljaju sve potrebne informacije iz kojih komponente upravljanja mogu obaviti dogovor sigurnosne poveznice. Teret Netlink poruke predstavljen je podatkovnom strukturom `xfrm_user_acquire`.

```
struct xfrm_user_acquire {
        struct xfrm_id                  id;
        xfrm_address_t                  saddr;
        struct xfrm_selector            sel;
        struct xfrm_userpolicy_info     policy;
        __u32                           aalgos;
        __u32                           ealgos;
        __u32                           calgos;
        __u32                           seq;
};
```

Ispis 10. Podatkovna struktura xfrm_user_acquire

Podatkovna struktura `xfrm_user_acquire` ima slijedeće članove:

- `id`

  Član strukture predstavlja identifikator koji jedinstveno opisuje sigurnosnu poveznicu.

- `saddr`

  Član strukture predstavlja izvorišnu adresu toka podataka koje je potrebno zaštiti.

- `sel`

  Član strukture predstavlja selektor prometa.

- `policy`

  Član strukture predstavlja sigurnosnu politiku koja se odnosi na tok podataka.

- `aalgos, ealgos, calgos`

  Članovi strukture predstavljaju algoritme enkripcije, ovjere i kompresije.

- `seq`

  Član strukture predstavlja slijedni broj poruke.

5.3.2. Istek ograničenja postojeće sigurnosne poveznice

Istek ograničenja postojeće sigurnosne poveznice ili politike, ravnina proslijeđivanja signalizira komponentama ravnine upravljanja. Jedna od operacija IPsec arhitekture predstavlja nadzor trenutno raspoloživih poveznica i politika u sigurnosnim bazama te u slučaju da je došlo do granice ograničenja potrebno je o tome obavijestiti sve komponente ravnine upravljanja registrirane za uslugu zaštite IP protokola. Nakon potpunog isteka ograničenja komponente upravljanja obavljaju ponovni izračun ključeva (eng. *rekeying*).

Upotrebom `XFRM_MSG_EXIPRE` tipa poruke ravnina proslijeđivanja obavještava komponente upravljanja da je isteklo određeno ograničenje sigurnosne poveznice. `XFRM_MSG_EXPIRE` tip poruke odašilje isključivo IPsec komponenta proslijeđivanja u slučaju da je istekao neki od prethodno definiranih *hard* ili *soft* ograničenja sigurnosne poveznice.

Teret `XFRM_MSG_EXPIRE` poruke predstavljen je podatkovnom strukturom `xfrm_user_expire`.

```
struct xfrm_user_expire {
        struct xfrm_usersa_info         state;
        __u8                            hard;
};
```

Ispis 11. Podatkovna struktura xfrm_user_expire

Podatkovna struktura `xfrm_user_expire` ima slijedeće članove:

- `state`

  Član strukture predstavlja podatkovnu strukturu sigurnosne poveznice kojoj je isteklo određeno ograničenje.

- `hard`

  Član strukture predstavlja zastavicu koja određuje odnosi li se ograničenje na *hard* ili *soft*. U slučaju da je zastavica postavljena, radi se o *hard* ograničenju.

Upotrebom `XFRM_MSG_POLEXPIRE` tipa poruke ravnina proslijeđivanja signalizira upravljačkoj ravnini da je isteklo određeno ograničenje sigurnosne politike. Teret `XFRM_MSG_POLEXPIRE` poruke predstavljen je podatkovnom strukturom `xfrm_user_polexpire`.

```
struct xfrm_user_polexpire {
        struct xfrm_userpolicy_info     pol;
        __u8                            hard;
};
```

Ispis 12. Podatkovna struktura xfrm_user_polexpire

Podatkovna struktura `xfrm_user_polexpire` ima slijedeće članove:

- `pol`

  Član strukture predstavlja podatkovnu strukturu sigurnosne politike kojoj je isteklo određeno ograničenje.

- `hard`

Član strukture predstavlja zastavicu koja određuje odnosi li se ograničenje na *hard* ili *soft*. U slučaju da je zastavica postavljena, radi se o *hard* ograničenju.

5.3.3. Stanje promjenjivih parametara sigurnosne poveznice

Prilikom prolaska paketa kroz IPsec komponentu proslijeđivanja kontinuirano se obavlja obnova određenih parametara sigurnosne poveznice. Promjenjivi parametri predstavljaju broj okteta koji su zahvaćeni sigurnosnom poveznicom, količina ponovljenih paketa (eng. *reply value*) i ??? (eng. *expiry timer)*. Navedene informacije ravnina upravljanja koristi za sinkronizaciju parametara sigurnosne poveznice. U poglavlju Upravljanje sigurnosnim bazama u okruženju sustava visoke dostupnosti detaljnije je objašnjena upotreba promjenjivih parametara sigurnosne poveznice.

Upotrebom poruke `XFRM_MSG_GETAE` komponente upravljanja obavlja dohvaćanje trenutnog stanja promjenjivih parametara. Poruka zahtjeva `XFRM_MSG_GETAE` nema dodatnih Netlink atributa. Upotrebom `XFRM_MSG_NEWAE` tipa poruke zajedno s pripadajućim poljem Netlink atributa IPsec komponenta proslijeđivanja obavještava komponente upravljanja o trenutnim vrijednostima promjenjivih parametara. Dodatno nakon što je pređen prag za određenu sigurnosnu poveznicu ravnina proslijeđivanja kontinuirano obavještava ravninu upravljanja o trenutnom stanja promjenjivih parametara sigurnosne poveznice.

Teret Netlink poruke tipa `XFRM_MSG_NEWAE` sastoji se od podatkovne strukture `xfrm_aevent_id` koja opisuje tip asinkronog događaja i dva Netlink atributa. Svaka poruka odgovora `XFRM_MSG_NEWAE` ravnine proslijeđivanja sadrži atribute tipa `XFRMA_LTIME_VAL` i `XFRMA_REPLAY_VAL`.

```
struct xfrm_aevent_id {
        struct xfrm_usersa_id           sa_id;
        xfrm_address_t                  saddr;
        __u32                           flags;
        __u32                           reqid;
};
```

Ispis 13. Podatkovna struktura xfrm_user_aevent_id

Podatkovna struktura `xfrm_aevent_id` ima slijedeće članove:

- `sa_id, saddr, reqid`

  Članovi strukture jednoznačno opisuju sigurnosnu poveznicu ravnini upravljanja za koju se obavještavaju promjenjivi parametri.

- `flags`

  Član strukture predstavlja zastavice pomoću kojih ravnina upravljanja razlikuje parametre u asinkronom događaju.

  - `XFRM_AE_RTHR` – prag ponovljenih paketa (eng. *replay threshold*)

- `XFRM_AE_RVAL` – količina ponovljenih paketa (eng. *replay value*)
- `XFRM_AE_LVAL` – vrijeme života sigurnosne poveznice (eng. *lifetime value*)
- `XFRM_AE_ETHR` – ??? (eng. *expiry timer threshold*)
- `XFRM_AE_CR` – uzrok događaja je obnova vrijednosti ponovljenih paketa (eng. *replay update*)
- `XFRM_AE_CE` – uzrok događaja je obnova vrijednosti ??? (eng. *expiry timer*)
- `XFRM_AE_CU` – uzrok događaja je obavijest o obnovi sigurnosne politike

Raspoloživi Netlink atributi i pripadajuća objašnjenja:

- `XFRMA_LTIME_VAL` – atribut sadrži vrijednost količine okteta
- `XFRMA_REPLAY_VAL` – atribut sadrži vrijednost količine ponovljenih paketa
- `XFRMA_REPLAY_THRESH` – atribut sadrži vrijednost praga koji jezgra koristi za okidanje događaja prema ravnini upravljanja
- `XFRMA_ETIMER_THRESH` – vrijednost vremenskog intervala u milisekundama koji se koristi u Nagle algoritmu za definiciju brzine kojom se događaji prosljeđuju ravnini upravljanja

5.4. Upravljanje bazom sigurnosnih poveznica

Upravljanje baze sigurnosnih poveznica odnosi se na slijedeće operacije:

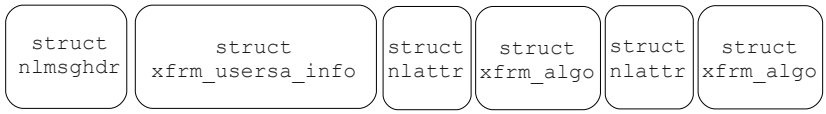
- unos nove sigurnosne poveznice
- nadopunu postojeće sigurnosne poveznice
- brisanje sigurnosne poveznice
- dohvaćanje sigurnosne poveznice
- brisanje cjelokupne baze sigurnosnih poveznica
- alokaciju privremene sigurnosne poveznice

5.4.1. Unos i nadopuna sigurnosne poveznice

Unos nove sigurnosne poveznice u bazu sigurnosnih poveznica komponente upravljanja obavljaju upotrebom `XFRM_MSG_NEWSA` tipa poruke. Nadopuna postojećeg zapisa ili privremenog zapisa sigurnosne poveznice obavlja se upotrebom `XFRM_MSG_UPDSA` tipa poruke. Unos i nadopuna sigurnosne poveznice u pravilu su vrlo slične operacije koje zahtijevaju isti format Netlink poruke zahtjeva.

Teret Netlink poruke zahtjeva sastoji se od podatkovne strukture `xfrm_usersa_info` i dva Netlink atributa. Podatkovna struktura `xfrm_usersa_info` opisuje sigurnosnu

poveznicu. Vrijednost Netlink atributa predstavlja se podatkovnom strukturom `xfrm_algo` koja opisuje algoritme transformacija. Ravnina proslijeđivanja obavlja traženu operaciju te porukom odgovora `XFRM_MSG_NEWSA` obavještava komponentu upravljanja o rezultatu obavljene operacije. Slika 5.2. prikazuje format Netlink poruke s pripadajućim teretom za unos ili nadopunu postojeće sigurnosne poveznice.



Slika 5.1. Format Netlink poruke za dodavanje sigurnosne poveznice

Podatkovna struktura `xfrm_usersa_info` predstavlja sigurnosnu poveznicu.

```
struct xfrm_usersa_info {
        struct xfrm_selector            sel;
        struct xfrm_id                  id;
        xfrm_address_t                  saddr;
        struct xfrm_lifetime_cfg        lft;
        struct xfrm_lifetime_cur        curlft;
        struct xfrm_stats               stats;
        __u32                           seq;
        __u32                           reqid;
        __u16                           family;
        __u8                            mode;
        __u8                            replay_window;
        __u8                            flags;

};
```

Ispis 14. Podatkovna struktura xfrm_usersa_info

Podatkovna struktura ima slijedeće članove:

- `sel`

  Član strukture predstavlja selektor prometa.

- `id`

  Član strukture predstavlja jedinstveni identifikator sigurnosne poveznice.

- `saddr`

  Član strukture predstavlja izvorišnu adresu sigurnosne poveznice.

- `lft, curlft`

  Članovi strukture predstavljaju vijek trajanja sigurnosne poveznice; `lft` se odnosi na postavljene vrijednosti ograničenja sigurnosne poveznice dok `curlft` predstavlja trenutna ograničenja.

- `stats`

Član strukture predstavlja podatkovnu strukturu koja sadrži različite statistike sigurnosne poveznice.

- `seq`

  Član strukture predstavlja slijedni broj sigurnosne poveznice.

- `reqid`

  Član strukture predstavlja vrijednost identifikatora zahtjeva sigurnosne poveznice.

- `family`

  Član strukture predstavlja porodicu protokola (IPv4 ili IPv6) sigurnosne poveznice.

- `mode`

  Član strukture predstavlja tip sigurnosne poveznice. Osnovni tipovi sigurnosne poveznice su – `XFRM_MODE_TUNNEL`, `XFRM_MODE_TRANSPORT`.

- `replay_window`

  Član strukture predstavlja

- `flags`

  Član strukture predstavlja zastavice koje opisuju dodatne parametre sigurnosne poveznice.

Poruka unosa ili nadopune postojeće sigurnosne poveznice zahtjeva postavljanje dva Netlink atributa. Obično se za sigurnosnu poveznicu postavljaju transformacije koje se odnose na zaštitu i ovjeru IP paketa. Sukladno tome u teret Netlink poruke postavlja se `XFRMA_ALG_CRYPT` i `XFRMA_ALG_AUTH` tip Netlink atributa. Dodatno, IPsec arhitektura nudi transformacije u vidu kompresije IP paketa (eng. *IP Payload Compression Protocol – IPcomp*). Vrijednost Netlink atributa predstavljena je podatkovnom strukturom `xfrm_algo` koja predstavlja određeni tip transformacije. Raspoloživi tipovi Netlink atributa su:

- `XFRMA_ALG_CRYPT` – predstavlja algoritam enkripcije
- `XFRMA_ALG_AUTH` – predstavlja algoritam ovjere
- `XFRMA_ALG_COMP` – predstavlja algoritam kompresije

Podatkovna struktura `xfrm_algo` predstavlja kriptografski algoritam zajedno s pripadajućim ključem te duljinom ključa.

```
struct xfrm_algo {
        char            alg_name[64];
        unsigned int    alg_key_len;    /* in bits */
        char            alg_key[0];
};
```

Ispis 15. Podatkovna struktura xfrm_algo

Podatkovna struktura `xfrm_algo` ima slijedeće članove:

- `alg_name`

  Član strukture predstavlja ime kriptografskog algoritma kojeg podatkovna struktura *xfrm_algo* predstavlja. Popis raspoloživih kriptografskih algoritama nalazi se u izvornom kôdu Linux jezgre u datoteci `<net/xfrm/xfrm_algo.c>`.

- `alg_key_len`

  Član strukture predstavlja duljinu ključa u brojevima bitova.

- `alg_key`

  Član strukture predstavlja ključ pripadajućeg kriptografskog algoritma.

5.4.2. Brisanje i dohvaćanje sigurnosne poveznice

Brisanje sigurnosne poveznice iz baze sigurnosnih poveznica, komponente upravljanja obavljaju upotrebom `XFRM_MSG_DELSA` tipa poruke. Dohvaćanje sigurnosne poveznice obavlja se upotrebom `XFRM_MSG_GETSA` tipa poruke. Brisanje i dohvaćanje sigurnosne poveznice u pravilu su vrlo slične operacije koje imaju isti format Netlink poruke zahtjeva.

Teret Netlink poruke zahtjeva sastoji se od podatkovne strukture `xfrm_usersa_id` i pripadajućeg Netlink atributa. Podatkovna struktura `xfrm_usersa_id` jedinstveno određuje sigurnosnu poveznicu nad kojom je potrebno obaviti jednu od navedenih operacija, brisanje ili dohvaćanje. Ravnina proslijeđivanja obavlja navedenu operaciju te porukom odgovora tipa `XFRM_MSG_NEWSA` obavještava komponentu upravljanja o rezultatu obavljene operacije.

Teret Netlink poruke za brisanje ili dohvaćanje sigurnosne poveznice predstavljen je podatkovnom strukturom `xfrm_usersa_id`.

```
struct xfrm_usersa_id {
        xfrm_address_t                  daddr;
        __be32                          spi;
        __u16                           family;
        __u8                            proto;
};
```

Ispis 16. Podatkovna struktura xfrm_usersa_id

Podatkovna struktura ima slijedeće članove:

- `daddr`

  Član strukture predstavlja odredišnu adresu sigurnosne poveznice.

- `spi`

  Član strukture predstavlja jedinstvenu vrijednost SPI parametra sigurnosne poveznice.

- `familiy`

  Član strukture predstavlja porodicu protokola (IPv4 ili IPv6) sigurnosne poveznice.

- `proto`

  Član strukture predstavlja IPsec protokol sigurnosne poveznice, ESP ili AH protokol.

5.4.3. Brisanje baze sigurnosnih poveznica

Brisanje cjelokupne baze sigurnosnih poveznica za određeni sigurnosni protokol komponente upravljanja obavljaju upotrebom `XFRM_MSG_FLUSHSA` tipa poruke. Teret Netlink poruke tipa `XFRM_MSG_FLUSHSA` predstavljen je podatkovnom strukturom `xfrm_usersa_flush`.

```
struct xfrm_usersa_flush {
        __u8                            proto;
};
```

Ispis 17. Podatkovna struktura xfrm_usersa_flush

Podatkovna struktura `xfrm_usersa_id` ima slijedeće članove:

- `proto`

  Član strukture predstavlja IPsec protokol sigurnosne poveznice, ESP ili AH protokol.

5.4.4. Alokacija privremene sigurnosne poveznice

Alokacija privremene sigurnosne poveznice i dohvaćanje jedinstvene SPI vrijednosti komponente upravljanja obavljaju upotrebom `XFRM_MSG_ALLOCSPI` tipa poruke. Ravnina proslijeđivanja obavlja postavljanje privremene sigurnosne poveznice (eng. *larval security association*) te porukom odgovora `XFRM_MSG_NEWSA` obavještava komponentu upravljanja o alociranoj poveznici i dodijeljenoj SPI vrijednosti. Teret Netlink poruke tipa `XFRM_MSG_ALLOCSPI` predstavljen je podatkovnom strukturom `xfrm_userspi_info` te ne sadrži dodatne atribute.

```
struct xfrm_userspi_info {
        struct xfrm_usersa_info         info;
        __u32                           min;
        __u32                           max;
};
```

Ispis 18. Podatkovna struktura xfrm_userspi_info

Podatkovna struktura `xfrm_userspi_info` ima slijedeće članove:

- `info`

  Član predstavlja privremenu sigurnosnu poveznicu.

- `min,max`

  Članovi predstavljaju donju i gornju granicu iz koje komponenta ravnine upravljanja očekuje SPI vrijednost.

5.5. Upravljanje bazom sigurnosnih politika

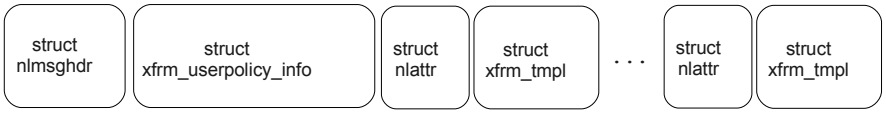
Upravljanje baze sigurnosnih politika odnosi se na slijedeće operacije:

- unos nove sigurnosne politike
- nadopunu postojeće sigurnosne politike
- brisanje sigurnosne politike
- dohvaćanje sigurnosne politike
- brisanje cjelokupne baze sigurnosnih politika

5.5.1. Unos i nadopuna sigurnosne politike

Unos nove sigurnosne politike u bazu sigurnosnih poveznica komponente upravljanja obavljaju upotrebom `XFRM_MSG_NEWPOLICY` tipa poruke. Nadopuna postojećeg zapisa sigurnosne politike obavlja se upotrebom `XFRM_MSG_UPDPOLICY` tipa poruke. Unos i nadopuna sigurnosne politike u pravilu su vrlo slične operacije koje zahtijevaju isti format Netlink poruke zahtjeva.

Teret Netlink poruke zahtjeva sastoji se od podatkovne strukture `xfrm_userpolicy_info` i jednog ili više Netlink atributa. Podatkovna struktura `xfrm_userpolicy_info` opisuje sigurnosnu politiku. Vrijednost Netlink atributa predstavlja se podatkovnom strukturom `xfrm_user_tmpl` koja opisuje predložak (eng. *template*). Ravnina proslijeđivanja obavlja traženu operaciju te porukom odgovora XFRM_MSG_NEWPOLICY informira komponentu upravljanja o rezultatu obavljene operacije. Slika 5.1. prikazuje format Netlink poruke s pripadajućim teretom za unos ili nadopunu postojeće sigurnosne politike.



Slika 5.2. Format Netlink poruke za dodavanje sigurnosne politike

Teret Netlink poruke tipa `XFRM_MSG_NEWPOLICY` predstavljen je podatkovnom strukturom `xfrm_userpolicy_info`.

```
struct xfrm_userpolicy_info {
        struct xfrm_selector            sel;
        struct xfrm_lifetime_cfg        lft;
        struct xfrm_lifetime_cur        curlft;
        __u32                           priority;
        __u32                           index;
        __u8                            dir;
        __u8                            action;
        __u8                            flags;
        __u8                            share;
```

Ispis 19. Podatkovna struktura xfrm_userpolicy_info

Osnovni članovi podatkovne strukture su:

- `sel`

  Član strukture predstavlja selektor prometa.

- `lft,curlft`

  Članovi strukture predstavljaju vijek trajanja sigurnosne politike; `lft` se odnosi na postavljene vrijednosti ograničenja sigurnosne politike dok `curlft` predstavlja trenutna ograničenja.

- `priority`

  Član strukture predstavlja vrijednost prioriteta sigurnosne politike.

- `index`

  Član strukture predstavlja vrijednost indeksa sigurnosne politike.

- `dir`

  Član strukture predstavlja smjer prometa na koji je primjenjiva sigurnosna politika. Raspoloživi smjerovi su – `XFRM_POLICY_IN`, `XFRM_POLICY_OUT`, `XFRM_POLICY_FWD`, `XFRM_POLICY_MASK`, `XFRM_POLICY_MAX`

- `action`

  Član strukture predstavlja akciju koju je potrebno primjeniti na tok podataka. Raspoložive akcije su – `XFRM_POLICY_BLOCK`, `XFRM_POLICY_ALLOW`

Poruka unosa ili nadopune postojeće sigurnosne politike zahtjeva postavljanje jednog ili više Netlink atributa. Vrijednost Netlink atributa predstavljena je podatkovnom strukturom `xfrm_user_tmpl`. Tip Netlink atributa je `XFRMA_TMPL`. Podatkovna struktura `xfrm_user_tmpl` predstavlja predložak pomoću kojeg se pretražuje koje su sve moguće sigurnosne poveznice vezane za specifičnu sigurnosnu politiku

```
struct xfrm_user_tmpl {
        struct xfrm_id          id;
        __u16                   family;
        xfrm_address_t          saddr;
        __u32                   reqid;
        __u8                    mode;
        __u8                    share;
        __u8                    optional;
        __u32                   aalgos;
        __u32                   ealgos;
        __u32                   calgos;
};
```

Ispis 20. Podatkovna struktura xfrm_user_tmpl

5.5.2. Brisanje i dohvaćanje sigurnosne politike

Brisanje sigurnosne politike iz baze sigurnosnih politika komponente upravljanja obavljaju upotrebom `XFRM_MSG_DELPOLICY` tipa poruke. Dohvaćanje sigurnosne politike obavlja se upotrebom `XFRM_MSG_GETPOLICY` tipa poruke. Brisanje i dohvaćanje sigurnosne politike u pravilu su vrlo slične operacije koje imaju isti format Netlink poruke zahtjeva. Teret Netlink poruke zahtjeva sastoji se od podatkovne strukture `xfrm_userpolicy_id` i pripadajućeg Netlink atributa. Podatkovna struktura `xfrm_userpolicy_id` jedinstveno određuje sigurnosnu politiku nad kojom je potrebno obaviti jednu od navedenih operacija, brisanje ili dohvaćanje. Vrijednost Netlink atribut tipa `XFRMA_POLICY_TYPE` potrebno je postaviti na podatkovnu strukturu `xfrm_userpolicy_type`. Ravnina proslijeđivanja obavlja navedenu operaciju te porukom odgovora tipa `XFRM_MSG_NEWPOLICY` informira komponentu upravljanja o rezultatu obavljene operacije.

Teret Netlink poruke za brisanje ili dohvaćanje sigurnosne poveznice predstavljen je podatkovnom strukturom `xfrm_userpolicy_id`.

```
struct xfrm_userpolicy_id {
        struct xfrm_selector            sel;
        __u32                           index;
        __u8                            dir;
};
```

Ispis 21. Podatkovna struktura xfrm_userpolicy_id

5.5.3. Brisanje baze sigurnosnih politika

Brisanje cjelokupne baze sigurnosnih politika komponente upravljanja obavljaju upotrebom `XFRM_MSG_FLUSHSA` tipa poruke. Navedena poruka ne sadrži teret u Netlink poruci već zahtjeva postavljanje ispravnog Netlink zaglavlja i tipa poruke bez tereta.

5.6. Upravljanje sigurnosnim bazama u okruženju sustava visoke dostupnosti

Trenutačni zahtjevi servisa koji se izvode na računalnim mrežama očekuju visoku dostupnost usluge. Za potrebe ostvarenja sustava visoke dostupnosti (eng. *high availability*) mrežnog elementa koji implementira uslugu zaštite IP protokola potrebno je obaviti sinkronizaciju baze sigurnosnih poveznica na drugi zamjenski mrežni element. Sinkronizacija se odnosi na ažuriranje cjelokupne baze sigurnosnih poveznica.

Komponenta upravljanja koja implementira IKE protokol obavlja postavljanje poveznica u bazu te je upoznata s svim parametrima sigurnosne poveznice. Promjenjivi parametri (*byte value, replay value, replay treshold, expiry timer*) koji se dinamički mijenjaju prilikom prolaska paketa kroz ravninu proslijeđivanja nisu poznati ravnini upravljanja.

Upotrebom `XFRM_MSG_GETAE` poruke, ravnina upravljanja eksplicitno zahtijeva sinkronizaciju promjenjivih parametara sigurnosne poveznice s ravninom upravljanja. Teret Netlink poruke tipa `XFRM_MSG_GETAE` predstavljen je podatkovnom strukturom `xfrm_aevent_id`.

```
struct xfrm_aevent_id {
        struct xfrm_usersa_id       sa_id;
        xfrm_address_t              saddr;
        __u32                       flags;
        __u32                       reqid;
};
```

Ispis 22. Podatkovna struktura xfrm_aevent_id

5.7. Upravljanje sigurnosnih baza u okruženju pokretnih agenata

Netlink usluga zaštite IP protokola omogućuje upravljanje sigurnosnim bazama u okruženju s pokretnim agentima (eng. *Mobile IP*) opisano u []. Okruženje pokretnih agenata omogućava održavanje stanja svih postojećih komunikacijskih kanala agenta uslijed promjene fizičke lokacije pokretnog agenata. Upotreba implementacije protokola za razmjenu ključeva (eng. *IKEv2 Mobility and Multihoming Protocol – MOBIKE*) na pokretnim agentima zahtijeva određene modifikacije. Navedene modifikacije odnose se na prilagodbu samog IKEv2 protokola i modifikaciju postojećih sigurnosnih poveznica prilikom promjene lokacije agenta opisano u []. Promjena lokacije agenta rezultira drugačijom IP adresom agenta te je navedenu promjenu potrebno registrirati u bazi sigurnosnih poveznica.

Upotrebom `XFRM_MSG_MIGRATE` tipa poruke, komponenta upravljanja obavještava ravninu proslijeđivanja o promjeni trenutne adrese (eng. *care-of address*) pokretnog agenta. Promjenom trenutne adrese, IPsec arhitektura ispravlja zapise u pripadajućim sigurnosnim poveznicama. Teret Netlink poruke tipa `XFRM_MSG_MIGRATE` predstavljen je podatkovnom

strukturom `xfrm_user_migrate`. Podatkovna struktura sadrži sve potrebne informacije koje je potrebno proslijediti IPsec arhitekturi kako bi obavila navedene promjene.

```
struct xfrm_user_migrate {
        xfrm_address_t              old_daddr;
        xfrm_address_t              old_saddr;
        xfrm_address_t              new_daddr;
        xfrm_address_t              new_saddr;
        __u8                        proto;
        __u8                        mode;
        __u16                       reserved;
        __u32                       reqid;
        __u16                       old_family;
        __u16                       new_family;
};
```

Ispis 23. Podatkovna struktura xfrm_user_migrate

Upotrebom `XFRM_MSG_REPORT` tipa poruke ravnina proslijeđivanja obavještava komponente ravnine upravljanja o promjeni točke povezivanja. Teret Netlink poruke tipa `XFRM_MSG_REPORT` predstavljen je podatkovnom strukturom `xfrm_user_report`.

```
struct xfrm_user_report {
        __u8                        proto;
        struct xfrm_selector        sel;
};
```

Ispis 24. Podatkovna struktura xfrm_user_report

5.8. Dohvaćanje informacija o sigurnosnim bazama

Ozbiljnije implementacije sigurnosnih prilaza mogu sadržavati vrlo velik broj unosa u sigurnosnim bazama. Za potrebe dohvaćanja pojedinih informacija komponenata upravljanja iz takvih baza Netlink sučelje definira posebnu vrstu poruka zahtjeva. Upotrebom ove vrste poruka ne utječe se na performanse cjelokupnog Netlink sustava i sučelja prema komponentama ravnine upravljanja.

Za dohvaćanje informacija o bazi sigurnosnih poveznica komponente upravljanja mogu koristiti tip poruke `XFRM_MSG_GETSADINFO` dok za dohvaćanje informacija o bazi sigurnosnih politika potrebno je koristiti tip poruke `XFRM_MSG_GETSPDINFO`. Ravnina proslijeđivanja poruke odgovora šalje upotrebom pripadajućih `XFRM_MSG_NEWSADINFO` i `XFRM_MSG_NEWSPDINFO` tipa poruka. Zatražene informacije nalaze se u polju Netlink atributa.

6. Praktični rad

6.1. Opis zadatka

Zadatak praktičnog dijela diplomskog rada je ostvariti programsku implementaciju upravljanja IPsec sigurnosnim poveznicama i politikama u implementaciji IKEv2 protokola za razmjenu ključeva. Upravljanje je potrebno ostvariti upotrebom Netlink sučelja koristeći uslugu zaštite IP protokola. U radu je korištena postojeća IKEv2 implementacija protokola za razmjenu ključeva, projekt Zavoda za elektroniku, mikroelektroniku, računalne i inteligentne sustave Fakulteta elektrotehnike i računarstva (u daljnjem tekstu ZEMRIS). ZEMRIS IKEv2 projekt ima za cilj implementaciju IKEv2 protokola kao što je opisano u RFC4306 i povezanim dokumentima.

U uvodnom dijelu rada opisano je teorijsko razmatranje Netlink protokola i sučelja za pristup Netlink IP uslugama. Detaljno je opisana i razmatrana Netlink usluga zaštite IP protokola. U sklopu praktičnog dijela diplomskog rada u potpunosti je ostvareno upravljanje sigurnosnim bazama za ZEMRIS IKEv2 projekt upotrebom Netlink usluge zaštite IP protokola. Upravljanje se odnosi na održavanje baze sigurnosnih poveznica i upravljanje bazom sigurnosnih politika. Obavljena je modifikacija implementacije postojećeg IPsec modula s ciljem unificiranja pristupa sigurnosnim bazama operacijskog sustava. U implementaciji pristupnog modula prema sigurnosnim bazama ostvareni su prethodno objašnjeni koncepti Netlink sustava. Izgrađena programska komponenta praktično je testirana za ispravnost rada u okruženju IKEv2 protokola. Prilikom izrade programskog dijela rada u potpunosti se pridržavalo uputa o načinu izrade programskih komponenti ZEMRIS IKEv2 projekta.

U nastavku slijedi osnovni opis arhitekture ZEMRIS IKEv2 komponente. Predstavljene su učinjene izmjene na pristupnom modulu prema jezgri operativnog sustava. Objašnjena je i prikazana razmjena Netlink poruka između IKE komponente upravljanja i IPsec komponente ravnine proslijeđivanja prilikom dogovora i unosa CHILD_SA sigurnosne poveznice. Na kraju rada opisano je praktično testiranje te su prezentirani rezultati testiranja programske izvedbe.

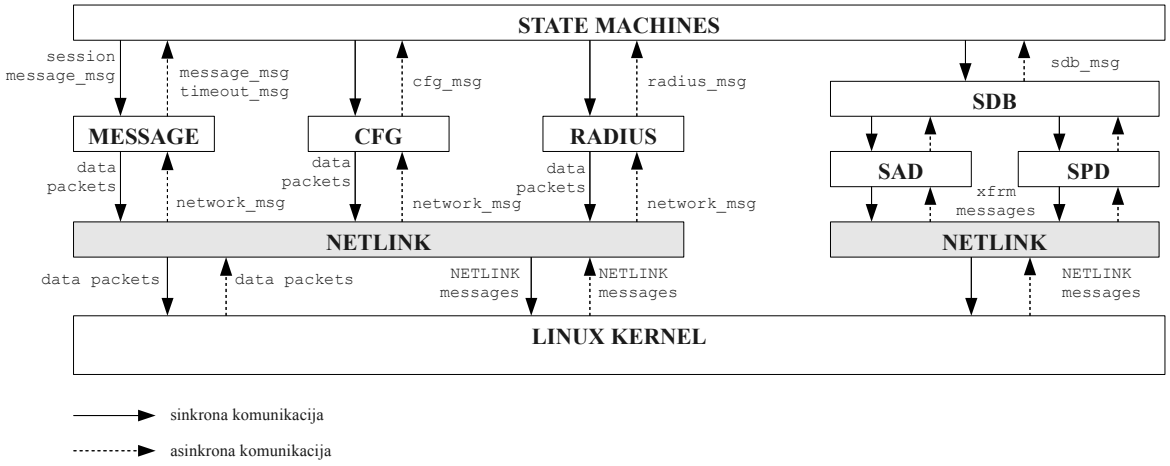
6.2. Upravljanje sigurnosnim bazama u IKEv2 implementaciji

IKEv2 protokol za razmjenu ključeva predstavlja opcionalni protokol IPsec arhitekture. U praktičnim primjenama protokol je neophodan jer dodatno podiže razinu sigurnosti i pojednostavljuje upotrebu IPsec arhitekture. Temeljna operacija IKEv2 protokola odnosi se na ovjeru IPsec sudionika i dogovor sigurnosnih poveznica između sudionika. Navedeno okruženje zahtjeva da svaki od IPsec sudionika posjeduje implementaciju IKEv2 protokola u ravnini upravljanja kao što je objašnjeno u poglavlju Netlink usluga zaštite IP protokola.

ZEMRIS IKEv2 komponenta napisana je kao program otvorenog programskog kôda za porodice *Linux* i *Unix* operacijskih sustava. Dizajn izrade cjelokupne komponente omogućava jednostavnu nadogradnju i mogućnost ponovne uporabe programskog kôda i izgrađenih modula. Implementacija komponente obavljena je upotrebom programskog jezika C, a prenosivost kôda komponente ostvarena je upotrebom *GNOME Glib2* biblioteke opisane u [].

Dizajn ZEMRIS IKEv2 komponente u potpunosti je ostvaren modularno. Implementacija je podijeljena na nekoliko neovisnih modula opisanih u []. Svaki od tih modula točno definira sučelje prema ostatku sustava te tako pojednostavljuje međusobnu interakciju. Arhitektura ZEMRIS IKEv2 implementacije s pripadajućim modulima prikazana je na slici 6.1.

Središnji modul predstavlja podsustav koji implementira automate stanja (eng. *state machines – SM*) IKE komponente. Modul automata stanja prihvaća poruke ostalih modula te ih obrađuje i sukladno tome postavlja IKEv2 komponentu u određeno stanje. Interakcija se svodi na razmjenu sinkronih i asinkronih poruka između modula ili pozivanje specifičnih funkcija određenog modula.



Slika 6.1. Arhitektura implementacije IKEv2 protokola

Postojeća implementacija protokola u ZEMRIS IKEv2 projektu, za pristup adresama i parametrima mrežnih sučelja upotrebljava Netlink uslugu IP proslijeđivanja. Pristup sigurnosnim bazama u jezgri operativnog sustava IKEv2 implementacija obavlja upotrebom SAD i SPD modula. SAD i SPD moduli pozicionirani su kao međusloj između SDB (eng. *Security Database*) modula i specifične implementacije pristupa sigurnosnim bazama za pojedini operacijski sustav.

Pristup sigurnosnim bazama u IKEv2 implementaciji originalno je ostvaren upotrebom PF_KEYv2 sučelja []. PF_KEYv2 sučelje originalno potječe iz 4.4-Lite BSD okruženja te predstavlja jednostavno i pomalo zastarjelo sučelje za upravljanje i pristup sigurnosnim bazama. Prilikom praktičnog testiranja i upotrebe ZEMRIS IKEv2 komponente uočeno je

niz nedostataka navedenog sučelja. IKEv2 implementacija razvojem prati trenutne standarde IKEv2 protokola te je bilo neophodno obaviti migraciju na naprednije i skalabilnije rješenje. Zamjena pristupnog modula s PF_KEYv2 sučelja na Netlink sučelje ostvareno je u sklopu praktičnog rada kako je prikazano na slici 6.1.

Netlink poruke od IPsec komponente proslijeđivanja se zaprimaju i odašilju upotrebom pristupnog modula implementiranog pomoću Netlink XFRM sučelja. Pristupni modul zaprima sinkrone zahtjeve za obavljanje određene operacije nad sigurnosnim bazama od SAD i SPD modula. Dodatno pristupni modul obavlja obradu poruka asinkronih događaja od IPsec komponente proslijeđivanja. Nakon obrade poruka obavlja enkapsulaciju u `sdb_msg` tip poruka te odašilje središnjem modulu automata stanja. Međusobni komunikacijski kanal između navedenih modula predstavlja asinkroni red.

Uočena prednost pri upotrebi Netlink sučelja je ostvarenje asinkrone komunikacije s IPsec arhitekturom unutar jezgre operativnog sustava. Dodatna prednost naspram postojećeg PF_KEYv2 sučelja predstavlja podršku IKEv2 komponente u okruženju Mobile IP protokola.

6.3. Opis implementacije

SAD i SPD moduli ZEMRIS IKEv2 komponente u pripadajućim zaglavnim datotekama detaljno specificiraju generičko sučelje (eng. *interface*) prema sigurnosnim bazama. Za primjenu ZERMIS IKEv2 komponente u specifičnom okruženju operacijskog sustava, zahtijeva implementaciju navedenih sučelja. Ostvarena implementacija u praktičnom dijelu rada se u datoteci `<src/xfrm.c>` , a pomoćne funkcije i deklaracije funkcija nalaze se u zaglavnoj datoteci `<src/xfrm.h>`.

Ispis 25. prikazuje sučelje prema bazi sigurnosnih poveznica.

```
struct sad_op {
        void *priv_data;
        guint32 (*sad_getspi)(struct netaddr *, struct netaddr *,
                        guint8, guint8, guint32, guint32);
        void (*sad_update)();
        int (*sad_add)(struct sad_item *, struct netaddr *,
                        struct netaddr *, gboolean, gboolean);
        int (*sad_delete)(struct sad_item *, struct netaddr *,
                        struct netaddr *);
        void (*sad_get)();
        void (*sad_acquire)();
        void (*sad_register)();
        void (*sad_expire)();
        void (*sad_flush)();
        void (*sad_dump)();

        GSList *(*sad_transforms_get)();

        void (*sad_shutdown)(struct sad_op *sad_op);
        void (*sad_unload)(struct sad_op *sad_op);
};
```

Ispis 25. Sučelje za registraciju protokola za pristup SA bazi

Ispis 26. prikazuje sučelje prema bazi sigurnosnih poveznica.

```
struct spd_op {
        void *priv_data;

        void (*spd_update)();
        int (*spd_add)(struct spd_item *);
        int (*spd_delete)(struct spd_item *);
        void (*spd_get)();
        void (*spd_acquire)();
        void (*spd_register)();
        void (*spd_expire)();
        int (*spd_flush)();
        int (*spd_dump)(GSList **);

        void (*spd_running)();
        void (*spd_shutdown)();
        void (*spd_unload)();
};
```

Ispis 26. Sučelje za registraciju protokola za pristup SP bazi

6.4. Uspostava CHILD_SA poveznice

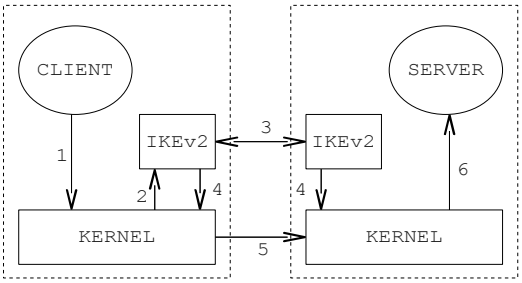
Uspostava CHILD_SA sigurnosne poveznice zahtjeva niz predradnji koje je potrebno obaviti od strane IKEv2 komponente. Za osnovno shvaćanje razmjene Netlink poruka između ravnine upravljanja i proslijeđivanja prilikom uspostave poveznice neophodno je opisati proces uspostave u potpunom IPsec okruženju.

U nastavku je opisan redoslijed obavljanja operacija prilikom dogovora CHILD_SA sigurnosne poveznice između dva IPsec sudionika upotrebom IKEv2 protokola. U nastavku je objašnjena i prikazana razmjena Netlink poruka između IKE komponente upravljanja i IPsec komponente ravnine proslijeđivanja prilikom dogovora i unosa CHILD_SA sigurnosne poveznice.

6.4.1. Uspostava CHILD_SA poveznice

Radi jednostavnijeg shvaćanja Netlink usluge zaštite IP protokola potrebno je objasniti interakciju između sudionika i način na koji se obavlja dogovor sigurnosnih parametara i ključeva.

Slika 6.2. prikazuje redoslijed obavljanja operacija u slijed komunikacije sigurnim kanalom. Klijentska aplikacija želi komunicirati sigurnim kanalom s aplikacijom na strani poslužitelja. Sigurnosna politika klijenta zahtijeva da navedena komunikacija bude zaštićena upotrebom algoritama za enkripciju i ovjeru. Prilikom odašiljanja prvog paketa (korak – 1) od strane klijentske aplikacije ravnina proslijeđivanja provjerava zapise u bazi sigurnosnih politika te zaključuje da je promet potrebno zaštiti. CHILD_SA sigurnosna poveznica opisuje način na koji je potrebno zaštiti promet. Kako se radi o prvom paketu navedene komunikacije baza sigurnosnih poveznica je trenutno prazna te ravnina proslijeđivanja o tome obavještava (korak – 2) komponentu za razmjenu ključeva ravnine upravljanja.



Slika 6.2. IPsec sustav

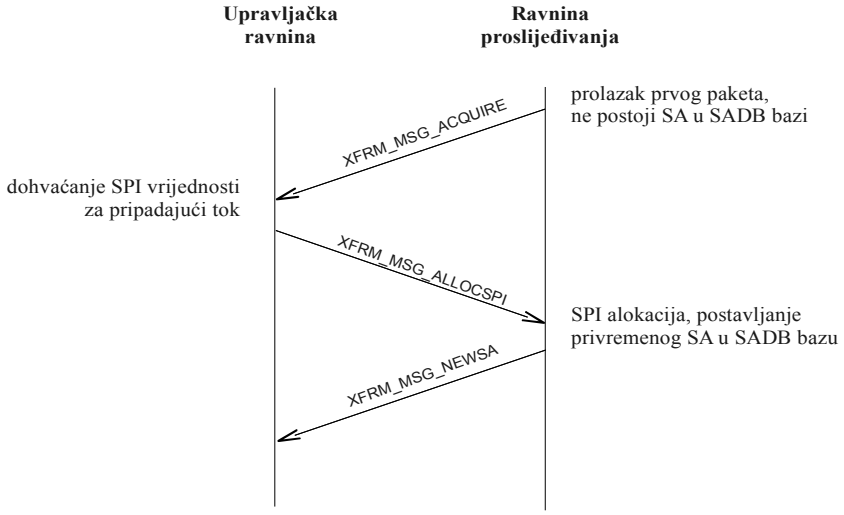
Komponenta za razmjenu ključeva, inicijator (eng. *IKE Initiator*) kontaktira komponentu za razmjenu ključeva odgovaratelja (eng. *IKE Responder*) na odredišnom poslužitelju i razmjenjuju poruke (korak – 3) s ciljem međusobne autentikacije i autorizacije te dogovora kriptografskih algoritama i enkripcijskih ključeva. Dogovorene parametre, komponenta ravnine upravljanja inicijatora i odgovaratelja šalje pripadajućoj ravnini proslijeđivanja koja parametre sprema u bazu sigurnosnih poveznica (korak – 4) kao CHILD_SA zapis. Navedena sigurnosna poveznica opisuje način zaštite prometa između sugovornika.

Upotrebom informacija iz CHILD_SA poveznice ravnina proslijeđivanja obavlja potrebne transformacije na toku podataka. Od ovog trenutka promet aplikacije klijenta prolazi zaštićen do poslužitelja (korak – 5) koji dostavlja nezaštićen promet do aplikacije na poslužitelju (korak – 6). Promet u obrnutom smjeru također je zaštićen, ali više nisu potrebne usluge komponenata za razmjenu ključeva jer je u prethodno opisanom procesu dogovorena CHILD_SA poveznica i na strani odgovaratelja.

6.4.2. Netlink razmjena poruka

Veliki dio implementacije upravljanja sigurnosnim bazama unutar IKEv2 implementacije odnosi se na upravljanje bazom sigurnosnih poveznica. Osnovna operacija IKE protokola je dogovor i uspostava sigurnosnih poveznica između IPsec sudionika. U nastavku je detaljno opisan redoslijed operacija i razmjena Netlink poruka između IKEv2 komponente upravljanja i IPsec komponente proslijeđivanja prilikom dogovora i unosa CHILD_SA sigurnosne poveznice.

Prilikom prolaska prvog paketa određenog toka podataka ravnina proslijeđivanja kontaktira bazu sigurnosnih politika. Sigurnosna politika specificira da se određena komunikacija mora zaštititi upotrebom enkripcijskih i ovjernih algoritama. Ukoliko je tok potrebno zaštititi tada se kontaktira baza sigurnosnih poveznica. Budući se radi o prvom paketu toka podataka baza sigurnih poveznica ne sadrži niti jedan zapis. Ravnina proslijeđivanja upotrebom poruke `XFRM_MSG_ACQUIRE` signalizira IKE komponenti da u bazi ne postoji pripadajuća sigurnosna poveznica za navedeni tok. Paket pripadajućeg toka je zaustavljen u IPsec komponenti koja očekuje postavljanje sigurnosne poveznice. Slika 6.3. prikazuje razmjenu poruka između IKE komponente upravljanja i IPsec komponente proslijeđivanja.

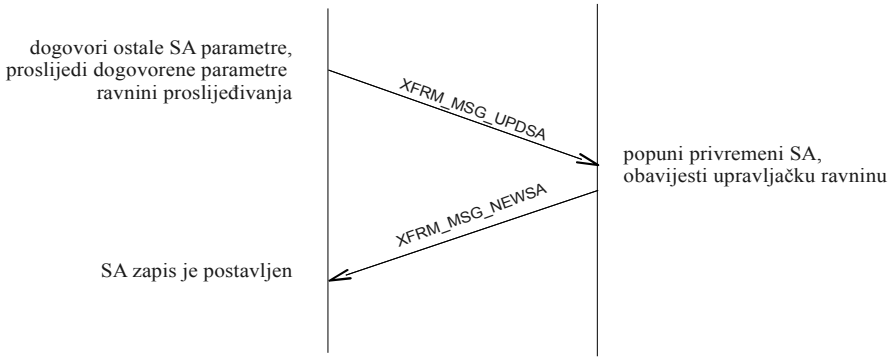


Slika 6.3. Razmjena poruka prilikom alokacije SPI vrijednosti

U okruženju s dinamičkom uspostavom sigurnosnih poveznica IKE komponenta zahtjeva vrijednost SPI parametra prije nego što su poznati ostali parametri sigurnosne poveznice. Prilikom uspostave CHILD_SA poveznice, u fazi 2 IKEv2 protokola zahtjeva se da IKE inicijator odašilje alociranu SPI vrijednost IKE komponenti odgovaratelja.

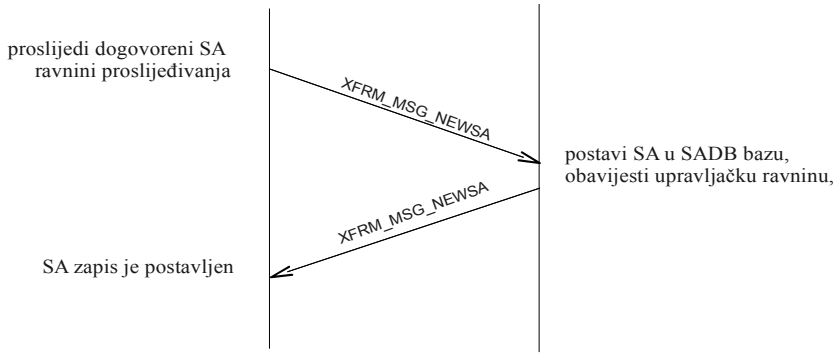
IKE komponenta upotrebom `XFRM_MSG_ALLOCSPI` tipa poruke traži SPI vrijednost od IPsec komponente. IPsec komponenta proslijeđivanja zauzima prostor za privremenu sigurnosnu poveznicu u bazi sigurnosnih poveznica i alocira SPI vrijednost poveznice. U privremenu sigurnosnu poveznicu postavlja se izvorišna i odredišna adresa te SPI parametar koju je IKE komponenta upravljanja poslala u strukturi `xfrm_userspi_info` kao teret poruke `XFRM_MSG_ALLOCSPI`. IPsec komponenta proslijeđivanja upotrebom `XFRM_MSG_NEWSA` poruke obavještava IKE komponentu o SPI parametru i privremenoj sigurnosnoj poveznici.

Ravnina proslijeđivanja očekuje popunjavanje privremene poveznice u određenom vremenu, u suprotnom se poveznica odbacuje iz baze kao neispravna. Nakon što su IKEv2 protokolom oba sudionika uspješno dogovorila parametre sigurnosne poveznice komponenta IKE implementacije odašilje `XFRM_MSG_UPDSA` poruku te obavještava ravninu proslijeđivanja o dogovorenim parametrima sigurnosne poveznice za koju je prethodno zatražena SPI vrijednost.



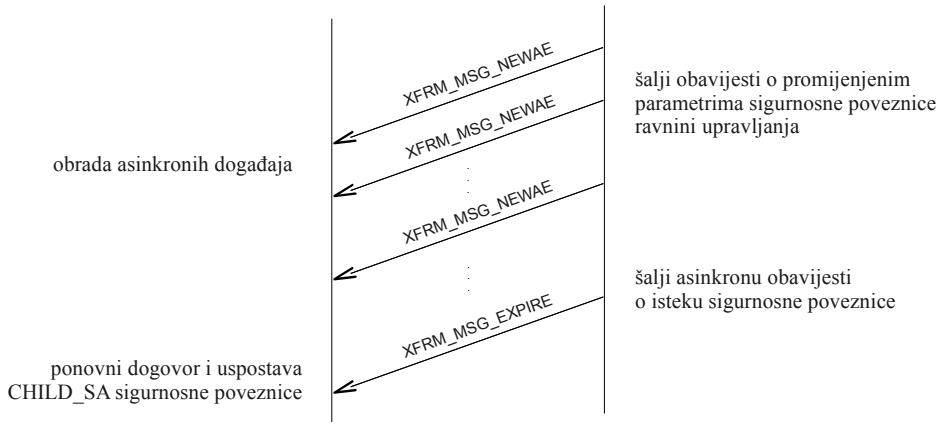
Slika 6.4. Razmjena poruka prilikom nadopune privremene sigurnosne poveznice

Ravnina proslijeđivanja postavlja parametre u već unijetu privremenu sigurnosnu poveznicu te odašilje komponentama ravnine upravljanja obavijest u obliku `XFRM_MSG_NEWSA` poruke. Drugi zapis CHILD_SA poveznice kreiran je u potpunosti u okruženju ravnine upravljanja te IKE komponenta šalje `XFRM_MSG_NEWSA` poruku ravnini proslijeđivanja i očekuje unos navedene sigurnosne poveznice u SAD bazu. Identično kao i u prošloj razmjeni, ravnina proslijeđivanja o unosu obavještava ravninu upravljanja `XFRM_MSG_NEWSA` tipom poruke. Slika 6.5. prikazuje razmjenu prilikom unosa CHILD_SA sigurnosne poveznice.



Slika 6.5. Razmjena poruka prilikom unosa sigurnosne poveznice

Rezultat navedenih koraka je uspješno postavljena CHILD_SA sigurnosna poveznica koja se sastoji od dva unosa u bazi sigurnosnih poveznica. Kao što je prethodno navedeno, da bi se omogućila dvosmjerna komunikacija između IPsec sudionika potrebna su dva unosa sigurnosne poveznice u bazi. IPsec komponenta ravnine proslijeđivanja ima sve potrebne informacije te obavlja transformacije nad paketima koje je potrebno zaštiti, tj. omogućena je prolazak paketa kroz ravninu proslijeđivanja.



Slika 6.6. Razmjena asinkronih poruka

Prilikom svakog prolaska paketa kroz IPsec komponentu ravnine proslijeđivanja, komponenta obavlja ažuriranje promjenjivih parametara za određenu sigurnosnu poveznicu kao što su broj okteta koji su prošli IPsec komponentom. O trenutnom stanju promjenjivih parametara ravnina prosljeđivanja upotrebom asinkrone poruke tipa `XFRM_MSG_NEWAE` obavještava komponente ravnine upravljanja. Dodatno, pri isteku prethodno namještenih ograničenja nekog parametra potrebno je obaviti ponovni dogovor CHILD_SA sigurnosne poveznice. Upotrebom asinkrone poruke `XFRM_MSG_EXPIRE` IPsec komponente proslijeđivanja obavještava komponente upravljanja da je došlo do isteka sigurnosne poveznice. Pri tome komponente upravljanja obavljaju ponovni izračun ključeva.

7. Zaključak

Zadatak diplomskog rada bilo je ostvariti upravljanje sigurnosnim bazama u okruženju implementacije IKEv2 protokola za razmjenu ključeva. U teoretskom razmatranju opisan je Netlink sustav zajedno s pripadajućim XFRM sučeljem za pristup sigurnosnim bazama. Tijekom praktičnog dijela rada u potpunosti je ostvareno navedeno upravljanje i testirano u praktičnom okruženju.

Upotreba Netlink XFRM sučelja za upravljanje sigurnosnim bazama u IKEv2 implementaciji donosi niz prednosti nad postojećim PF_KEYv2 sučeljem. Omogućen je prihvat asinkronih poruka od IPsec arhitekture što osigurava povećanje performansi IKEv2 komponente. Implementacijom Netlink sustava za pristup bazama osigurani su svi preduvjeti za daljnji razvoj i nadogradnju IKEv2 implementacije protokola za razmjenu ključeva u smjeru okruženja pokretljivosti u mreži.

8. Literatura

1. Khosravi H., Anderson T., *Requirements for Separation of IP Control and Forwarding,* RFC3654, November 2003.
2. Baker F., Cisco Systems, *Requirements for IP Version 4 Routers*, RFC1812, June 1995.
3. Salim J., Khosravi H., Kleen A., Kuznetsov. A., *Linux Netlink as an IP Service Protocol,* RFC 3549, July 2003.
4. Perkins C., Nokia Research Center, *IP Mobility Support for IPv4*, RFC3344, August 2002.
5. McDonald D., Metz C., Phan B., *PF_KEY Key Management API, Version 2*, RFC2367, July 1998.
6. Schiller J., *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2),* RFC4307, December 2005.
7. Kent S., BBN Corp, Atkinson R., *Security Architecture for the Internet Protocol,* RFC2401, November 1998
8. Kent S., Seo K., *Security Architecture for the Internet Protocol,* RFC4301, December 2005.
9. Eronen P., *IKEv2 Mobility and Multihoming Protocol (MOBIKE), RFC4555, June 2006.*
10. Groš S., Glavinić V., *Architecture of an IKEv2 protocol implementation*, May 2007.