VISOKA ŠKOLA STRUKOVNIH STUDIJA ZA INFORMACIONE TEHNOLOGIJE

Računarske mreže

Seminarski rad

IP Security

Predmetni nastavnik:
prof. dr Slavko Pokorni, dipl. inž. el.

Student:
Šandor Lajko
Datum predaje
2.7.2010.

REZIME

U uvodu je opisan razlog i istorijat razvoja IPsec protokola.

Nakon kratog objašnjenja načina na koji IPsec funkcioniše, u poglavlju *Osnovni IPsec protokoli* prikazuju se *Authentication Header (AH)* i *Encapsulating Security Payload (ESP)*. Poglavlje *Pomoćne IPsec komponente* prikazuje pomoćne tehnologije, koje su neophodne za funkcionisanje AH i ESP. U sledeća dva poglavlja objašnjeni su metodi implementacije i arhitekture za implementaciju IPsec bezbednosti. Poglavlje *IPsec modovi* bavi se modovima putem kojih IPsec protokoli pružsju bezbenost IP komunikaciji. U poglavlju *Mehanizmi bezbednosti IPsec protokola* predstavljaju se pojmovi *bezbednosne polise* i *bezbednosne asociacije*, kao i upravljanje bazama podataka u kojima se skladište. Poglavlje *Razmena ključeva u IPsec protokolu* govori o IKE protokolu za razmenu kriptografskih ključeva. Poglavlje *NAT traversal problem* bavi se nezgodnim osobinama IPv4 implementacije IPsec protokola. U delu *Primena IPsec protokola u izgradnji IP paketa*, uz pomoć ilustracija prikazani su razni načini na koje se IPsec zaglavlja raspoređuju unutar obezbeđenog IP paketa. Na kraju, poglavlje *IPsec standardi* nabraja dokumente u kojima su definisane osobine ovog standarda.

Ključne reči: IP security, IPsec, Authentication Header, Encapsulating Security Payload, Internet Key Exchange

SADRŽAJ

UVOD

ARPANET, preteča današnjeg Interneta, nastao je šezdesetih godina dvadesetog veka, kao projekat ministarstva odbrane Sjedinjenih Američkih Država. Agencija DARPA (Defence Advanced Research Projects Agency) razvijala je novi tip mrežne arhitekture, čiji je glavni cilj bio uspostavljanje posredne komunikacije između čvorova. U vremenu velikog straha od nuklearnih sukoba, vojska je htela da napravi mrežu koja bi funkcionisala čak i ako dođe do uništenja infrastrukture čitavog jednog grada. APANET je osmišljen kao međumreža, način povezivanja lokalnih mreža u postojećim vojnim objektima. Vremenom, u ARPANET su priključene i akademske mreže mnogih univerziteta u Sjedinjenim Državama. Već tada, postao je vidljiv jedan od glavnih nedostataka osnovnog seta mrežnih protokola; TCT/IP stek ne sadrži adekvatne mehanizme za sigurnost i bezbednost podataka koji se prenose. To u samom početku i nije bilo portebno. Svi čvorovi međumreže nalazili su se na lokacijama koje su bile poznate i fizički obezbeđene. Ovaj nedostatak u bezbednosti najpre je rešen podelom međumreže; vojne instalacije izdvojene su u MILNET mežu, a civilni deo zadržao je naziv ARPANET. To je rešilo probleme zaštite strateški važnih informacija, ali je TCP/IP i dalje ostao nepromenjen. Kako je u daljnjem periodu civilni deo doživeo veliku ekspanziju, vremenom je prihvaćen i naziv Internet, kao (među)mreža svih mreža. Pojava e-biznisa i prometa novca putem Interneta zahevala je razvoj metoda koji koriguju nedostatak bezbednosti u internet protokolima.

Tokom godina nastao čitav niz rešenja koja se bave sigurnošću i bezbednošću. Većina ovih rešenja odnose se na više nivoe OSI mrežnog modela, čime se kompenzuju nedostaci IP (mrežnog) protokola. Ovakva rešenja su veoma praktična za neke primene, ali im nedostaje element univerzalnosti. SSL (Secure Socets Layer) je, na primer, vrlo dobar za primenu na World Wide Web-u, ali nije praktičan za mnoge druge svrhe. Ukazala se potreba za načinom obezbeđivanja komunikacije na mrežnom nivou, koji bi mogao transparentno da bude korišćen od strane viših nivoa OSI modela.

Kako je postalo očigledno da IPv4 pati od manjka mogućih Internet adresa, pristupilo se definisanju novog standarda za mrežnu komunikaciju. Izrada IPv6 protokola bila je i idealna prilika da se reše i drugi nedostaci IP standarda, pa je poseban akcenat stavljen i na sigurnost i bezbednost podataka. Tehnologija koja je razvijena u tom cilju nazvana je IP Security, ili skraćeno IPsec. Pošto je razvoj i primena IPv6 standarda spor i mukotrpan proces, IPsec je dizajniran tako da bude primenljiv kako u IPv6, tako i u IPv4 komunikaciji.

U ovom radu predstaviću koncepte i tehnike koje se primenjuju u oviru IP Security standarda, njegove gradivne elemente i načine na koji se on upotrebljava.

IP SECURITY

IETF (*Internet Engeneering Task Force*) je dizajniranje IPsec standarda počeo 1992. godine, kao naslednika ISO standarda NLSP (*Network Layer Security Protocol*). Sam NLSP je bio baziran na SP3 protokolu, kojeg je objavio NIST (*National Institute of Standards and Technology*), a razvijen je u okviru *Secure Data Network System* projekta američke agencije za nacionalnu bezbednost (NSA).

Od samog početka IPsec je razvijan kao otvoreni standard, koji je pod stalnim nadzorom javnosti. Ovakva otvorenost pri razvoju kriptografskih algoritama je neophodna i mnogo efikasnija od vlasničkih rešenja. Cilj je svođenje rizika na najmanju meru. Upotrebom otvorenog standarda, poput IPsec, dobija se mnogo jača garancija da su algoritmi i protokoli dovoljno kvalitatno osmišljeni. Naravno, to samo po sebi nije garancija bezbednosti, pošto ona u najvećoj meri zavisi od konkretne implementacije. Takođe, može se pojaviti i novi tip napada koji nije predviđen pri dizajnu standarda, ali otvoreni standardi ipak predstavljaju dokaz da su algoritmi i protokoli odoleli visokom nivou analiza i testiranja.

Način funkcionisanja IPsec-a

IPsec pruža bezbednosne servise na IP sloju, koje ostali TCP/IP protokoli mogu da koriste. Ovo znači da IPsec sadrži alate koji su neophodni uređajima u TCP/IP mreži, kako bi mogli da komuniciraju na bezbedan način. Da bi dva uređaja započela bezbednu komunikaciju, oni moraju između sebe da stvore bezbedni putanju, koja može da prolazi kroz brojne neobezbeđene međusisteme. Ovo se najjednostavnije postiže izvršavanjem sledećih koraka:

1. Uređaji moraju da se dogovore o skupu bezbednosnih protokola koje će koristiti, kako bi podaci bili poslati u formatu koji će druga strana moći da razume.
2. Moraju da odluče koji će se algoritam za šifrovanje koristiti.
3. Moraju da razmene ključeve neophodne za dešifrovanje kodiranih podataka.
4. Kada se ovaj pozadinski proces okonča, uređaji moraju da upotrebe dogovorene protokole, metode i ključeve za šifrovanje podataka i njihovo slanje kroz mrežu.

Da bi poržao ove korake, IPsec sadrži skup različitih komponenti, koje se nazivaju *osnovni IPsec protokoli* (core protocols).

Osnovni IPsec protokoli

Dve osnovne tehnologije unutar IPsec protokola, koje pružaju bezbednost prenosa putem šifrovanja podataka su IPsec Authentication Header (AH) i Encapsulating Security Payload (ESP).

- ***IPSec Authentication Header (AH):*** Ovaj protokol se koristi za obezbeđivanje ***autentifikacije*** u IPsec-u. Uz pomoć autentifikacije, primalac poruke može da se uveri u identitet pošaljioca poruke. Takođe, primalac može da proveri dali je neki deo datagrama promenjen na putu od pošaljioca. AH sadrži i mehanizme za odbranu od takozvanih „replay" napada, kada neautorizovani korisnik može da presretne poruku, i zatim je kasnije ponovo pošalje primaocu. Authentication Header obezbeđuje integritet podataka u datagramu, ali ne štiti njegovu privatnost.

- ***Encapsulating Security Payload (ESP):*** Kada je neophodno da se sačuva privatnost podataka, koristi se ESP protokol, koji šifruje celokupni sadržaj IP datagrama. Pored enkripcije, ESP opciono može da vrši i autentifikaciju, koristeći isti proces kao i AH. Međutim, ESP autentifikacija ne pokriva ceo IP paket, već samo ESP zaglavlje i šifrovani sadržaj paketa. U praksi se pokazalo da ovo ne umanjuje previše bezbednost autentifikacije.

AH i ESP nazivaju „protokolima", ali se u praksi implementiraju kao zaglavlja koja se dodaju na IP datagram. Oni se mogu upotrebiti i istovremeno, i na taj način osiguravati i autentifikaciju i privatnost, ali se to u praksi retko dešava. Da bi ova zaglavlja pravilno funkcionisala, neophodna je podrška još nekih pomoćnih protokola i servisa.

Pomoćne IPsec komponente

Među najvažnije pomoćne komponente IPsec protokola spadaju:

- ***Algoritmi za šifrovanje:*** AH i ESP protokoli ne specificiraju konkretan mehanizam za enkripciju. Ovim je postignuta fleksibilnost za rad sa velikim brojem takvih algoritama, i mogućnošću njihovog odabira u skladu sa potrebama. Algoritmi koji se najčešće koriste u IPsec komunikaciji su *Message Digest 5* (MD5) i *Secure Hash Algorithm 1* (SHA-1). Ovo su heš algoritmi za jednosmernu enkripciju. Heš algoritmi koriste formulu pomoću koje se na osnovu ulaznih podataka i ključa. Mogu se koristiti samo za verifikaciju podataka, pošto se na osnovu dobijenog heš koda ne mogu rekonstruisati podaci iz kojih je on izračunat.

- ***Bezbednosne polise i asociacije, i metode za menadžment:*** IPsec dizajniran da bude fleksibilan, i dozvoljava mrežnim uređajima da odlučuju o načinu na koji će da primene mere bezbednosti. Zbog toga je neophodan način za praćenje bezbednosnih relacija između uređaja. Ovo se postiže upotrebom bezbednosnih asociacija i polisa, i uređenim metodama njihove razmene.

- ***Mehanizam za razmenu ključeva:*** Da bi dva uređaja mogla da razmenjuju šifrovane poruke, moraju da razmemenjuju ključeve za dešifrovanje poruka. Potreban im je i način za razmenu bezbednosnih asocijacija. Internet Key Exchange (IKE) je protokol koji u IPsec-u obezbeđuje ove zadatke.

Metodi za IPsec implementaciju

Postoji nekoliko načina za implementaciju IPsec protokola u TCP/IP mreže, koji su opisani u RFC 2401. Izbor implementacije zavisi od verzije IP koji se koristi, zahteva koje mreža treba da ispuni, finansijskih mogućnosti, itd. Bitno pitanje u procesu implementacije IPsec protokola je da li treba zaštititi i saobraćaj unutar lokalne mreže, ili samo komunikacija sa računarima izvan lokalne mreže. IPsec se može implementirati na svim hostovima u mreži, ili samo u ruterima.

Implementacija u hostovima (End Host Implementation): Ugrađivanje IPsec-a u sve host uređaje na mreži daje najveću fleksibilnost i bezbednost. Međutim, u mreži može biti veliki broj različitih hostova, pa ovakvo rešenje znači i puno više posla oko njenog konfigurisanja i održavanja.

Implementacija u ruterima je mnogo jednostavnija za realizaciju, pošto se promene moraju izvesti samo u nekoliko rutera, umesto u nekoliko desetina (ili stotina) pojedinačnih uređaja. Na ovaj način se štiti samo saobraćaj između parova rutera koji koji su osposobljeni za IPsec, ali je to dovoljno za veliki broj primena, poput virtualnih privatnih mreža. Ovakvi ruteri po pravilu štite datagrame na delu puta izvan organizacije, dok saobraćaj između rutera i hostova ostaje nebezbedan (ili se štiti na neki drugi način).

IPSec arhitekture

Postoje tri različite arhitekture koje opisuju načine za primenu IPsec protokola u TCP/IP steku.

Integrisana arhitektura predstavlja idealan način za integraciju IPsec protokola direktno u sam IP. Na ovaj način se bezbednost koristi jednostavno kao i običan IP. Nema potrebe za dodatnim hardverom ili slojevima u arhitekturi. Na žalost, ova arhitektura je najčešće moguća samo sa "čistim" IPv6 mrežama. Kod IPv4, integracija zahteva intervencija na svakom uređaju u mreži, a to je nepraktično, skupo i teško za realizaciju.

"Bump In The Stack" (BITS) arhitektura: kod ove tehnike, IPsec se uvodi kao poseban sloj (layer) između mrežnog sloja i sloja veze. IPsec presreće datagrame koji se kreću niz slojeve steka protokola, i primenjuje na njih mehanizme bezbednosti, pre nego što ih prosledi sloju veze. Prednost ovakvog pristupa je što se IPsec nadograđuje na bilo koji IP uređaj, pošto su njegove funkcije odvojene od IP protokola. Nedostatak u poređenju sa integrisanom arhitekturom predstavlja dupliranje obrade datagrama. BITS arhitektura se primenjuje kod IPv4 mreža.

"Bump In The Wire" (BITW) arhitektura je slična BITS-u, sa tom razlikom da se IPsec funkcionalnost izdvaja u poseban hardverski uređaj. Ovakav specializovani IPsec uređaj postavlja se između rutera i prokljućka na internet. Na ovaj način se bezbednos postojeće mreže vrlo jednostavno može unaprediti, bez promene na hardveru ili softveru koji već funkcionišu. Nedostatak ovakvog pristupa je jedino cena samog dodatnog uređaja.

IPSec modovi: Transportni i Tunel mod

U okviru IPsec protokola definisana su dva moda za njegovu primenu. Ovi modovi su usko povezani sa osnovnim protokolima *Authentication Header* (AH) i *Encapsulating Security Payload* (ESP). Oba osnovna protokola pružaju zaštitu za IP datagram dodavanjem zaglavlja koje sadrži informacije o bezbednosti. Odabirom moda određujemo koji deo datagrama želimo da zaštitimo i kakav će ta bude redosled ovih zaglavlja, ali ne utičemo na metod generisanja ovih zaglavlja. IPsec mod se koristi kao osnova za definisanje bezbednosnih asocijacija (*security associations - SAs*).

Transportni mod

U transportnom modu IPsec štiti sadržaj koji u IP stiže sa transportnog sloja. Sadržaj se zatim obrađuje od strane AH ili ESP, i njihova zaglavlja se dodaju ispred transportnog (TCP ili UDP) zaglavlja. Standardno IP zaglavlje se dodaje ispred IPsec zaglavlja. Kada se koristi transportni mod, IPsec se primenjuje samo na sadžaj IP paketa, a ne i na IP zaglavlje. AH i ESP zaglavlja se postavljaju između sadržaja IP paketa i IP zaglavlja.

Tunel mod

U tunel modu IPsec zaštita se primenjuje na kompletan datagram, nakon formiranja IP paketa. IPsec zaglavlje se postavlja ispred originalnog IP zaglavlja. Zatim se generiše novo IP zaglavlje koje se postavlja ispred IPsec zaglavlja. Na ovaj način se obezbeđuje kompletan originalni IP datagram, koji se zatim pakuje u nov IP datagram.

Dakle, tunel mod primenjuje mehanizme bezbednosti na kompletan IP datagram, a transporni mod samo na njegov deo. U slučaju IPv4, hederi se postavljaju u sledećem redosledu:

Transportni mod:

IP heder	IPsec hederi (AH i/ili ESP)	sadržaj IP paketa (payload)

Tunel mod:

novi IP heder	IPsec hederi (AH i/ili ESP)	stari IP heder	sadržaj IP paketa (payload)

Kod IPv6, primena je veoma slična. Najveća razlika je u tome, što IPv6 koristi zaglavlja za proširenja (*extension headers*), koja prilikom upotrebe IPsec-a moraju da se postave u određeni redosled. Prvo seređaju zaglavlja koje se menjaju tokom rutiranja paketa (*mutable field headers*), a iza njih fiksna zaglavlja (*immutable field headers*). U praksi, zaglavlja se nalaze u sledećem redosledu:

Transportni mod:

IP heder	promenljiva zaglavlja	IPsec hederi (AH i/ili ESP)	nepromenljiva zaglavlja	sadržaj IP paketa (payload)

Tunel mod:

novi IP heder	nova zaglavlja za proširenja	IPsec hederi (AH i/ili ESP)	stari IP heder	stara zaglavlja za proširenja	sadržaj IP paketa (payload)

Ovi prikazi redosleda su uproščeni za lakše razumevanje, u realnosti je proces generisanj zaglavlja mnogo komplikovaniji. Takođe, moguće je koristiti AH i ESP istovremeno (mada nije uobičajeno). Tada AH zaglavlje uvek dolazi ispred ESP zaglavlja. U slučaju upotrebe ESP protokola, mora postojati završni blok (*ESP trailer*), koji se nalazi iza šifrovanih podataka.

Iz svega do sada opisanog vidimo da postoji mnogo opcija za implementaciju IPsec zaštite. Na raspolaganju su tri mogućnosti za osnovni protokol (AH, ESP ili AH+ESP), dva IPsec moda (transportni ili tunel), pa još i dve vrste IP protokola na koje se sve to primenjuje (IPv4 ili IPv6). Koja od ovih kombinacija će se upotrebiti zavisi od konkretnih potreba. Transportni mod zahteva dodavanje IPsec zaglavlja u procesu kreiranja originalnog IP paketa, i zato se koristi kod integrisane arhitekture. U tunel modu se već gotov IP datagram učaurava u IPsec paket, pa se ovaj mod može primeniti kod BITS i BITW arhitektura, i najčešće se upotrebljava u VPN rešenjima (virtualne privatne mreže).

Mehanizmi bezbednosti IPsec protokola

Osnovni elementi bezbednosti u IPsec protokolu su bezbednosne asociacije (*Security Associations - SA)* sa bazom bezbednosnih asociacija (*Security Association Database - SAD*), bezbednosne polise (*Security Policies - SP*) sa bazom bezbednosnih polisa (*Security Policy Database - SPD*) i selektori. Svi ovi pojmovi su veoma slični i usko povezani, ali se moraju razumeti i razlikovati da bi se shvatio način funkcionisanja samih baznih IPsec protokola. Ovi elementi upravljaju opštim funkcionisanjem IPsec-a, kao i specifičnom razmenom podataka između uređaja.

Mehanizmi bezbednosti dobijaju pravi smisao kada posmatramo komunikaciju na uređaju koji razmenjuje podatke sa mnogo različitih uređaja. Primena bezbednosti na IP pakete zahteva slanje dodatnih informacija, koje opterećuju uvek tesan propusni opseg mreže. Samo tumačenje obezbeđenih podataka zahteva neko vreme, što takođe usporava saobrećaj. Zbog toga nije dobro obezbeđivati svaki paket koji ulazi ili izlazi iz uređaja. Neki podaci zahtevaju visok nivo bezbednosti, a drugi znatno manji. Pored toga, komunikacija sa raznim uređajima često zahteva različite načine obrade.

Da bi omogućio upravljanje ovako kompleksnim sistemom komunikacije, IPsec je opremljen moćnim i fleksibilnim načinom za specifikaciju metoda obrade različitih tipova datagrama. Za razumeli ovih funkcionalnosti, moramo definisati dva važna logička koncepta, a to su *bezbednosne polise* i *bezbednosne asociacije*.

Bezbednosne polise

Bezbednosna polisa (SP) je pravilo koje je programirano u IPsec implementaciju, i određuje na koji način se obrađuju razni datagrami koje uređaj prima.

Na primer, bezbednosna polisa se koristi u odlučivanju da li određeni paket uopšte treba da se obrađuje od strane IPsec-a. Ako ne treba da se obredi, paket u potpunosti zaobilazi AH i ESP. Ukoliko je bezbenost neophodna, polisa sadrži opšte smernice o tome kako ona treba da se primeni, i, ako je potrebno, pokazuje na mesto gde je detaljnije opisana procedura. Bezbednosne polise koje uređaj poznaje čuvaju se u bazi bezbednosnih polisa uređaja, *Security Policies Database* (SPD).

Bezbednosne asociacije

Bezbednosna asociacija (SA) je skup bezbednosnih informacija koje opisuju vrstu bezbedne veze između jednog uređaja i drugog. Ona predstavlja specifikaciju konkretnih bezbednosnih mehanizama koji se koriste u komunikaciji među njima. Bezbednosne asocijacije koje uređaj upotrebjava čuvaju se u bazi bezbednosnih asocijacija uređaja, *Security Associations Database* (SAD).

SPD i SAD prate jako sličan koncept, pa ih je dosta teško razlikovati. Osnovna razlika među njima je njihova određenost. Bezbednosne polise sadrže opšta pravila za obradu datagrama, a bezbednosne asociacije pravila za komunikaciju sa određenim uređajem. Da bi odredio šta da uradi sa pristiglim datagramom, uređaj najpre proverava SPD. Polise koje se tu nalaze mogu da referenciraju određenu asociaciju u SAD. Ako takva referenca postoji, uređaj pronalazi bezbednosnu asociaciju, i koristi je daljnju obradu datagrama.

Selektori

Selektori se koriste da bi uređaj mogao da odredi koju polisu ili asociaciju treba da koristi za određeni datagram. IPsec definiše veoma fleksibilan sistem koji dozvoljava svakoj bezbednosnoj asociaciji da definiše skup pravila za odabir datagrama na koje se SA odnosi. Svaki od ovih skupova pravila naziva se selektor. Na primer, možemo napraviti selektor kojim definišemo da na datagram, koji ima izvornu adesu (*source address*) u određenom opsegu adresa, kombinovanu sa odredišnom adresom (*destination address*) određene vrednosti, mora biti primenjena specifična bezbednosna asociacija.

Svaka bezbedna komunikacija koju uređaj ostvari sa drugim uređajem zahteva uspostavljanje bezbednosne asociacije. Ove asociacije su jednosmerne i svaka reguliše ili dolazeći, ili odlazeći saobraćaj prema nekom uređaju. Na ovaj način moguće je ostvariti različite nivoe bezbednosti za tok podataka od uređaja A do uređaja B, i od uređaja B prema uređaju A. Prilikom ovakve dvosmerne komunikacije, svaki od uređaja stvara po dve bezbednosne asociacije, jednu za ulaznu i jednu izlaznu.

Triplet bezbednosne asociacije i Security Parameter Index (SPI)

Bezbednosne asociacije (SA) koje su uskladištene u bazi bezbednosnih asociacija (SAD) nemaju svoj naziv. One se definišu skupom tri parametra, koji se nazivaju *triplet*:

- **Security Parameter Index (SPI):** 32-bitni broj koji se odabira da jednoznačno obeleži određenu SA za svaki povezani uređaj. SPI se smešta u AH ili ESP zaglavlje i na taj način pravi vezu za svaki IPsec paket sa bezbednosnom asociacijom. Koristi ga primalac paketa da bi znao koji SA se koristi za njegovo tumačenje.
- **Ciljna IP adresa** (IP Destination Address): Adresa uređaja sa kojim je bezbednosna asociacija uspostavljena.
- **Security Protocol Identifier:** Određuje da li je asociacija namenjena za AH ili ESP. Kada se u komunikaciji koriste oba protokola, svaki od njih zahteva posebnu bezbednosnu asociaciju.

Funkcionisanje oba bezbednosna protokola, AH i ESP, zavise od bezbednosnih asociacija i polisa, i baza podataka koje kontrolišu njihovu upotrebu. Upravljanje ovim bazama je veoma važno, i predstavlja jednu od kompleksnijih oblasti implementacije IPsec-a. Bezbednosne asociacije mogu da se definišu manuelno, što je dosta obiman dodatni posao, ili može da se uptrebi neki od automatizovanih sistema, kakav je IKE.

Razmena ključeva u IPsec protokolu

IPsec bezbednost se bazira na konceptu "deljene tajne". Dva uređaja koja bezbedno komuniciraju, šifriraju i dešifruju podatke pomoću informacije koja je samo njima poznata. Neko ko nije upozanat sa ovom tajnom može da presretne ove podatke, ali ne može da ih protumači (ako se pomoću ESP šifrira sadržaj), ili ne može da ih neopaženo promeni (ako se koristi AH osnovni protokol). Pre nego što se primeni AH ili ESP protokol, oba uređaja koji komuniciraju moraju podele "tajnu", odnosno opis bezbednosnih protokola koje će koristiti u razmeni podataka. IPsec u ovu svrhu najčešće koristi pomoćni protokol IKE (*Internet Key Exchange*).

IKE je definisan u ***RFC 2409*** i predstavlja IPsec komponentu koja je verovatno najteža za razumevanje. Duboko razumevanje ovog mehanizma zahteva obimno teoretsko znanje iz oblasti kriptografije. Zbog toga ću ovde opisati samo osnove njegovog funkcionisanja i način na koji se upotrebljava.

IPsec key Exchange (IKE)

Namena IKE je da uređajima omogući razmenu neophodnih informacija za uspostavljanje bezbedne komunikacije. Ovo se postiže upotrebom ključeva za šifrovanje autentifikacionih podataka i sadržaja IP paketa. Funkcionalnost IKE protokola odnosi se na razmenu bezbednosnih asociacija između IPsec uređaja, i popunjavanje njihovih baza asociacija. Ove asociacije se nakon toga koriste u razmeni datagrama koji su obezbeđeni putem AH ili ESP protokola. IKE je hibridni protokol, i kombinuje funkcionalnosti tri druga protokola.

Prvi od ovih protokola je *Internet Security Association and Key Management Protocol* (ISAKMP). On predstavlja okvir (framework) za razmenu kriptografskih ključeva i informacija za bezbednosne asociacije. Bezbednosne asociacije se uspostavljaju procesom dogovaranja između uređaja, koji se odvija u više faza. ISAKMP je generički protokol koji podržava različite metode za razmenu klučeva. U okviru IKE, ISAKMP framework se koristi kao osnova za specifičan metod razmene, koji kombinuje funkcionalnosti dva druga protokola za razmenu ključeva:

- ***OAKLEY:*** Opisuje konkretan mehanizam razmene ključeva definisanjem različitih „modova" za njihovu razmenu. Veći deo IKE razmene je baziran na ovom protokolu.
- ***SKEME:*** Opisuje mehanizam za razmenu ključeva drugačiji od OAKLEY protokola. IKE koristi neke funkcionalnosti SKEME-a, kao što je njegov metod enkripcije javnim ključem, i mogućnost brze zamene upotrebljenih ključeva.

Način funkcionisanja IKE

U procesu dogovaranja i razmene ključeva između dva uređaja, po ISAKMP specifikaciji postoje dve faze:

- ***ISAKMP faza 1:*** Tokom prve faze urađaji se dogovaraju oko načina za daljnju razmenu podataka. Naziva se još i *Setup* faza. Prilikom ovog dogovaranja, uređaji stvaraju SA (bezbednosnu asociaciju) za upotrebu u samom ISAKMP procesu. Ova asociacija se zatim koristi za bezbednu razmeni detaljnijih informacija u fazi 2.

- ***ISAKMP faza 2:*** Tokom ove faze se SA koja je uspostavljena u fazi 1 koristi za stvaranje bezbednosnih asociacija za druge protokole bezbednosti. U ovoj fazi se kreiraju parametri za konkretne SA koje koriste AH i ESP.

Nakon završene faze 1, moguće je ostvariti više ciklusa dogovaranja faze 2. Mada su u IPsec-u bezbednosne asociacije uvek jednosmerne, SA koji se uspostavlja u ISAKMP fazi 1 je dvosmerna. Kada se jednom uspostavi SA za razmenu ključeva u fazi 1, dozvoljen je i pojednostavljen metod dogovaranja u fazi 2. Parametri koji se ugovaraju u ISAKMP fazi 2 su:

- ***Algoritam enkripcije*** koji će se koristiti za šifrovanje podataka. Postoji više standarda koje IPsec podržava, među kojima su DES (Digital Encryption Standard), AES (Advanced Encryption Standard), Blowfish i drugi.
- ***Heš algoritam.*** Ovo je algoritam jednosmerno šifrovanje podataka i obično se koriste MD5 (*Message Digest 5*) ili SHA-1 (*Secure Hash Algorythm 1*).
- ***Metod autentikacije***, poput autentikacije korišćenjem prethodno dogovorenih ključeva.
- ***Diffe-Hellman grupa***. Diffie i Hellman su pioniri kriptografske industrije koji su izmislili kriptografiju javnim ključem. Kod ovog tipa enkripcije postoje različiti ključevi šifrovanje i dešifrovanje podataka. Podaci šifriraju javnim ključem koji je svima dostupan, ali se dešifruju privatnim ključem koji se drži u tajnosti. Diffie-Hellman grupa definiše atribute na osnovu kojih se primenjuje ovakav tip kriptografije.

IKE razmena ključeva može se koristiti u dva moda operacije. Na ovaj način se raguliše balans između efikasnosti i bezbednosti. ***Main*** mod je standardni postupak razmene, i u ovom modu se između uređaja šalje šest paketa da bi se uspostavile bezbednosne asociacije. U ***Agressive*** modu se razmenjuje samo tri paketa, ali se time žrtvuje na bezbednosti, pošto se deo informacija prenosi u čitljivoj formi.

NAT traversal problem

AH vrši veoma snažno obezbeđenje sadržaja paketa zato što pokriva sve njegove elemente kod kojih može da dođe do zloupotrebe. Ovo je sasvim prirodno za IPv6, ali je prouzrokovalo veliki problem kod IPsec implementacije u IPv4 protokolu.

NAT (*Native Address Translation*) se koristi da bi se mapirao opseg privatnih adresa u LAN mreži na jednu, ili mali broj javnih IP adresa, i time se štede javne IP adresa. U ovom procesu, NAT uređaj menja zaglavlje IP paketa promenom ciljne ili odredišne IP adrese. Prolazak kroz NAT uređaj se takođe računa kao hop, pa dolazi i do promene TTL vrednosti. Prilikom ovih promena mora da se izvrši ponovno računanje *header checksum* polja. Pošto se *TTL* i *header checksum* uvek menjaju tokom rutiranja paketa, ova polja se ne pokrivaju AH autentifikacijom. Međutim, promena IP adrese u zaglavlju paketa dovodi do neslaganja sa AH ICV (*Integrity Check Value*) vrednošću, i zato paket obavezno pada prilikom AH verifikacije. Pošto ICV sadrži tajni ključ koji je poznat samo izvornom i odredišnom uređaju, NAT nije u stanju da izvrši pravilno preračunavanje ICV polja IPsec paketa.

Iz ovog razloga je AH protokol, bilo u transportnom ili tunel modu, potpuno nekompatibilan sa NAT-om, i može se koristiti samo ako tokom putanje paketa ne dolazi do translacije adresa.

Isti problem javlja se i u **PAT** (*Port Address Translation*) procesu, koji menja još i brojeve TCP, odnosno UDP portova.

Ovaj konkretan nedostatak ne postoji u ESP protokolu, pošto njegova autentifikacija ne uključuje IP zaglavlje koje se menja prilikom NAT procesa, ali ipak postoje poteškoće i u translaciji ovih paketa.

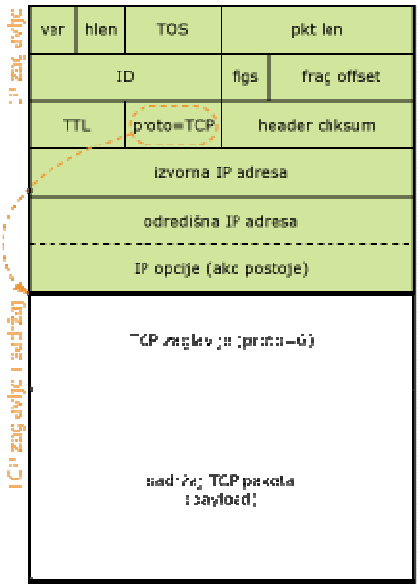
Prolazak IPsec paketa kroz NAT rešava se posebnom procedurom koja se zove NAT traversal. Postoje mnoge tehnike, ali ni jedna ne funkcioniše u svakoj situaciji, pošto ni sam NAT proces nije standardizovan. Mnoge tehnike zahtevaju asistenciju servera koji se nalazi na javno dostupnoj IP adresi. Neke koriste ovakav server samo prilikom uspostavljanja (npr. STUN), dok druge koriste ovaj server ka relej za prosleđivanje paketa.

Primena IPsec protokola u izgradnji IP paketa

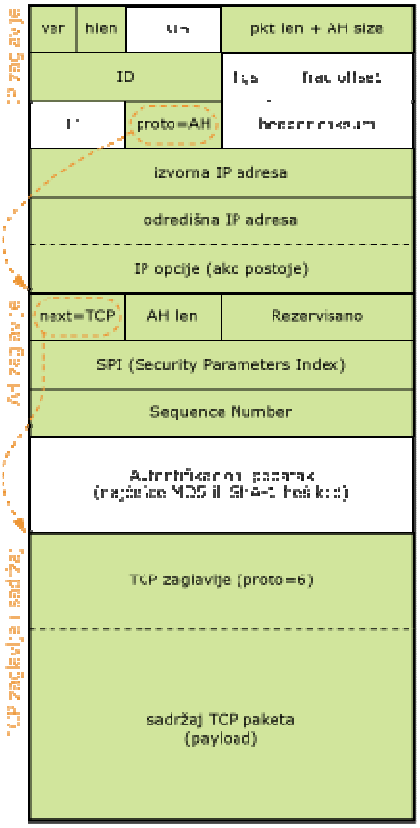
Mada je IPsec prvenstveno dizajniran za primenu u IPv6 protokolu, njegova implementacija definisana je i za primenu IP verziji 4. Zbog prilično sporog prihvatanja IPv6 na globalnom nivou, danas se IPsec najčešće primenjuje u IPv4 mrežama. Na nekoliko sledećih primera videćemo kako se primena IPsec bezbednosti odražava na izgradnju IPv4 paketa.

Na *slici 1.* prikazan je IP paket bez primenjene IPsec zaštite. Zatamnjena polja označavaju polja koja se koriste u izračunavanju *header checksum*-a.

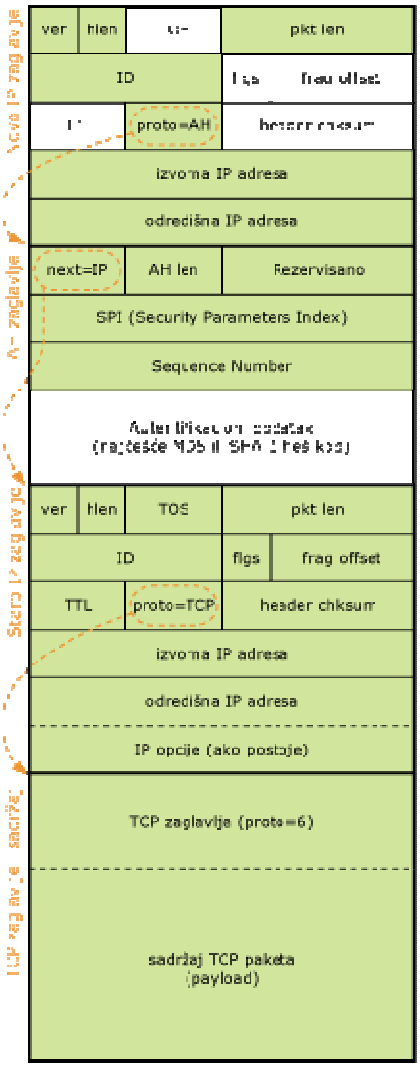
- ***ver:*** Verzija IP protokola, u ovom slučaju 4 = IPv4
- ***hlen:*** Dužina IP zaglavlja. Ne računa se dužina drugih zaglavlja i samog sadržaja paketa.
- ***TOS (Type of Service):*** polje je bitmaska koj opisuje tip usluge koju paket treba da dobije.
- ***pkt len:*** dužina celokupnog paketa u bajtima. Najveća vrednost je 65535, i ona uključuje i dužinu zaglavlja.
- ***ID:*** ovo polje se koristi da bi se povezali fragmentisani paketi
- ***flgs:*** polje bit-zastavica koj se uglavnom koriste za kontrolu fragmentacije
- ***frag offset:*** kada je paket fragmentiran, ovo polje sadrži lokaciju fragmenta u celokupnom paketu.
- ***TTL:*** Time to Live polje, koje se dekrementira prilikom svakog prolaska kroz neki ruter. Kada dostigne vrednost nula, paket se odbacuje.
- ***proto:*** predstavlja kod protokola koji je učauren unutar IP paketa. U ovom primeru sadrži vrednost 6, koja predtavlja TCP paket.
- ***header chksum:*** sadrži *checksum* vrednost celog IP zaglavlja i koristi se za detekciju grešaka u prenosu.
- ***izvorišna IP adresa:*** 32-bitna IP adresa koja identifikuje uređaj koji je prvobitno poslao paket. Ovo polje se kod neobezbeđenih datagrama lako može promeniti, što se koristi u raznim tipovima zloupotreba.
- ***odredišna IP adresa:*** 32-bitna IP adresa koja identifikuje uređaj kojem je paket namenjen.
- ***IP opcije:*** opcionalni deo IP zaglavlja, koji se retko koristi u svakodnevnom saobraćaju. Postojanje IP opcija rezultuje *hlen* vrednošću većom od 5, i one se uključuju u *header checksum* proračun.



Slika1.: Neobezbeđeni IP paket



Slika 2.: IPsec paket sa AH protokolom u transportnom modu



Slika 3.: IPsec paket sa AH protokolom u tunel modu

Na *slici 2.* prikazan je IP paket zaštićen AH protokolom u transportnom modu. Zelena polja označavaju polja koja su obezbeđena AH atentifikacionim podacima.

IP paket zaštićen AH protokolom u tunel modu prikazan je na *slici 3*. Ceo početni IP paket učauren je u IPsec zaglavlje, koje sadrži AH i novo IP zaglavlje. *Next hdr* polje u AH hederu ne pokazuje na sadržaj IP paketa, već na originalno IP zaglavlje.

- ***proto:*** kod primene AH protokola, ovo polje IP zaglavlja sadrži kod 51.

- ***next hdr:*** predstavlja kod protokola koji je učauren unutar IP paketa, i kod transportnog moda to je vrednost *proto* polja IP datagrama pre primene IPsec zaštite. Pri upotrebi tunel moda, sadrži proto kod 4 (IPv4), i time saopštava da sledi originalno IP zaglavlje. Na ovaj način se zaglavlja povezuju u niz.
- ***AH len:*** definiše dužinu AH zaglavlja u 32-bitnim rečima, umanjenu za 2 (po *RFC 1883* za IPv6)
- ***Rezervisano:*** ovo polje je rezervisano za buduće namene i mora biti postavljeno na nulu.
- ***Security Parameters Index:*** 32-bitni identifikator načina na koji IPsec obezbeđuje paket.
- ***Sequence Number:*** monotono rastući identifikator redosleda paketa, koji se koristi u zaštiti od replay napada.
- ***Autentifikacioni podatak:*** Podatak koji se izračunava za ceo IPsec paket pre njegovog slanja. Primalac ponavlja ovaj proračun, i ako se brojevi ne slažu, paket je kompromitovan ili oštećen u prenosu, pa se odbacuje.

Slika 4. prikazuje IP paket obezbeđen ESP protokolom u transportnom modu, a *slika 5.* isti protokol u tunel modu. Zelena polja označavaju polja koja su obezbeđena opcionim ESP atentifikacionim podacima. Deo paketa koji je uokviren plavom bojom sadrži polja koja su kriptovana.

IPsec standardi

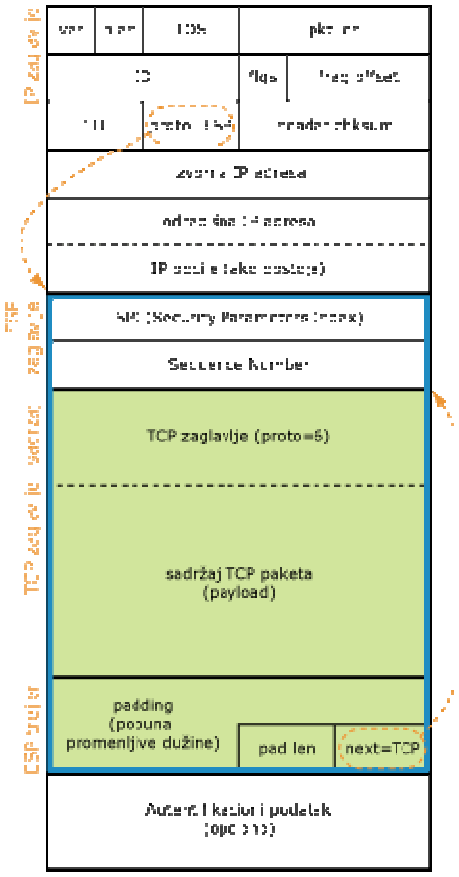
IPsec je prvenstveno razvijen za upotrebu u IPv6 standardu i podrška za njega je obavezna u svim implementacijama IPv6. Primena u IPv4 implementacijama je opciona.

Originalne definicije IPsec protokola nalaze se u *Request for Comments* dokumentima ***RFC 1825*** i ***RFC 1829*** iz 1995. godine.

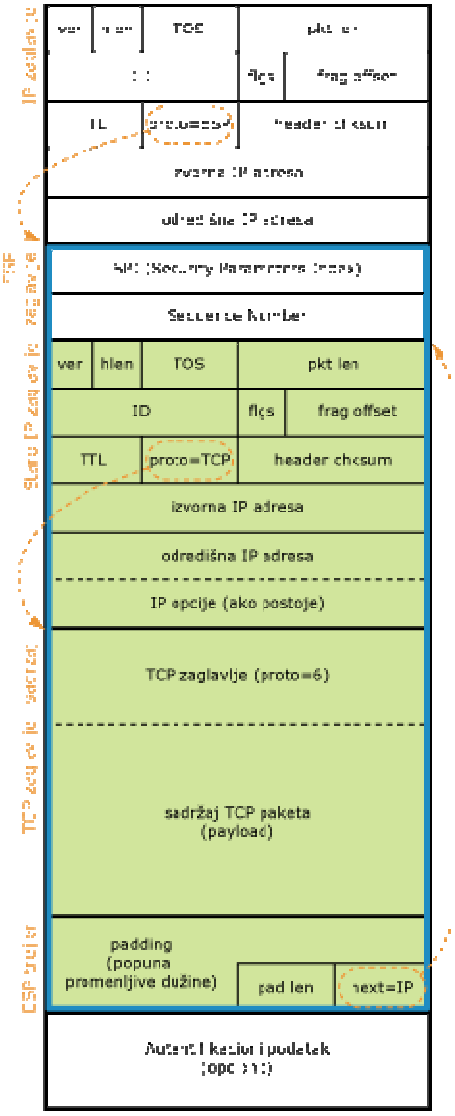
1998. godine ove definicije su zamenjene u ***RFC 2401*** i ***RFC 2412***, koji imaju isti koncept, ali nisu kompatibilni sa prehodnim dokumentima. Dodat je i zajednički protokol za razmenu ključeva, *Internet Key Exchange (IKE)*.

U decembru 2005. godine definisani su novi standardi u ***RFC 4301*** i ***RFC 4309***, koji predstavljaju nadgradnju prethodnih standarda, sa dodatkom druge verzije protokola za razmenu ključeva *IKEv2*. U ovoj trećoj generaciji standarda usvojena je i zvanična skraćenica, u obliku "*IPsec*".

Od sredine 2008. godine u okviru IETF funkcioniše *IPsec Maintenance and Extensions working group*.



Slika 4.: IPsec paket sa ESP protokolom u transportnom modu



Slika 5.: IPsec paket sa ESP protokolom u tunel modu

ZAKLJUČAK

IPsec je standard koji se menja i definiše „u hodu". Malo je verovatno da ćemo u skorijoj budućnosti imati njegovu konačnu verziju. Postoji puno razloga za to, a najbitniji su sporo prihvaćanje IPv6 protokola, i kreativna rešenja kojima se produžuje životni vek IPv4. Najveći deo problema koji postoje u primeni IPsec standarda ograničeni su na neadekvatnosti koncepta IPv4 u modernoj informacionoj sferi.

Postoji i dosta kritika na račun komlikovanosti IPsec-a. Mnogi stručnjaci zastupaju tezu da je previše komplikovan da bi ikada mogao da bude potpuno bezbedan. Video sam nekoliko interesantnih predloga za pojednostavljivanje IPsec protokola. Na primer, postoji predlog da se Authentication Header u potpunosti izbaci iz upotrebe, pošto ESP svakako sadrži dovoljno bezbedan set autentifikacionih metoda. Sa druge strane, video sam i VPN rešenje koje koristi isključivo AH protokol, što opet dovodi u pitanje neophodnost ESP-a (većina VPN saobraćaja se svakako šifrira na višim nivoima OSI modela). Ja predviđam da će oba protokola ostati i dalje u upotrebi, pa svako može da koristi onaj koji mu više odgovara.

Uz svu moju volju, nisam uspeo da napravim i prikaz praktične primene ovih tehnologija u radu običnih korisnika. To je, naravno, sasvim opravdano; IPsec funkcioniše na mrežnom nivou, pa korisnici najčešće i neznaju da li ga koriste. Svi poznatiji klijentski operativni sistemi već godinama imaju podršku za rad sa IPsec protokolima, a njena podešavanja spadaju u domen administratodskih poslova.

LITERATURA

[1] "An Overview of Cryptography", 2010,
< http://www.garykessler.net/library/crypto.html > (pristupano 05.06.2010.)

[2] DORASWAMY N., HARKINS D., *IPSec: the new security standard for the Internet, intranets, and virtual private networks, Second Edition*, Sun Microsystems, Prentice Hall PTR, 2003.

[3] "Future of Internet Security - IPSec", 2010,
< http://www.securitydocs.com/pdf/2926.PDF > (pristupano 05.06.2010.)

[4] "Information security", Wikipedia, the free encyclopedia, 2010,
< http://en.wikipedia.org/wiki/Information_security > (pristupano 19.03.2010.)

[5] "IPSec & IPv6 - Securing the NextGen Internet", 2010,
< http://ipv6.com/articles/security/IPsec.htm > (pristupano 13.06.2010.)

[6] "IPsec", Wikipedia, the free encyclopedia, 2010,
< http://en.wikipedia.org/wiki/IPsec > (pristupano 19.03.2010.)

[7] "IPsec's Role in Network Security: Past, Present, Future", 2010,
< http://www.sans.org/reading_room/whitepapers/vpns/ipsecs-role-network-security-past-present-future_742 > (pristupano 05.06.2010.)

[8] "IPv6 Authentication Header and Encapsulated Security Payload", 2010,
< http://www.tml.tkk.fi/Opinnot/Tik-110.551/1996/ahesp.html > (pristupano 13.06.2010.)

[9] KOZIEROK C., 2005. *The TCP/IP Guide*, verzija 3.0, (s.l.): (s.n.)

[10] "Steve Friedl's Unixwiz.net Tech Tips - An Illustrated Guide to IPsec",
< http://unixwiz.net/techtips/iguide-ipsec.html > (pristupano 19.3.2010.)

[11] "TCP/IP Security CHRIS CHAMBERS, JUSTIN DOLSKE, and JAYARAMAN IYER", 2010,
< http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html > (pristupano 19.03.2010.)

[12] "The official IPsec Howto for Linux", 2010,
< http://www.ipsec-howto.org/ > (pristupano 19.03.2010.)

[13] "The TCP/IP Guide - IPSec Overview, History and Standards", 2010,
< http://www.tcpipguide.com/free/t_IPSecOverviewHistoryandStandards.htm > (pristupano 05.06.2010.)