Protokol IPsec

Radivoj Fajt

Fakulteta za računalništvo in informatiko Univerze v Ljubljani

E-pošta: radivoj_fajt@t-2.net

Marec 2009

Abstract

IPsec is a family of standards that specify security enhancements for both IP protocol versions, version 4 and version 6 by introducing extension header to the IP packet. IPsec enables secure communication across local area networks as well as across the global internet. It provides data authentication, integrity and confidentiality of the each IP packet data. Implementing IPsec also requires being aware of the protocol weaknesses and security flows as well as the overall security concept. The goal of this article is to present specific security mechanism and weaknesses of IPsec and to introduce some real implementations.

Povzetek

Protokol IPsec je niz varnostnih standardov in nadgradnja protokola IP obeh različic, torej različice IPv4 in IPv6, za zagotavljanje varne komunikacije znotraj lokalnega omrežja kot tudi prek interneta. Osnova delovanja je overjanje, zagotavljanje celovitosti in šifriranje podatkov vsakega posameznega paketa IP. Pri izvedbi protokola pa se je treba zavedati tudi njegovih šibkosti in varnostnih lukenj, kot tudi koncepta varnosti sploh. Namen naloge je predstaviti osnovne komponente protokola, njegove šibkosti in nekatere izvedbe protokola v praksi.

VSEBINA

1 Uvod

Razmah uporabe interneta in razširjenost omrežij TCP/IP sta glavni spodbudi vpeljave standardov za zagotavljanje varnosti prometa v teh omrežjih. Pod okriljem organizacije IETF je tako že leta 1992 začel nastajati varnostni protokol IPsec (IP security), katerega osnovni namen je bil zagotoviti privzeto varnost prometa v internetnih omrežjih ali natančneje omrežjih IP. Kot že ime pove, temelji protokol na ideji varnostne zaščite vsakega posameznega paketa IP in s tem podatkov, ki jih tak paket nosi. Ideja sama je sicer že stara, vendar prihaja do praktičnih izvedb širše uporabe v zadnjih letih bolj kot kadarkoli prej, kjer je uporaba osredotočena predvsem na gradnjo navideznih zasebnih omrežij VPN (Virtual Private Network) za povezovanje prostorsko ločenih lokalnih omrežij in za povezovanje domačega ali prenosnega računalnika z lokalnim omrežjem podjetja. To pomeni, da lahko dve sodelujoči strani, med katerima je računalniško omrežje, npr. internet, medsebojno komunicirata po varni povezavi.

Protokol IPsec je dejansko skupek varnostnih standardov, ki določajo varnostno razširitev ali nadgradnjo internetnega protokola IP za zaščito omrežnih povezav in temelji na vpeljavi razširjene glave pri vsakemu paketu IP. Pri različici IPv6 je protokol IPsec že del samega standarda in je uporaba takorekoč privzeta, pri IPv4 pa je njegova uporaba možna. Ker deluje protokol IPsec v omrežnem sloju modela OSI, je popolnoma neodvisen od oblike in vrste podatkov aplikacij višjih slojev tega modela, njegovo delovanje pa popolnoma transparentno za uporabnike. To pomeni, da v aplikacije ni treba vgrajevati dodatnih varnostnih modulov za zagotavljanje varnosti podatkov in uporabniki ne potrebujejo dodatnega znanja o uporabi varnostnih mehanizmov.

Izvedba protokola IPsec v osnovi zagotavlja:

- overjanje izvora podatkov (data origin authentication),
- nepovezavno celovitost (connectionless integrity),
- zaupnost (confidentiality),
- nadzor dostopa (access control),
- delno zaupnost prometnega pretoka (limited confidentiality of traffic flow),
- zaščito zoper podvajanje paketov (replay prevention) in
- overjanje varnostnih prehodov.

V naslednjem poglavju so predstavljeni glavni gradniki protokola IPsec, ki so v nadaljevanju tudi podrobneje opisani: v 3. in 4. poglavju sta opisani varnostni storitvi AH in ESP, v 5. in 6. poglavju pa varnostna zveza SA in specifikacija IKE s protokoloma OAKLEY in ISAKMP. V 7. poglavju so navedeni primeri izvedb protokola v praksi, kje ima protokol šibkosti in katera priporočila je treba upoštevati pri izvedbah ter implementacijah protokola, v 8. poglavju pa je podan zaključek.

2 Gradniki protokola IPsec

Protokol IPsec omogoča uporabo več vrst varnostnih mehanizmov, šifrirnih algoritmov, funkcij overjanja, šifriranja itd. Namesto točno določenih pravil v resnici določa le okvir ali varnostno arhitekturo izvedbe protokola, znotraj katere je dovoljeno skoraj vse, o čemer se obe strani lahko medsebojno dogovorita. Kljub temu lahko varnostno arhitekturo razdelimo na osnovne gradnike, ki opredeljujejo večino, če že ne vseh izvedb protokola.

(a)Varnostni storitvi

- glava za overjanje AH (Authentication Header) in
- varovanje vsebine z inkapsulacijo ESP (Encapsulating Security Payload).

Navadno sta storitvi uporabljeni samostojno, možno pa ju je uporabiti tudi v medsebojni kombinaciji, vendar pa taka uporaba ni običajna. Zgornji varnostni storitvi sta glavna mehanizma zaščite protokola IPsec in služita za:

- overjanje izvora in zagotavljanje celovitosti podatkov (AH), pri čemer so najpogosteje uporabljene zgoščevalne funkcije MD5 in SHA1, algoritem AES-XCBC itd.;
- šifriranje podatkov z izbirnim overjanjem izvora in zagotavljanjem celovitosti podatkov (ESP), pri čemer so najpogosteje uporabljeni šifrirni algoritmi 3DES-CBC, AES-CBC s ključem dolžine 128 bitov, AES-CTR, DES-CBC, Blowfish itd.

Protokol IPsec sicer omogoča uporabo več vrst šifrirnih algoritmov, vendar sta znotraj določene povezave IPsec istočasno lahko uporabljena največ dva, redkeje trije. Ker pa so algoritmi podvrženi različnim napadom razbijanja šifer, njihova varnost ni zagotovljena za vedno. Zato protokol IPsec določa uporabo trenutno obveznih algoritmov, priporoča uporabo algoritmov, ki bodo z veliko verjetnostjo postali obvezni in še vedno dopušča algoritme, katerih uporaba je zaradi njihovih znanih šibkosti že vprašljiva. Vsaka izvedba protokola IPsec mora zagotavljati podporo obveznim algoritmom zaradi združljivosti različnih izvedb, lahko pa podpira tudi druge algoritme.

Obe varnostni storitvi (AH in ESP) lahko delujeta v dveh osnovnih načinih:

- transportni način (transport mode),
- tunelski način (tunnel mode).

V transportnem načinu je overjen in šifriran le podatkovni del paketa IP, ne pa tudi njegova glava, medtem ko je v tunelskem načinu overjena in šifrirana tudi glava paketa IP, paketu pa dodana nova glava. S tem je izvorni paket IP popolnoma skrit pred zunanjimi opazovalci.

(b)Varnostna zveza SA (Security Association)

Varnostna zveza SA je zbirka parametrov, ki določajo varnostne storitve za upravljanje z algoritmi in mehanizme za upravljanje s ključi pri zaščiti prenosa paketov IP med sodelujočima stranema. Varnostne zveze SA uporabljata obe varnostni storitvi (AH in

ESP), vsak paket IP po obdelavi z eno od storitev pa je enolično povezan z ustrezno varnostno zvezo.

(c)Internetni dogovor o ključu IKE (Internet Key Exchange)

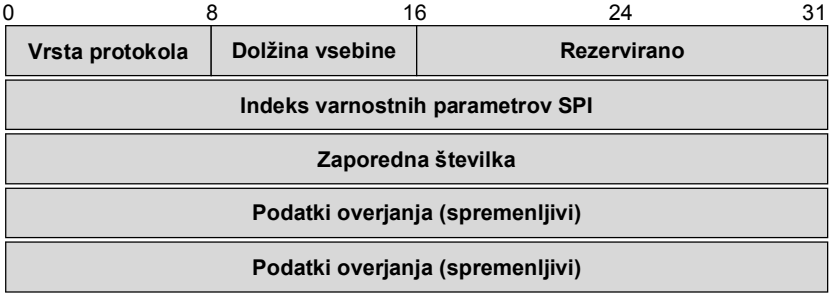
Za vzpostavitev varne povezave ali v procesu overjanja izvora in zagotavljanja celovitosti podatkov ter šifriranja podatkov, morata obe sodelujoči strani poznati skrivni ključ. Poleg tega si morata obe strani izmenjati ustrezne parametre in vzpostaviti varnostno zvezo SA. Te postopke in mehanizme, ki so lahko ročni ali samodejni, določa specifikacija IKE. V primeru slednjih določa specifikacija IKE dva privzeta protokola: dogovor o ključu OAKLEY ter internetno varnostno zvezo in protokol upravljanja s ključi ISAKMP (Internet Security Association and Key Management Protocol). Protokol OAKLEY, ki temelji na protokolu Diffie-Hellman, je namenjen dogovoru o ključu, medtem ko protokol ISAKMP določa postopke upravljanja s podatki potrebnimi za dogovor o ključu in za vzpostavljanje ter upravljanje varnostnih zvez SA.

3 Glava za overjanje AH

Varnostna storitev Glava za overjanje AH se v osnovi uporablja takrat, ko se želi zagotoviti, da se podatki paketa IP med potjo od pošiljatelja do prejemnika niso spremenili. Varnostna storitev torej zagotavlja:

- nepovezavno celovitost,
- overjanje izvora podatkov in izbirno
- zaščito zoper podvajanje paketov.

Varnostna storitev AH zagotavlja overjanje izvora in zagotavljanje celovitosti podatkov višjih slojev modela OSI (prenosni, aplikacijski sloj) ter polj izvorne glave paketa IP in glave AH, ki se jim vrednosti med prenosom ne spreminjajo ali jih je mogoče pri prejemniku enolično predvideti. Storitev zaščite zoper podvajanje paketov pa je izbirna storitev, o uporabi katere odloča prejemnik paketov IP in katere uporaba je omejena le na varnostne zveze SA vodene s protokolom ISAKMP. Overjanje podatkov se doseže z izračunom vrednosti preverjanja celovitosti ICV (Integrity Check Value). Vrednost ICV je v resnici zgoščena vrednost kode overjanja sporočila MAC (Message Authentication Code) z uporabo enosmernih zgoščevalnih



Slika 1. Glava varnostne storitve AH

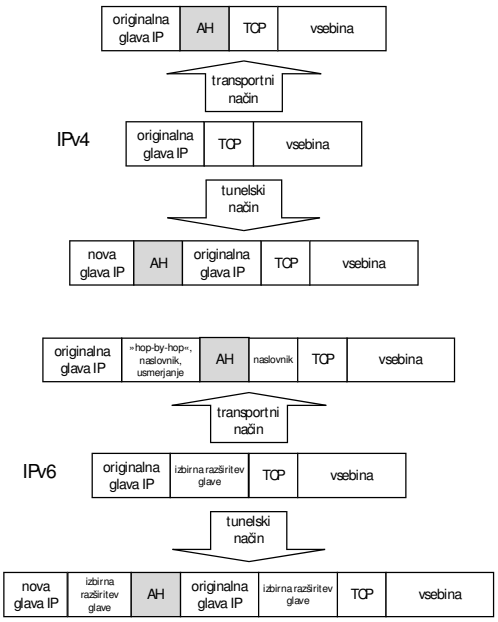
funkcij ali simetričnih šifrirnih algoritmov v kombinaciji s skrivnim ključem. Vrednost ICV je zapisana v glavi AH v polju Podatki overjanja. Na sliki 1 je prikazana zgradba glave AH, na sliki 2 pa njena umestitev znotraj paketa IP.

Posamezna polja glave AH so:

- Vrsta protokola (Next Header): vrednost polja določa uporabljeni protokol, po katerem so obravnavani paketi IP. Vrednost je izbrana iz množice števil protokola IP, ki je definirana na spletni strani urada IANA (http://www.iana.org). Tako npr. vrednost 4 določa protokol IPv4, vrednost 41 protokol IPv6, vrednost 6 protokol TCP itd.
- Dolžina vsebine (Payload length): vrednost polja določa dolžino glave AH. Vrednost je izražena v enotah po 32 bitov, dejanski dolžini pa je odšteta vrednost 2. V primeru, ko je dolžina vrednosti ICV 96 bitov, je vrednost polja enaka 4 (trikrat po 32 bitov polj nespremenljive dolžine + trikrat po 32 bitov vrednosti ICV - 2 = 3 + 3 - 2 = 4).
- Rezervirano (Reserved): polje je rezervirano za prihodnjo uporabo. Vrednost polja mora biti postavljena na 0, ker je polje vključeno v izračun vrednosti ICV.
- Indeks varnostnih parametrov SPI (Security Parameters Index): vrednost polja skupaj z naslovom IP prejemnika in vrsto varnostne storitve (AH) enolično določa vsako varnostno zvezo SA, s katero je povezan določeni paket IP.
- Zaporedna številka (Sequence Number): vrednost polja je v osnovi namenjena zagotavljanju zaščite zoper podvajanje paketov, vendar pa se številčenje paketov izvaja tudi takrat, ko omenjena funkcionalnost ni aktivirana. Vrednost je v trenutku vzpostavitve varnostne zveze SA med sodelujočima stranema postavljena na 0 in se ob vsakem poslanem paketu ter pri dani varnostni zvezi poveča za 1. Ko je presežena največja možna vrednost 2^{32}-1, se vzpostavi nova varnostna zveza SA in posledično nov ključ, vrednost števca pa se postavi nazaj na 0, saj se vrednost pri dani varnostni zvezi ne sme ponoviti. Vendar se ta postopek izvede le v primeru aktivirane zaščite zoper podvajanje paketov, sicer se zgodi le to, da se vrednost števca postavi na 0.
- Podatki overjanja (Authentication Data): polje je spremenljive dolžine, odvisne od uporabljenih algoritmov za overjanje podatkov in ustreza večkratniku števila 32 bitov. Polje vsebuje vrednost ICV za overjanje izvora in zagotavljanje celovitosti podatkov posameznega paketa IP. Poleg tega pa lahko polje vsebuje tudi zapolnjevalne bite, ko se zahteva, da je dolžina glave AH večkratnik števila 32 bitov v primeru protokola IPv4 ali števila 64 bitov v primeru protokola IPv6.

Na sliki 2 je prikazana umestitev glave AH znotraj paketa IP za obe različici protokola IP (IPv4 in IPv6). Seveda je položaj glave odvisen tudi od uporabljenega načina delovanja storitve, transportnega ali tunelskega načina.

V primeru protokola IPv6 je paket IP opremljen še z dodatnim poljem Izbirna razširitev glave (Optional extension header), ki je po obdelavi lahko pred ali za glavo AH ali oboje, pač odvisno od želene semantike.



Slika 2. Oblika paketa IP po obdelavi z varnostno storitvijo AH

(a)Transportni način

V transportnem načinu delovanja je glava AH vrinjena med izvorno glavo paketa IP in poljem, ki določa uporabljeni protokol paketa IP (TCP, ICMP itd.). V tem načinu je za obdelani paket IP uporabljena ista izvorna glava IP, kot jo ima izvorni paket IP in seveda le ta ni vključena v izračun vrednosti ICV.

(b)Tunelski način

V tunelskem načinu delovanja je na začetku izvornega paketa IP dodana nova glava ali tudi zunanja glava IP in za njo glava AH. Zunanja glava IP vsebuje naslov namenjen naslavljanju elementov varnostnega protokola IPsec, npr. varnostnih prehodov, medtem ko ostaja v notranji ali izvorni glavi IP naslov končnega prejemnika. Pomembno dejstvo je, da je v tem načinu delovanja celotni izvorni paket IP vključen v novi paket z novo glavo IP. Tako je vrednost ICV izračunana nad celotnim izvornim paketom IP, vključno z njegovo izvorno glavo IP.

V izračun vrednosti ICV so vključena vsa polja paketa IP, ki so na sliki 2 za poljem glave AH. Dodatno so v izračunu upoštevana še polja glave AH Naslednja glava, Dolžina vsebine, Rezervirano, Indeks varnostnih parametrov SPI, Zaporedna številka, Podatki overjanja, katerega vrednost ICV je pred izračunom enaka 0 in zapolnjevalni biti (padding), če so prisotni ter polja glave paketa IP, ki se med prenosom ne spreminjajo ali jih je mogoče po prenosu enolično predvideti. Ostala polja glave paketa IP so v izračunu upoštevana tako, da je njihova vrednost postavljena na 0. S tem se ohranja dolžina polj paketa IP, ki lahko služi kot dodatna vrednost za preverjanje njegove ustreznosti pri prejemniku. Za izračun vrednosti ICV

določa protokol IPsec uporabo naslednjih enosmernih zgoščevalnih funkcij ali simetričnih šifrirnih algoritmov, ki so skupaj s skrivnim ključem določene v ustrezni varnostni zvezi SA:

- HMAC-SHA1-96 (trenutno minimalna zahteva protokola),
- AES-XCBC-MAC-96 (trenutno priporočilo protokola),
- HMAC-MD5-96 (uporaba je s protokolom še dovoljena, vendar ni priporočljiva).

HMAC pomeni, da je vrednost ICV v resnici zgoščena vrednost MAC (hash MAC), SHA1 ali MD5 sta pri tem uporabljeni enosmerni zgoščevalni funkciji v kombinaciji s skrivnim ključem, število 96 pa določa dolžino bloka podatkov v bitih, nad katerimi se funkcija zgoščevanja izvede. V primeru uporabe simetričnega šifrirnega algoritma AES pa se funkcija zgoščevanja vrednosti MAC izvede z načinom AES-XCBC v kombinaciji s skrivnim ključem. Poleg zgoraj omenjenih algoritmov je seveda mogoče uporabiti tudi druge. V vsakem primeru pa je izhodna vrednost teh algoritmov omejena na dolžino večkratnika dolžine 32 bitov, tako za protokol IPv4 kot tudi za protokol IPv6. Kateri algoritem bo uporabljen, pa je določeno z varnostno zvezo SA.

4 Varovanje vsebine z inkapsulacijo (ESP)

Osnova delovanja varnostne storitve Varovanje vsebine z inkapsulacijo (ESP) je šifriranje podatkov paketa IP na poti od pošiljatelja do prejemnika. Poleg tega je možno izbirno uporabiti iste varnostne mehanizme overjanja izvora in zagotavljanja celovitosti podatkov kot pri varnostni storitvi AH (glej poglavje 3). Varnostna storitev ESP torej zagotavlja:

- zaupnost podatkov,
- delno zaupnost prometnega pretoka

in izbirno

- nepovezavno celovitosti,
- overjanje izvora podatkov,
- zaščito zoper podvajanje paketov.

Izbirna možnost overjanja izvora in zagotavljanja celovitosti podatkov se izvede enako kot pri varnostni storitvi AH in z istimi varnostnimi algoritmi, le da je v tem primeru vrednost ICV zapisana v glavi ESP v polju Podatki overjanja. Šifriranje podatkov pa se doseže z uporabo simetričnih šifrirnih algoritmov v kombinaciji s skrivnim ključem. Na sliki 3 je prikazana zgradba glave ESP, na sliki 4 pa njena umestitev znotraj paketa IP. Pri tem je med glavama AH in ESP bistvena razlika. Medtem ko je glava AH iz enega kosa in umeščena pred podatki paketa IP (glej sliko 2), se glava ESP zaključuje s poljema imenovanima Rep ESP (ESP trailer) in Overjanje ESP (ESP authentication) ter tako v bistvu obkroža podatke paketa IP (glej sliko 4). Pred podatki paketa IP sta polji Indeks varnostnih parametrov SPI in Zaporedna številka (ESP), za podatki pa polja Zapolnjevalni biti, Dolžina zapolnjevalnih bitov in Naslednja glava (rep ESP) ter na koncu polje Podatki overjanja (overjanje ESP). Vrednost polja Zapolnjevalni biti se uporablja zaradi simetričnih (bločnih) šifrirnih algoritmov, ki

Slika 3. Glava varnostne storitve ESP

delujejo le nad bloki podatkov fiksne dolžine, medtem ko se polje Podatki overjanja uporablja le v primeru izbirne možnosti overjanja podatkov.

Posamezna polja glave ESP so:

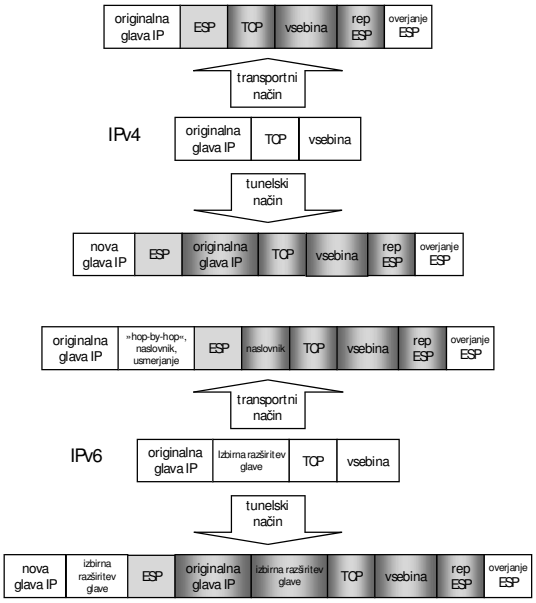
- Indeks varnostnih parametrov SPI (Security Parameters Index): vrednost polja skupaj z naslovom IP prejemnika in vrsto varnostne storitve (ESP) enolično določa varnostno zvezo SA, s katero je povezan določeni paket IP.
- Zaporedna številka (Sequence Number): vrednost polja je v osnovi namenjena zagotavljanju zaščite zoper podvajanje paketov, vendar pa se številčenje paketov izvaja tudi takrat, ko omenjena funkcionalnost ni aktivirana. Vrednost je v trenutku vzpostavitve varnostne zveze SA med sodelujočima stranema postavljena na 0 in se ob vsakem poslanem paketu ter pri dani varnostni zvezi poveča za 1. Ko je presežena največja možna vrednost 2^{32}-1, se vzpostavi nova varnostna zveza SA in posledično nov ključ, vrednost števca pa se postavi nazaj na 0, saj se vrednost pri dani varnostni zvezi ne sme ponoviti. Vendar se ta postopek izvede le v primeru aktivirane zaščite zoper podvajanje paketov, sicer se zgodi le to, da se vrednost števca postavi na 0.
- Vsebina (Payload Data): polje je spremenljive dolžine in hkrati večkratnik dolžine 8 bitov, vsebuje pa informacije o podatkih višjih slojev, katerih vrsta je določena v polju Naslednja glava. Če je za izbrani šifrirni algoritem potreben npr. inicializacijski vektor IV (Initialisation Vector), se v tem polju prenaša tudi vrednost tega vektorja, vendar pa je vrednost v resnici »skrita« v vsebini celotnega polja.
- Zapolnjevalni biti (Padding): polje vsebuje zapolnjevalne bite za zagotavljanje ustrezne dolžine polja ali za zakrivanje resnične dolžine uporabnih podatkov. Zapolnjevalni biti so potrebni zaradi simetričnih (bločnih) šifrirnih algoritmov, ki delujejo nad bloki podatkov fiksne dolžine.
- Dolžina zapolnjevalnih bitov (Padding Length): vrednost polja določa število zlogov (byte) zapolnjevalnih bitov prejšnjega polja.
- Vrsta protokola (Next Header): vrednost polja določa uporabljeni protokol, po katerem so obravnavani paketi IP. Vrednost tega polja je izbrana iz množice števil protokola IP,

ki je definirana na spletni strani urada IANA (http://www.iana.org). Tako npr. vrednost 4 določa protokol IPv4, vrednost 41 protokol IPv6, vrednost 6 protokol TCP itd.

- Podatki overjanja (Authentication Data): polje je spremenljive dolžine, odvisne od uporabljenih algoritmov za overjanje podatkov in ustreza večkratniku števila 32 bitov. Polje vsebuje vrednost ICV za overjanje izvora in zagotavljanje celovitosti podatkov posameznega paketa IP, ki je v primeru varnostne storitve ESP izbirna možnost.

Na sliki 4 je prikazana umestitev glave ESP znotraj paketa IP za obe različici protokola IPv4 in IPv6. Seveda je položaj glave odvisen tudi od uporabljenega načina delovanja storitve, transportnega ali tunelskega načina.

V primeru protokola IPv6 je paket IP opremljen še z dodatnim poljem Izbirna razširitev glave (Optional extension header), ki je po obdelavi paketa IP lahko pred ali za poljem ESP ali



Slika 4. Oblika paketa IP po obdelavi z varnostno storitvijo ESP

oboje, pač odvisno od želene semantike. Ker pa so dejansko šifrirana le polja za poljem ESP (slika 4), je smiselno to polje postaviti za poljem ESP.

(a)Transportni način

V transportnem načinu delovanja je polje ESP vrinjeno med izvorno glavo paketa IP in podatki protokolov višjih slojev, npr. poljem, ki določa uporabljeni protokol paketa IP (TCP, ICMP itd.), polji Rep ESP in Overjanje ESP pa sta dodani na konec paketa IP. V tem načinu je za obdelani paket IP uporabljena ista izvorna glava IP kot jo ima izvorni paket IP. Izvorna glava seveda ni šifrirana in ni vključena v izračun vrednosti ICV.

(b)Tunelski način

V tunelskem načinu delovanja pa je polje ESP dodano na začetek paketa IP, pred njim pa je dodana nova glava ali tudi zunanja glava IP. Zunanja glava IP vsebuje naslov namenjen naslavljanju elementov varnostnega protokola IPsec, npr. varnostnih prehodov, medtem ko ostaja v notranji ali izvorni glavi IP naslov končnega prejemnika. Pomembno dejstvo je, da je v tem načinu delovanja znotraj obdelanega paketa IP celotni izvorni paket IP, kateremu je dodana nova glava IP. Tako je šifriranje izvedeno in vrednost ICV izračunana nad celotnim izvornim paketom IP, vključno z njegovo izvorno glavo IP.

V procesu obdelave paketa IP z varnostno storitvijo ESP se šifrirajo vsa polja paketa IP, ki so na sliki 4 za poljem ESP, razen polja Overjanje ESP, ki mora ostati nešifrirano, saj vsebuje vrednost ICV. Prav tako se ne šifrirata polji glave ESP Indeks varnostnih parametrov SPI, ki določa povezavo z ustrezno varnostno zvezo SA in Zaporedna številka, ki služi zaščiti zoper podvajanje paketov, šifrirajo pa se polja Vsebina, Zapolnjevalni biti, Dolžina zapolnjevalnih bitov in Naslednja glava. Tako se v transportnem načinu delovanja varnostne storitve ESP ne šifrira izvorna glava IP, medtem ko se v tunelskem načinu delovanja šifrira celoten paket IP. Za šifriranje podatkov določa protokol IPsec uporabo naslednjih simetričnih šifrirnih algoritmih, ki so skupaj s skrivnim ključem določeni v ustrezni varnostni zvezi SA:

- 3DES-CBC (trenutno minimalna zahteva protokola),
- AES-CBC (trenutno priporočilo protokola),
- AES-CTR (trenutno priporočilo protokola),
- DES-CBC (uporaba je s protokolom še dovoljena, vendar ni priporočljiva).

V izračun vrednosti ICV so vključena vsa polja paketa IPsec, ki so na sliki 4 za poljem ESP in vsa polja glave ESP. V izračun je torej vključena celotna šifrirana vsebina paketa IP in celotna glava ESP s polji Indeks varnostnih parametrov SPI, Zaporedna številka, Vsebina, Zapolnjevalni biti, Dolžina zapolnjevalnih bitov, Naslednja glava in Podatki overjanja, katerega vrednost ICV je pred izračunom enaka 0. In seveda so polja Vsebina, Zapolnjevalni biti, Dolžina zapolnjevalnih bitov in Naslednja glava tudi šifrirana.

Ko sta izbrani obe možnosti, overjanje (overjanje izvora in zagotavljanje celovitosti podatkov) ter šifriranje podatkov, se na pošiljateljevi strani najprej izvede šifriranje, medtem ko se na prejemnikovi strani postopek obrne; najprej se izvede overjanje, šele nato se dešifrira vsebina. Na ta način so postopki na prejemnikovi strani hitrejši, saj prejemnik preprosto zavrže vse neoverjene pakete IPsec, še preden se prične časovno potratnejši proces dešifriranja. In čeprav protokol IPsec dopušča, da je v primeru varnostne storitve ESP uporaba šifriranja in overjanja v celoti izbirna, pa mora biti uporabljena vsaj ena izmed obeh možnosti. Uporaba varnostne storitve ESP je v nasprotnem primeru nesmiselna, razen mogoče v namen testiranja.

5 Varnostna zveza (SA)

Pomemben koncept protokola IPsec je ravno varnostna zveza SA. Varnostna zveza SA je zbirka parametrov, kot so skrivni ključ, šifrirni algoritem, politike delovanja itd., v osnovi pa opredeljuje »enosmerno povezavo« med sodelujočima stranema, med pošiljateljem in prejemnikom, ki zagotavlja storitve varnosti prometa med njima. »Povezava« pomeni predvsem terminološki pojem in ne fizične povezave, medtem ko »enosmerna« pomeni, da sta v primeru dvosmernega prometa IPsec z enakimi lastnostmi med obema stranema potrebni dve varnostni zvezi SA (vsaka za svojo smer). Poleg tega je v eno varnostno zvezo SA lahko vključena le ena varnostna storitev (AH ali ESP), medtem ko jo obe storitvi uporabljata.

Model izvedbe varnostne zveze SA temelji na treh podatkovnih zbirkah:

- Podatkovna zbirka varnostnih politik SPD (Security Policy Database)
- Podatkovna zbirka varnostnih zvez SAD (Security Association Database)
- Podatkovna zbirka overjanja sodelujočih strani PAD (Peer Authentication Database)

Za boljše razumevanje varnostne zveze SA so v nadaljevanju opisane posamezne podatkovne zbirke s parametri, ki posamezno zvezo sestavljajo in jo opredeljujejo.

(a)Podatkovna zbirka varnostnih politik SPD

Podatkovna zbirka varnostnih politik SPD vsebuje zapise, ki določajo način zaščite paketov IP med obema sodelujočima stranema. S tem zagotavlja podrobno varnostno politiko komunikacije med njima in je zato predpogoj za vzpostavljanje varnostnih zvez SA. Posamezni zapis v zbirki določa tri vrste obdelave paketov IP, ki se izvedejo tako na strani pošiljatelja kot na strani prejemnika: paketi bodo preprosto zavrženi (discard), paketi bodo spuščeni naprej brez varnostne obdelave (bypass) in paketi bodo varnostno obdelani s protokolom IPsec (protect). V prvem primeru so to paketi, ki nimajo dovoljenja za prehod od pošiljatelja k prejemniku, v drugem primeru so to paketi, ki imajo dovoljenje za prehod brez varnostne zaščite IPsec, v tretjem primeru pa paketi IP, ki bodo obdelani z varnostno storitvijo IPsec. V slednjem primeru mora zapis podatkovne zbirke SPD določati uporabljeno varnostno storitev (AH ali ESP) in način njene uporabe (transportni ali tunelski), uporabljene varnostne mehanizme in šifrirne algoritme ter njihove medsebojne povezave. Zbirka SPD je zato razdeljena v tri logične enote: SPD-S z zapisi o paketih, ki morajo biti obdelani z varnostno storitvijo IPsec, SPD-O z zapisi o odhodnih paketih, ki naj bodo brez varnostne obdelave ali zavrženi in SPD-I z zapisi o dohodnih paketih, ki naj bodo brez varnostne obdelave ali zavrženi. Posamezni zapis v podatkovni zbirki SPD je kombinacija izbirnikov (selectors), ki v resnici sestavljajo filtre prometa paketov IP. Glavni izbirniki so:

- Naslov IP prejemnika (IPv4, IPv6): vrednost izbirnika je v splošnem naslov IP, več naslovov IP ali vrsta naslovov IP določenih s prepustnico (wildcard). Za podporo več uporabnikov, npr. v primeru varnostnih prehodov, je poleg naslova podana še maska.

Naslov IP se nanaša na končnega prejemnika podatkov, torej na naslov, ki je v primeru tunelskega načina prenosa zapisan v notranji glavi IP.

- Naslov IP pošiljatelja (IPv4, IPv6): tudi v tem primeru je vrednost izbirnika v splošnem naslov IP, več naslovov IP ali vrsta naslovov IP določenih s prepustnico (wildcard). Za podporo več uporabnikov se uporabljajo enaki postopki kot v prejšnjem primeru.
- Protokol naslednjega sloja (Next Layer Protocol): vrednost izbirnika je pridobljena iz glave paketa IPv4 ali IPv6, od te vrednosti pa so odvisni nekateri dodatni izbirniki: vrata pošiljatelja in prejemnika, vrsta mobilne glave protokola IPv6 ter vrsta sporočila ICMP.
- Ime: vrednost izbirnika ni pridobljena iz paketa IP, kot v prejšnjih primerih, ampak je to le simbolni identifikator pošiljateljevega ali prejemnikovega naslova IP, ki je lahko popolno internetno uporabniško ime ali e-poštno ime (nekdo@fe.uni-lj.si), popolno internetno domensko ime FQDN (fe.uni-lj.si), razločevalno ime po standardu X.500 (cn=NEKDO, o=Fakulteta za računalništvo, c=SI) ali zlog (byte) besedila.

Poleg varnostnih politik določa podatkovna zbirka SPD tudi način upravljanja prometa, saj se vsakemu posameznemu paketu IP dodeli v zbirki posamezna varnostna zveza SA, po kateri bo le ta obdelan. Zapisi v zbirki SPD so urejeni po prednostnem seznamu, zato se v primeru možnosti uporabe več varnostnih zvez SA za posamezni paket IP le ta obdela po prvi ustrezni varnostni zvezi. Postopek zagotavlja determinističnost procesa in preprečuje zmedo. Dodatna funkcionalnost zbirke SPD je sodelovanje pri izmenjavi sporočil IKE med sodelujočima stranema, pri kateri se komunikacija odvija z običajnimi paketi IP naslovljenimi na vrata 500 protokola UDP.

Podatkovna zbirka SPD je urejen seznam zapisov, skladen s seznami nadzora dostopa ACL (Access Control List) ali filtri paketov IP požarnih zidov, usmerjevalnikov itd.

(b)Podatkovna zbirka varnostnih zvez SAD

Podatkovna zbirka varnostnih zvez SAD vsebuje zapise parametrov, ki določajo posamezno varnostno zvezo SA ali ob vsaki vzpostavitvi varnostne zveze SA se v podatkovni zbirki SAD ustvari nov zapis. Na te zapise so v primeru odhodnega prometa (pri pošiljatelju) usmerjeni kazalci iz posameznega zapisa v zbirki SPD ali natančneje v delu SPD-S. Poudariti velja, da lahko ostanejo zapisi v zbirki SAD tudi še potem, ko so se zapisi v zbirki SPD že spremenili ali izbrisali. V tem primeru nanje ne kažejo nobeni kazalci zapisov zbirke SPD, določila protokola IPsec pa tudi ne določajo selektivnega brisanja takih zapisov iz zbirke SAD. Poleg tega so zapisi v zbirko SAD lahko dodani ročno in tudi v tem primeru ni nanje ustreznih kazalcev iz zbirke SPD. V primeru dohodnega prometa (pri prejemniku) pa je vsak zapis v zbirki SAD definiran s tremi parametri, ki enolično določajo vsako varnostno zvezo SA:

- Indeks varnostnih parametrov SPI (Security Parameters Index): parameter določa enolično povezavo ustrezne varnostne zveze SA s posameznim paketom IP prek polja v glavi AH ali ESP.

- Naslov IP prejemnika: parameter z običajnim naslovom IP prejemnika. Trenutno je možen le enojni naslov IP.
- Identifikator varnostnega protokola (Security Protocol Identifier): parameter določa uporabljeno varnostno storitev (AH ali ESP).

Poleg zgoraj naštetih osnovnih parametrov, pa vsebuje posamezni zapis podatkovne zbirke SAD še dodatne, ki dopolnjujejo posamezno varnostno zvezo SA:

- Števec zaporedne številke (Sequence Number Counter): števec, katerega vrednost se zapiše v polje Zaporedna številka (Sequence Number) glav AH ali ESP.
- Prekoračitev števca zaporedne številke (Sequence Counter Overflow): parameter označuje trenutek, ko je števec zaporedne številke dosegel največjo možno dovoljeno vrednost 2^{32}-1.
- Okno proti ponovitvam (Anti-Replay Window): parameter določa ali je prispeli paket IP ponovljen.
- Algoritem overjanja, pripadajoči ključi in njihova življenjska doba ter drugi podatki, potrebni za izvedbo varnostne storitve AH: parameter je prisoten le, če je omogočena varnostna storitev AH.
- Algoritem šifriranja, pripadajoči ključi in njihova življenjska doba, inicializacijski vektor IV ter drugi podatki, potrebni za izvedbo varnostne storitve ESP: parameter je prisoten le, če niso omogočeni algoritmi sestavljenega načina.
- Algoritem overjanja, pripadajoči ključi in njihova življenjska doba ter drugi podatki, potrebni za izvedbo varnostne storitve ESP: parameter je prisoten le, če je omogočena varnostna storitev ESP z overjanjem izvora in zagotavljanjem celovitosti podatkov ter niso omogočeni algoritmi sestavljenega načina.
- Algoritmi sestavljenega načina, pripadajoči ključi in drugi podatki, potrebni za izvedbo varnostne storitve ESP: parameter je prisoten le, če je omogočen algoritem kombiniranega načina s podporo šifriranju kot tudi overjanju izvora in zagotavljanju celovitosti podatkov.
- Življenjska doba SA (SA Lifetime): parameter določa časovni interval, po katerem je treba varnostno zvezo SA ukiniti ali jo nadomestiti z novo (z novim indeksom SPI) in katera izmed obeh operacij se bo izvedla. Interval je lahko izražen časovno, s količino prenesenih zlogov (bytes) ali kombinacijo obojega. V primeru časovno izražene življenjske dobe in vzpostavljanja varnostne zveze SA z uporabo digitalnih potrdil (standard X.509), mora biti varnostna zveza omejena tudi s časovno veljavnostjo digitalnih potrdil in datumom naslednje izdaje seznama preklicanih potrdil CRL (Certificate Revocation List).
- Način delovanja protokola IPsec: parameter določa način delovanja uporabljene varnostne storitve, ki je lahko transportni, tunelski ali način »wildcard«. Slednji omogoča uporabo tako transportnega kot tunelskega načina v okviru iste varnostne zveze SA.
- Pot enote maksimalnega prenosa (Path MTU - Maximum transmission unit): parameter določa maksimalno velikost paketa, ki je lahko poslan brez fragmentacije.

- Parametri, ki natančneje določajo postopke obdelave in prenosa paketov IP: Zastavica preverjanja fragmentacije (Stateful fragment checking flag), Prepusti bit Brez fragmentacije (Bypass Don't Fragment bit (T/F)), Vrednosti DSCP (Diferentiated Services Code Points), Prepusti vrednosti DSCP (T/F) ali poveži z nezaščitenimi vrednostmi DSCP (Bypass DSCP (T/F) or map to unprotected DSCP values) ter glava v tunelskem načinu z naslovom IP pošiljatelja in prejemnika (Tunnel header IP source and destination address).

Podatkovna zbirka SAD služi pošiljatelju za preverjanje primernosti varnostne zveze SA pri obdelavi in prenosu določenega paketa IP ter prejemniku, da preverja skladnost prejetega paketa in pogojev (filtrov) varnostne zveze SA, po kateri je bil paket obdelan.

(c)Podatkovna zbirka overjanja sodelujočih strani PAD

Podatkovna zbirka overjanja sodelujočih strani PAD vsebuje zapise povezav med podatkovno zbirko SPD ter protokolom dogovora o ključu in varnostnih zvezah SA, npr. protokolom IKE. Prek zbirke se določa protokol za upravljanje varnostnih zvez SA, zagotavljajo se metode in podatki za preverjanje identitete ter overjanje sodelujočih strani, omejuje se vrsta in vrednost identifikatorjev ID, ki jih posamezna stran lahko zahteva, lahko pa vključuje tudi informacije varnostnega prehoda, ko je posamezna stran za njim. Za zagotavljanje teh funkcionalnosti so v zbirki PAD zapisi o posamezni sodelujoči strani (uporabnik, končna naprava ali varnostni prehod) ali skupini le teh, določeni z uporabo pravil ujemanja identifikatorja ID. Podatkovna zbirka PAD namreč podpira šest vrst identifikatorjev ID, ki predstavljajo njen indeks in so skladni s simbolnimi imeni ter naslovi IP, določenimi v zbirki SPD: ime DNS, ki je lahko točno določeno ali delno, razločevalno ime (Distinguished Name), ki je lahko polno ali omejeno z poddrevesom, e-poštni naslov po specifikaciji RFC 822, ki je lahko poln ali le delni, naslova IPv4 in IPv6, ki sta lahko tudi območji naslovov in ključ identifikatorja ID, ki mora ustrezati natančnemu ujemanju. Poleg tega vsak zapis vključuje dogovor o ključu in varnostnih zvezah SA, npr. IKEv1, IKEv2, KINK (Kerberized Internet Negotiation Of Keys), način overjanja, npr. s predhodno določeno skrivnostjo v skupni rabi (pre-shared secret) ali z digitalnimi potrdili in podatke overjanja, npr. skrivnost v skupni rabi ali informacije o zaupanja vredni entiteti CA (Certification Authority) za overjanje digitalnih potrdil. V primeru izvedbe z digitalnimi potrdili lahko vsebuje tudi informacije o preklicanih digitalnih potrdilih, npr. kazalec na seznam preklicanih potrdil CRL, ime strežnika sprotnega stanja digitalnih potrdil OCSP (Online Certificate Status Protocol) ipd.

6 Internetni dogovor o ključu (IKE)

Preden se komunikacija IPsec med sodelujočima stranema lahko začne, se mora med njima vzpostaviti stanje vzajemnega zaupanja in poskrbeti za izmenjavo šifrirnih podatkov: obe strani se morata medsebojno identificirati, overiti, se dogovoriti o ključu in izmenjati druge podatke protokola IPsec, vzpostaviti varnostno zvezo SA, med komunikacijo poskrbeti za

vzdrževanje te zveze in jo na koncu ukiniti. Ti postopki se lahko izvedejo ročno tako, da so skrivni ključ in drugi parametri ročno vpisani v ustrezne podatkovne zbirke varnostnih zvez SA vsake sodelujoče strani posebej ali samodejno, dinamično, z uporabo sofisticiranih mehanizmov. Vsaka izvedba protokola IPsec pa mora podpirati obe možnosti. In čeprav ta izbira neposredno ne vpliva na uporabo varnostnih storitev AH ali ESP, pa vpliva na izbirno možnost zaščite zoper podvajanje paketov (replay prevention), ki se lahko uporabi le v primeru samodejne izvedbe omenjenih postopkov. Poleg tega je od načina izvedbe teh postopkov in posledično uporabljenih skrivnosti v skupni rabi ali ključev odvisna tudi učinkovitost overjanja posameznih strani, kot tudi algoritmov za overjanje izvora in zagotavljanje celovitosti podatkov ter šifriranje podatkov. Medtem, ko je uporaba ročnega načina vzpostavljanja vzajemnega zaupanja in dogovora o ključu primerna le za manjša in pretežno statična okolja, pa večina izvedb protokola IPsec uporablja samodejni način. To področje pokriva specifikacija Internetni dogovor o ključu IKE (Internet Key Exchange) ali trenutno izpopolnjena različica IKEv2, ki je sestavni del določil protokola IPsec. In čeprav je mogoče uporabiti tudi druge protokole, sta privzeta protokola specifikacije IKE:

- dogovor o ključu OAKLEY,
- internetna varnostna zveza in protokol upravljanja s ključi ISAKMP (Internet Security Association and Key Management Protocol).

Protokoli dogovora o ključu so jedro sistemov za zaščito podatkov, ki temeljijo na šifriranju in bistveni element protokola IPsec. Prilagodljiv ter varen mehanizem preverjanja identitete, overjanja sodelujočih strani in dogovora o močnem ključu v internetu, brez ročnega posredovanja, je namreč nuja za zagotavljanje učinkovite in varne komunikacije in protokol OAKLEY je tak mehanizem. Poleg protokola OAKLEY je sicer mogoče uporabiti tudi nekatere druge protokole dogovora o ključih, npr. sam protokol Diffie-Hellman, protokol RSA itd.

Za obliko in način prenosa podatkov v procesu preverjanja identitete in overjanja sodelujočih strani, dogovora o ključu ter za vzpostavljanje in upravljanje varnostnih zvez SA, je potrebno vpeljati neko dosledno skupno ogrodje, ki vse to zagotavlja. Protokol ISAKMP določa tako ogrodje, ki je sicer popolnoma neodvisno od uporabljenih tehnik za dosego tega. Protokol ISAKMP torej določa, kako se parametri protokola OAKLEY obravnavajo in prenašajo v sporočilih ISAKMP, medtem ko je protokol OAKLEY v svojem bistvu namenjen dogovoru o ključu med sodelujočima stranema. Zato je slednji popolnoma združljiv s protokolom ISAKMP. Poleg tega specifikacija protokola ISAKMP natančno določa obliko in način izmenjave podatkov, namenjenih vzpostavljanju varnostnih zvez SA ter funkcionalnost njihovega upravljanja.

Na tem mestu velja poudariti, da so v določilih Internetnega dogovora o ključu IKE uporabljene tudi nekatere funkcionalnosti protokola SKEME (A Versatile Secure Key Exchange Mechanism for Internet), ki sicer določa uporabo večjega števila mehanizmov dogovora o ključu in njegovega osveževanja ter zaščite identitete sodelujočih strani.

6.1 Protokol OAKLEY

Protokol OAKLEY je splošni protokol dogovora o ključu, kar pomeni, da so osnove delovanja podane brez podrobnih določil izvedbe. Protokol zagotavlja varno overjanje sodelujočih strani, zaščito njune identitete in dogovor o ključu ali natančneje izmenjavo zaupnih šifrirnih podatkov med njima za izračun skrivnega ključa v skupni rabi brez uporabe šifriranja. Temelji na protokolu dogovora o ključu Diffie-Hellman, zagotavlja pa še dodatne mehanizme, ki nadgrajujejo ta protokol ali odpravljajo njegove šibkosti:

- omogoča razdeljevanje ključev zunanjega izvora tako, da jih šifrira,
- zagotavlja overjanje protokola Diffie-Hellman za preprečevanje napada »man-in-the-middle«,
- uporablja naključna števila (nonce) za preprečevanje napadov s ponovitvami,
- uporablja piškotke (cookies) za preprečevanje napadov z izčrpavanjem sistemskih virov,
- določa način izbire matematičnih funkcij za uporabo v algoritmu Diffie-Hellman.

Protokol OAKLEY omogoča uporabo več načinov preverjanja identitete in overjanja sodelujočih strani: overjanje z digitalnim podpisom, kjer vsaka stran podpiše ali šifrira zgostitveno vrednost (hash) izmenjanih parametrov, npr. ID uporabnika in naključnih števil (nonces), overjanje z javnim ključem, kjer vsaka stran šifrira izmenjane parametre s pošiljateljevim javnim ključem, overjanje z izboljšanim načinom uporabe javnih ključev, overjanje z uporabo algoritma Kerberos, ki je med drugim uporabljen v Microsoftovi izvedbi IPsec, overjanje z uporabo predhodno določenega ključa ali skrivnosti v skupni rabi itd. V primeru skrivnosti v skupni rabi se le ta ročno dodeli obema stranema, v vseh ostalih primerih pa mora biti za zagotavljanje vzajemnega zaupanja med posameznimi sodelujočimi stranmi vzpostavljena zunanja, samostojna, zaupanja vredna entiteta. V primeru overjanja z digitalnimi potrdili je to infrastruktura javnih ključev PKI (Public Key Infrastructure), ki skrbi za upravljanje in razdeljevanje digitalnih potrdil z zasebnimi in javnimi ključi ter seznama preklicanih potrdil CRL, v primeru overjanja z algoritmom Kerberos pa center za razdeljevanje ključev KDC (Key Distribution Center).

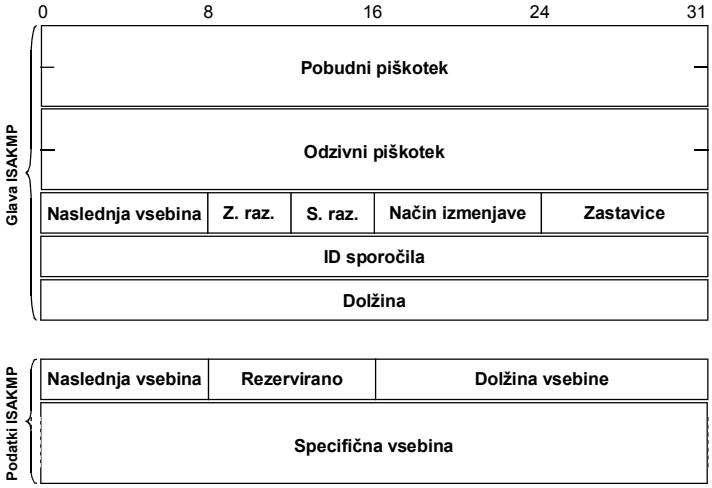
Delovanje protokola OAKLEY lahko strnemo v dva načina:

- osnovni način (Main Mode),
- agresivni način (Aggressive Mode).

Skupni učinek obeh načinov je, da sta obe strani medsebojno overjeni. Vendar pa se z agresivnim načinom overjanje obeh sodelujočih strani izvede z manjšim številom izmenjanih sporočil, seveda brez zaščite njune identitete. Dodatno ta način postavlja še nekaj omejitev, npr. prejemnik ne more odločati o izbiri matematične funkcije algoritma Diffie-Hellman. Po zaključenem procesu overjanja si lahko obe strani varno izmenjata zaupne šifrirne podatke za izračun skrivnega ključa v skupni rabi ali za dogovor o ključu in podatke za vzpostavljanje ustrezne varnostne zveze. Izračunani skrivni ključ se kasneje uporabi s šifrirnimi algoritmi overjanja izvora in zagotavljanja celovitosti podatkov ter šifriranja podatkov (varnostni storitvi AH in ESP) ter za nekatere druge varnostne namene protokola IPsec.

6.2 Protokol ISAKMP

Internetna varnostna zveza in protokol upravljanja s ključi ISAKMP določa obliko sporočil in način prenosa podatkov za overjanje sodelujočih strani in prenosa zaupnih šifrirnih podatkov za dogovor o skrivnem ključu. To pomeni, da podpira delovanje protokola OAKLEY. Poleg tega določa obliko sporočil in postopke za dogovarjanje o parametrih pri vzpostavljanju varnostne zveze SA, za njeno vzdrževanje med komunikacijo ter ukinitev po zaključeni



Slika 5. Oblika sporočila ISAKMP

komunikaciji med obema stranema. Ko sta sodelujoči strani medsebojno overjeni in dogovorjeni o skupnem ključu (npr. s protokolom OAKLEY), si strani izmenjata dodatne zaupne podatke, iz katerih se določa vsebina parametrov varnostne zveze SA v procesu njenega vzpostavljanja. Oblika sporočil ISAKMP je pri tem popolnoma neodvisna od uporabljenih varnostnih mehanizmov, npr. uporabljenega dogovora o ključu, storitev overjanja izvora in zagotavljanja celovitosti podatkov ter šifriranja podatkov, šifrirnih algoritmov itd. Na sliki 5 je prikazana oblika sporočila ISAKMP.

Sporočilo ISAKMP je sestavljeno iz glave in najmanj enega sklopa podatkov, medtem ko je vsak sklop podatkov sestavljen iz splošne glave podatkov in podatkov samih. Posamezna polja glave sporočila ISAKMP so:

- Pobudni piškotek (Initiator Cookie): piškotek strani, ki je pobudnica vzpostavitve varnostne zveze SA, obveščanja o njej ali njene ukinitve.
- Odzivni piškotek (Responder Cookie): piškotek strani, ki se odziva na pobudo vzpostavitve varnostne zveze SA.
- Naslednja vsebina (Next Payload): polje določa vrsto naslednjih podatkov v sporočilu ISAKMP, npr. podatkov varnostne zveze SA, digitalnega potrdila, proizvajalca itd.
- Zgornja različica (Major version): polje določa najvišjo različico protokola ISAKMP, ki je pri trenutni izvedbi v uporabi.

- Spodnja različica (Minor version): polje določa najnižjo različico protokola ISAKMP, ki je pri trenutni izvedbi v uporabi.
- Način izmenjave (Exchange Type): polje določa način izmenjave sporočil ISAKMP. Načini izmenjave sporočil so osnovna izmenjava, izmenjava Zaščita identitete, izmenjava Samo overjanje, agresivna izmenjava in informativna izmenjava.
- Zastavice (Flags): polje določa specifične možnosti izmenjave sporočil ISAKMP. Tako je lahko npr. nastavljen šifrirni bit (encryption bit), ko so vsi podatki za glavo sporočila ISAKMP šifrirani, potrditveni bit (commit bit), ko se želi zagotoviti, da se šifrirni podatki med sodelujočima stranema izmenjajo šele po vzpostaviti varnostne zveze SA itd.
- ID sporočila (Message ID): enolični identifikator sporočila ISAKMP.
- Dolžina (Length): celotna dolžina glave in podatkov sporočila ISAKMP v zlogih (bytes).

Splošno glavo podatkov sestavljajo naslednja polja:

- Naslednja vsebina (Next Payload): vrednost polja določa vrsto naslednjih podatkov v sporočilu ISAKMP. Če so trenutni podatki zadnji v sporočilu, je vrednost polja enaka 0.
- Rezervirano (Reserved): polje je rezervirano za uporabo v prihodnosti.
- Dolžina vsebine (Payload Length): vrednost polja določa celotno dolžino sklopa podatkov, glave podatkov in podatkov samih.

Vsebina sama pa je lahko naslednjih vrst:

- Vsebina varnostne zveze (Security Association Payload): podatki so namenjeni uporabi v procesu dogovarjanja o parametrih pri vzpostavljanju varnostne zveze SA, o pogojih, pri katerih pride do tega dogovarjanja in za določanje vrednosti identifikatorja DOI (Domain of Interpretation).
- Vsebina predloga (Proposal Payload): podatki so namenjeni uporabi v procesu dogovarjanja o parametrih pri vzpostavljanju varnostne zveze SA. Določajo uporabljeno varnostno storitev (AH, ESP) in šifrirne algoritme ter vrednost SPI pošiljatelja.
- Transformacijska vsebina (Transform Payload): podatki so namenjeni uporabi v procesu dogovarjanja o parametrih pri vzpostavljanju varnostne zveze SA, določajo pa šifrirne algoritme, ki so na voljo in med katerimi mora prejemnik izbrati ustreznega ali ga preprosto zavrniti. Šifrirni algoritmi so določeni z vrednostjo ID in atributi, ki med drugim določajo tudi namen njihove uporabe, npr. šifrirni algoritem AES-CBC za varnostno storitev ESP.
- Vsebina dogovora o ključu (Key Exchange Payload): podatki so namenjeni podpori različnim protokolom dogovora o ključu. Primeri teh protokolov so Diffie-Hellman (osnovni protokol ali njegove dopolnjene različice), OAKLEY, RSA itd.

- Vsebina preverjanja identitete (Identification Payload): podatki so namenjeni preverjanju identitete obeh sodelujočih strani, lahko pa dodatno služijo tudi za ugotavljanje verodostojnosti teh podatkov. Primer takih podatkov je naslov IP.
- Vsebina digitalnega potrdila (Certificate Payload): podatki so namenjeni prenosu digitalnih potrdil, seznama preklicanih potrdil CRL in drugih s tem povezanih podatkov. Primeri podprtih digitalnih potrdil so potrdila, ki ustrezajo standardu X.509, PGP, SPKI itd.
- Vsebina zahteve po digitalnem potrdilu (Certificate Request Payload): podatki so namenjeni izvedbi zahteve po digitalnih potrdilih. Določajo dovoljene vrste potrdil in entitet za overjanje CA.
- Zgostitvena vsebina (Hash Payload): podatki določajo zgostitveno vrednost sporočila ali stanja ISAKMP. Ta vrednost torej zagotavlja celovitost sporočila ISAKMP, lahko pa je uporabljena tudi za overjanje sodelujočih strani v procesu dogovarjanja o parametrih pri vzpostavljanju varnostne zveze SA.
- Vsebina podpisa (Signature Payload): podatki so namenjeni zagotavljanju celovitosti sporočila ISAKMP (podobno kot pri zgostitvenih podatkih zgoraj), le da gre v tem primeru za podpis, s katerim se dodatno zagotavlja storitev onemogočanja zanikanja identitete podpisnika (non-repudiation).
- Vsebina naključnega števila (Nonce Payload): podatki so namenjeni prepoznavanju veljavnosti sporočil izmenjave in s tem zaščiti zoper podvajanje paketov IP.
- Vsebina obveščanja (Notification Payload): podatki so namenjeni prenosu vsebine informativnega značaja, npr. sporočil o napakah ali stanju varnostne zveze SA. Znotraj posameznega sporočila ISAKMP je možnih več takih podatkov.
- Vsebina brisanja (Delete Payload): podatki so namenjeni določanju neveljavnosti varnostnih zvez SA, ko jih pošiljatelj izbriše iz svoje podatkovne zbirke SAD.
- Identifikacija proizvajalca (Vendor ID): podatki so namenjeni izključno proizvajalcem za prepoznavanje svojih implementacij pri uvajanju novih funkcionalnosti in istočasnemu ohranjanju združljivosti s predhodnimi različicami.

Zgoraj naštete vsebine so torej uporabljene pri ustvarjanju sporočil ISAKMP, ki se izmenjujejo med obema sodelujočima stranema. Pri tem protokol ISAKMP omogoča pet različnih načinov izmenjave teh sporočil:

- Osnovna izmenjava (Base Exchange): Ta način omogoča istočasen dogovor o ključu in izmenjavo podatkov za overjanje sodelujočih strani, vendar pa zaradi tega ni zagotovljena zaščita identitete. Med obema stranema se tako izmenjajo štiri sporočila.
- Izmenjava Zaščita identitete (Identity Protection Exchange): Pri tem načinu je dogovor o ključu ločen od izmenjave podatkov za overjanje sodelujočih strani, s čimer se zagotavlja tudi zaščita identitete, vendar pa se s tem poveča število izmenjanih sporočil med obema sodelujočima stranema na skupno šest sporočil.

- Izmenjava Samo overjanje (Authentication Only Exchange): Ta način omogoča le izmenjavo podatkov za overjanje sodelujočih strani. Obe strani sta s tem medsebojno overjeni, vendar pa se ne dogovorita o ključu v skupni rabi. Prednost tega načina izmenjave je v hitrosti in manjši procesni moči, saj se ne izvedejo računsko in časovno zahtevne operacije šifriranja, sodelujoči strani pa si izmenjata le tri sporočila.
- Agresivna izmenjava (Aggressive Exchange): Ta način omogoča istočasno dogovor o ključu in izmenjavo podatkov za overjanje sodelujočih strani z minimalnim številom izmenjanih sporočil (3), vendar pa tudi v tem primeru ni predvidena zaščita identitete.
- Informativna izmenjava (Informational Exchange): To je najenostavnejši način izmenjave sporočil ISAKMP med dvema sodelujočima stranema, saj se v tem primeru izvede le enosmerni prenos podatkov za vzpostavljanje in upravljanje varnostnih zvez SA.

7 Uporaba protokola IPsec

Glavna uporaba protokola IPsec je danes osredotočena predvsem na gradnjo navideznih zasebnih omrežij VPN za povezovanje prostorsko ločenih lokalnih omrežij in za povezovanje domačega ali prenosnega računalnika z lokalnim omrežjem podjetja. Najbolj splošno uporabna izvedba protokola IPsec je pri tem izvedba z varnostno storitvijo ESP v tunelskem načinu delovanja z vklopljenim overjanjem podatkov in z uporabo protokolov samodejnega dogovora o ključu ter vzpostavljanja in upravljanja varnostnih zvez SA, npr. protokolov OAKLEY in ISAKMP. Le tako lahko dosežemo, da so podatki, ki se pretakajo v internetu, v resnici »skriti« pred drugimi uporabniki interneta in tudi overjeni, dogovor o ključu in izmenjava drugih zaupnih podatkov med dvema sodelujočima stranema pa samodejna. Ostale izvedbe, ki jih protokol IPsec sicer dopušča, so namenjene predvsem nekaterim bolj specifičnim potrebam, čeprav se zdi, da gre le za zagotavljanje združljivosti za nazaj.

Na tem mestu velja omeniti varnostno nadgradnjo standarda IEEE 802.1x za vzpostavitev varnega brezžičnega omrežja. Standard namreč ne podaja določil za varno komunikacijo med overiteljem, vstopno točko in strežnikom za overjanje RADIUS skozi nenadzorovana vrata, skozi katera se izmenjujejo zahteve po overjanju in skrivni ključ prek protokola RADIUS. Izvedba je prepuščena proizvajalcem in pogostokrat ni dovolj varna. Komunikacijo bi lahko dodatno varnostno zaščitili z izvedbo protokola IPsec med vstopno točko in strežnikom RADIUS.

7.1 Izvedbe protokola IPsec v operacijskih sistemih

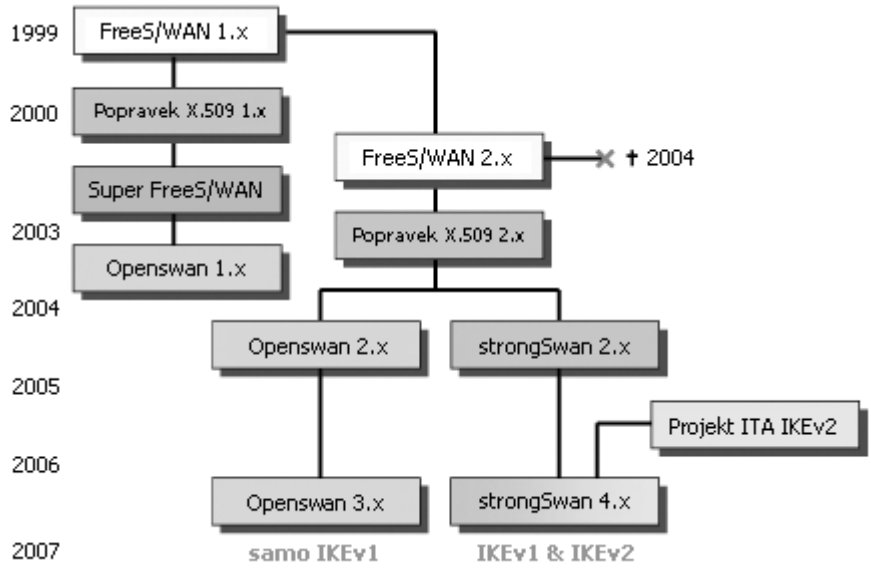
V nadaljevanju so podane nekatere izvedbe protokola IPsec najpogosteje uporabljenih operacijskih sistemov: Linux, Mac OS X, DragonFly BSD, NetBSD, FreeBSD, OpenBSD, Microsoft Windows in Cisco IOS. Poleg omenjenih izvedb je seveda še veliko drugih, ki so

namenjene predvsem ozko usmerjenim ali profesionalnim operacijskim sistemom, npr. IBM AIX, HP UX, VxWorks itd.

(a)Operacijski sistem Linux

Projekt FreeS/WAN je bil prvi projekt odprtokodne izvedbe celotnega protokola IPsec za Linux in Unix. Izvedba vključuje modul jedra imenovan KLIPS, delovanje pa temelji na procesu (daemon) za dogovor o ključu in varnostnih zvezah SA imenovanim *pluto*. Osnovni namen projekta je bil realizacija ideje oportunističnega šifriranja (Opportunistic Encryption), kjer bi se ves promet IP v internetu privzeto overjal in šifriral brez predhodnega dogovarjanja o tem. V primeru neuspele komunikacije z zaščitenimi paketi IP, pa bi se samodejno izvedla nezaščitena komunikacija. Projekt je bil leta 2004 razpuščen, ne da bi ideja v resnici zaživela. Vendar pa je bil projekt osnova za nastanek in razvoj dveh novih projektov, projekta Openswan in strongSwan. Evolucija razvoja je prikazana na sliki 6.

Izvorna izvedba FreeS/WAN 1.x uporablja zgolj ključe RSA za overjanje sodelujočih strani. Predvsem zaradi nekompatibilnosti s standardom X.509 in posledično digitalnimi potrdili je bil projekt obsojen na neuspeh. Zato je bila kmalu zatem razvita nova izvedba protokola imenovana Super FreeS/WAN, ki je bila kasneje preimenovana in distribuirana pod imenom Openswan 1.x. Ta izvedba temelji na izvorni kodi FreeS/WAN 1.x, nadgrajeni z dodatki za podporo standardu X.509, za podporo prevajanju omrežnih naslovov NAT (Network Address Translation), za zaznavanje neaktivnih strani (Dead Peer Detection), za možnost uporabe dodatnih šifrirnih algoritmov itd. Vzporedno s tem razvojem je potekal tudi razvoj izvedbe FreeS/WAN 2.x. Medtem, ko izvedba FreeS/WAN 1.x deluje z jedri operacijskega sistema Linux 2.0, 2.2 in 2.4 z uporabo lastnega modula KLIPS, deluje izvedba FreeS/WAN 2.x tudi z jedrom 2.6 operacijskega sistema Linux z uporabo modula NETKEY, ki je izvorni modul operacijskega sistema Linux.



Slika 6. FreeS/WAN in evolucija nadaljnjega razvoja

Izvedba FreeS/WAN 2.x je bila tako osnova za razvoj dveh novih izvedb, Openswan 2.x in strongSwan 2.x. Openswan 2.x je izvedba celotnega protokola IPsec za operacijski sistem Linux z jedri 2.0, 2.2, 2.4 in 2.6. Razvoj trenutne izvedbe Openswan 3.x je osredotočen predvsem na delovanje z jedrom 2.6 operacijskega sistema Linux z uporabo modula KLIPS in z vgrajenimi strojnimi šifrirnimi pospeševalniki. StrongSwan 2.x pa je izvedba celotnega protokola IPsec za operacijski sistem Linux z jedri 2.4 in 2.6, ki se osredotoča predvsem na razvoj močnih varnostnih mehanizmov overjanja sodelujočih strani. Osnova teh mehanizmov je uporaba digitalnih potrdil z javnimi ključi po standardu X.509, ki so lahko varno shranjena tudi na pametnih karticah z uporabo standarda PKCS#11, prevajanje omrežnih naslovov NAT, overjanje sodelujočih strani XAUTH itd. Trenutna izvedba strongSwan 4.x podpira oba protokola, IKEv1 in IKEv2. Za podporo protokolu IKEv1 služi proces *pluto*, ki je bil v to izvedbo vključen iz prejšnje, medtem ko za podporo protokolu IKEv2 služi proces *charon*.

Omenjeni modul jedra KLIPS ni bil nikoli vključen v samo jedro operacijskega sistema Linux. Prav tako ni bil v jedro tega operacijskega sistema vključen modul projekta KAME, opisan v naslednji točki. V jedro 2.6 je izvorno vključen modul NETKEY, ki je bil v resnici razvit na novo konec leta 2002. Za komunikacijo z jedrom operacijskega sistema uporablja protokol PF_KEY, za upravljanje s ključi pa vmesnik XFRM. Tako je popolnoma združljiv s procesi za dogovor o ključu in varnostnih zvezah SA projektov FreeS/WAN, Openswan in strongSwan, pa tudi s procesi projekta KAME. Na tem mestu velja poudariti, da dajejo različne izdaje operacijskega sistema Linux prednost različnim izvedbam protokola IPsec.

(b)Operacijski sistemi DragonFly BSD, NetBSD, FreeBSD, OpenBSD in Mac OS X

Operacijski sistemi BSD vključujejo izvedbo protokola IPsec, ki temelji na projektu KAME. Projekt je leta 1998 podprlo več Japonskih podjetij, katerih namen je bil odprtokodna izvedba

protokola IPsec in IPv6 za vse operacijske sisteme temelječe na sistemu BSD Unix (tudi OpenBSD). Proces (daemon) za dogovor o ključu in varnostnih zvezah SA s podporo protokolu IKEv1 so pri projektu imenovali *racoon*, projekt pa se je uradno zaključil leta 2006.

Nadaljevanje razvoja protokola IPsec operacijskih sistemov BSD je prevzela delovna skupina v okviru projekta RACOON2 pod okriljem projekta WIDE. Rezultat je dodatna podpora protokolom IKEv2 in KINK, še vedno pa je podprt tudi protokol IKEv1. Zaradi možnosti podpore več protokolom sta tudi struktura izvedbe in konfiguracija protokola IPsec drugačni. Tako so za delovanje potrebni trije prikriti procesi: *spmd*, *iked* in *kinkd*. Proces *spmd* služi za upravljanje politik IPsec in za shranjevanje preslikav med naslovi IP in polnimi internetnimi domenskimi imeni FQDN. Proces vedno deluje v kombinaciji s skritim procesom *iked*, ki služi za izvedbo protokolov IKEv1 in IKEv2 ali s skritim procesom *kinkd*, ki služi za izvedbo protokola KINK. Oba procesa za dogovor o ključu in varnostnih zvezah SA komunicirata z jedrom operacijskega sistema prek protokola PF_KEYv2 in vmesnika XFRM.

Izvedbo protokola IPsec projekta KAME je mogoče dobiti tudi v operacijskih sistemih OpenBSD, vendar pa je bila za ta operacijski sistem dodatno razvita lastna izvedba protokola, katerega prikriti proces je imenovan preprosto *isakmpd*. Izvedba podpira protokol IKEv1, ne pa tudi IKEv2, možno pa jo je vključiti tudi v druge operacijske sisteme, npr. NetBSD, FreeBSD, Linux itd.

Operacijski sistem Mac OS X vključuje pretežni del operacijskega sistema FreeBSD, med drugim tudi izvedbo protokola IPsec, torej izvedbo projekta KAME.

(c)Operacijski sistemi Windows 2000, XP, 2003, 2008 in Vista

Izvedbo in vključitev protokola IPsec v omenjene operacijske sisteme sta složno načrtovala podjetji Microsoft in Cisco. Želeli sta izvedbo, ki je skladna z določili standarda in združila Ciscotovo storitev ISAKMP/IKE z Microsoftovim gonilnikom jedra IPsec. Poleg tega je izvedba protokola načrtovana tako, da je neposredno vključena v strukturo Microsoftovega aktivnega direktorija AD (Active Directory) in posledično povezana s storitvijo grupne politike (Group Policy). S to storitvijo je mogoče nastavitve IPsec določati na ravni domene (domain), mesta (site), organizacijske enote (organizational unit) ali pa tudi samo za posamezne računalnike in uporabnike. Izvedba protokola vključuje tri glavne sestavne dele, ki skupaj z npr. gonilnikom TCP/IP in storitvijo CryptoAPI zagotavljajo delovanje protokola IPsec:

- Agent upravljanja politik (Policy Agent),
- Modul IKE,
- Gonilnik IPsec.

Agent upravljanja politik deluje kot storitev (service) operacijskega sistema Windows. Naloga agenta je pridobivanje in razdeljevanje politik IPsec, ki jih je predhodno določil skrbnik. Storitev najprej pridobi politiko IPsec iz ustrezne shrambe (AD, nabor lokalnih politik ali

lokalni predpomnilnik) in nato ustrezne parametre politike razdeli med modul IKE (varnostne nastavitve in nastavitve overjanja) in gonilnik IPsec (filtri IP).

Modul IKE je ključni sestavni del Microsoftove izvedbe protokola IPsec, ki se zažene na poziv storitve agenta za upravljanje politik. Njegova naloga je zagotavljanje procesa dogovarjanja o parametrih pri vzpostavljanju zaupanja vredne povezave med sodelujočima stranema in varnostne zveze SA, na podlagi varnostnih nastavitev, ki jih dobi od agenta.

Naloga gonilnika IPsec je vzdrževanje zaupanja vredne povezave med sodelujočima stranema in uporaba filtrov IP, na podlagi katerih se pakete IP blokira, dovoli prenos nezaščitenih ali varnostno obdela.

Izvedba protokola IPsec v operacijskih sistemih Windows torej temelji na uvedbi politik, ki v bistvu določajo delovanje protokola IPsec. Posamezne politike so sestavljene iz več različnih pravil, le ta pa določajo različne metode overjanja in šifriranja ter filtre IP, s katerimi se filtrira posamezen paket IP. V posameznem operacijskem sistemu Windows se istočasno lahko izvaja le ena politika.

(d)Operacijski sistem Cisco IOS

Operacijski sistemi IOS so vgrajeni v Ciscove omrežne naprave (usmerjevalniki, stikala, požarni zidovi itd.) in vključujejo lastno izvedbo protokola IPsec, ki je sestavni del operacijskega sistema Cisco IOS različice 11.3(3)T in novejših različic.

7.2 Priporočila

Na podlagi analiz posameznih izvedb protokola IPsec, ki jih je izvedla kriptografska skupnost, so bile ugotovljene in dokazane različne varnostne luknje, tako na teoretični osnovi kot tudi s praktičnimi primeri napadov. Večina teh ugotovitev je v obliki priporočil vključena v standard. Zato je za izvedbo protokola IPsec z najvišjo možno varnostjo smiselno brezpogojno upoštevati ta priporočila, kot tudi nekatera dodatna pravila dobre rabe, ki jih protokol posebej ne določa ali jih celo dopušča:

- priporoča se dosledno upoštevanje vseh varnostnih navodil in priporočil standarda IPsec: izvedba mehanizmov preverjanja politik vhodnega in izhodnega prometa in postopkov upravljanja s fragmenti, preverjanje sporočil ICMP, nadzor delovanja protokola in zapis dogodkov v nadzorno datoteko, zagotavljanje skladnosti med različnimi izvedbami protokola IPsec itd.;
- priporoča se preverjanje šifrirnih zapolnjevalnih bitov;
- odsvetuje se uporaba šifriranega odgovora na zahtevo v čistopisu in obratno;
- odsvetuje se uporaba transportnega načina delovanja varnostnih storitev AH in ESP;
- odsvetuje se uporaba varnostne storitve AH;
- priporoča se uporaba varnostne storitve ESP z aktivirano možnostjo overjanja izvora in zagotavljanja celovitosti podatkov;

- priporoča se prilagoditev varnostne storitve ESP tako, da se poleg tajnopisa overja tudi šifrirni ključ, s katerim se tajnopis dešifrira;
- odsvetuje se uporaba mehanizma za izločanje šibkih ključev (šifrirni algoritmi z velikim številom šibkih ključev, ki predstavljajo varnostno grožnjo za sistem, naj se preprosto ne uporabljajo);
- priporoča se izboljšanje formul za izračun vrednosti SKEYID in ustreznih povezanih vrednosti;
- priporoča se izboljšanje določil za izračun zgostitvene vrednosti (hash), predvsem zaradi učinkovitejšega overjanja izvora in zagotavljanja celovitosti podatkov;
- priporoča se sprememba postopka izračuna vrednosti KEYMAT zaradi preprečevanja izračuna istega ključa za dve različni varnostni zvezi SA v postopku dogovarjanja.

7.3 Šibkosti protokola IPsec

V tem poglavju so navedene nekatere glavne šibkosti ali varnostne luknje protokola IPsec. Varnostnih lukenj je seveda več, opazimo pa lahko, da je večina njih predvsem posledica kompleksnosti določil protokola in posledično zagotavljanja kompatibilnosti za nazaj. V primeru slednjega se zdi, kot da je zagotavljanje kompatibilnosti pomembnejše od zagotavljanja same varnosti.

Največ kritik protokola IPsec gre torej na račun kompleksnosti in nejasnosti določil protokola, brez jasno izraženih temeljnih načel, namena ali cilja, kaj se želi s protokolom doseči. Protokol namreč ne določa uporabe obveznih varnostnih mehanizmov in storitev, ampak podaja neke vrste smernice. Znotraj teh je mogoče uporabiti celo vrsto varnostnih mehanizmov in storitev, o katerih se obe strani lahko medsebojno dogovorita. Seveda je zaradi tega protokol bolj prilagodljiv različnim situacijam, ampak tudi bolj ranljiv, saj omogoča več različnih načinov za dosego istega ali podobnega rezultata. Poleg tega so vse ugotovitve o varnostnih luknjah protokola v določila dodane le kot priporočila, kako se jim v izvedbah izogniti. Kritiki kompleksnosti določil protokola IPsec opozarjajo na to, da je kompleksnost določil vsakega protokola istočasno tudi sinonim za šibko varnost le tega.

Možnost uporabe varnostne storitve ESP ali šifriranja podatkov brez overjanja izvora in zagotavljanja celovitosti podatkov je ena izmed varnostnih šibkosti protokola IPsec, ki bi jo lahko pripisali kompleksnosti njegovih določil. Protokol IPsec namreč dopušča možnost take izvedbe. V laičnih krogih se predpostavlja, da preverjanje celovitosti v primeru šifriranja podatkov ni nujno, saj dešifriranje z napačnim ključem proizvede le neuporabno besedilo. Žal to ni res. Splošno znano dejstvo je tudi, da izvedba overjanja za procesom šifriranja teoretično ne zagotavlja večje varnosti. Zato tudi uporaba kombinacije varnostne storitve AH znotraj storitve ESP, ko je za overjanje izvora in zagotavljanje celovitosti podatkov storitve ESP dodatno uporabljena storitev AH, ne doprinese k večji varnosti. Šibko varnost protokola IPsec pa dosežemo tudi v primeru, ko je overjanje podatkov izvedeno ločeno od šifriranja, npr. v višjih ravneh modela OSI. Šifriranje in overjanje podatkov se v tem primeru izvedeta v

različnih točkah ali ob različnih trenutkih, kar predstavlja varnostno luknjo za morebitni napad. Omenjeno varnostno luknjo protokola je izpostavil že Bellovin ob izdaji prve različice določil protokola IPsec, katerega teoretični napad z izbranim čistopisom temelji na predpostavki, da:

- napadalec lahko dostopa do vsaj ene sodelujoče strani z uporabniškimi pravicami;
- napadalec lahko prisluškuje prometu (bere, spreminja ali briše podatke) ali aktivno dodaja nove pakete;
- sodelujoči strani uporabljata enojen ključ, kar pomeni, da se ključ ne spremeni z novim uporabnikom ali z vzpostavitvijo nove povezave;
- izvedba protokola ne vključuje različnih varnostnih politik preverjanja zapolnjevalnih bitov šifriranih paketov v procesu sprejema le teh in dopušča možnost šifriranega odgovora na zahtevo v čistopisu ali obratno.

Trenutna določila standarda sicer podajajo dodatna priporočila za zaščito zoper ta napad v obliki zahteve po varnostnih politikah preverjanja zapolnjevalnih bitov šifriranih paketov, vendar pa vse izvedbe protokola IPsec teh priporočil še vedno ne upoštevajo.

Poleg tega napada so znani napadi [8] novejšega datuma na izvedbe protokola IPsec z varnostno storitvijo ESP brez overjanja izvora in zagotavljanja celovitosti podatkov, tako v tunelskem kot tudi transportnem načinu delovanja, ki izkoriščajo ravno zahtevo po varnostnih politikah preverjanja zapolnjevalnih bitov, kar je pogoj za zaščito pred napadom Bellovin. Napadi so prilagodljivi, zelo učinkoviti in predvsem realni. Možno je namreč izvesti kriptoanalizo šifriranih paketov v realnem času pri uporabi kateregakoli šifrirnega algoritma pri katerikoli dolžini ključa. Napadi so bili uspešno izvedeni izvorno na izvedbi protokola IPsec v operacijskem sistemu OpenSolaris, klonila pa je tudi izvorna izvedba protokola v operacijskem sistemu Linux, izvedbi Openswan in strongSwan ter izvedbe v operacijskih sistemih FreeBSD, NetBSD in OpenBSD. Velika verjetnost pa je, da napadom podležejo tudi nekatere izvedbe protokola IPsec v drugih operacijskih sistemih. Pri teh napadih samo s tajnopisom (ciphertext-only attack), ki potrebujejo le manjšo količino tajnopisa, je dovolj prisluškovati šifriranemu prometu in aktivno vriniti vanj nekaj napadalčevih paketov. Osnova ideje napadov je, kako vplivati na izbrana polja notranje glave paketa IP, šifriranega z varnostno storitvijo ESP tako, da prejemnik zaradi tega dosledno odgovarja s sporočili o napakah ICMP, ki potujejo po omrežju in jih protokol IPsec ne blokira. Napadi temeljijo na spremembah polj Internet Header Length (IHL), Protocol, Time to Live (TTL) ali Identification v glavi paketa IP, ki jih napadalec pošilja prejemniku in pri katerih se polji Header Checksum in Total Length ne smeta spremeniti. Prejemnik pa na napake odgovarja s sporočili ICMP le, če je zagotovljeno preverjanje zapolnjevalnih bitov v repu ESP šifriranega paketa IP tako, kot to določajo priporočila standarda in je oblika polj repa ESP taka, da paket ni preprosto zavržen brez odgovora. Sporočila o napakah ICMP so sicer šifrirana, vendar je njihova dolžina ponavljajočega vzorca, zato jih je mogoče v omrežju enostavno odkriti. Prisotnost ali odsotnost sporočil ICMP je torej tisti vir informacije, ki razkriva pravilnost ali

nepravilnost podatkov repa in na podlagi katere se posledično dešifrira celoten paket IP. Napadalec namreč pošilja prejemniku različno spremenjene pakete IP, v odgovor pa dobiva za ustrezno spremenjene pakete vedno enaka sporočila o napakah ICMP. S temi podatki tako postopoma dešifrira paket IP in posledično šifrirane podatke. Ideja napadov je nadgradnja osnutka o odkrivanju informacij šifriranih podatkov na osnovi pravilnosti ali nepravilnosti podatkov zapolnjevalnih bitov, ki jo je predstavil Vaudenay [10] in nadgradil Canvel z realnimi napadi na protokol SSL/TLS [11]. Iz tega preprosto sledi, da je vsaka izvedba protokola IPsec z varnostno storitvijo ESP brez overjanja izvora in zagotavljanja celovitosti podatkov ranljiva, tako v tunelskem kot tudi transportnem načinu delovanja, čeprav upošteva priporočila standarda po zagotavljanju preverjanja zapolnjevalnih bitov. Pravzaprav tudi zaradi tega. Vendar pa določila protokola IPsec, kljub znanim napadom, še vedno dovoljujejo take izvedbe.

Dodatna kritika protokola IPsec gre na račun pomanjkljivosti varnostne storitve AH, tako v transportnem kot tudi tunelskem načinu njenega delovanja, saj je nekompatibilna s storitvijo prevajanja omrežnih naslovov NAT. Storitev NAT se uporablja za preslikavo zasebnih ali notranjih naslovov IP v javne ali zunanje in obratno. V postopku te preslikave se glava paketa ali natančneje naslov IP paketa spremeni. Ker pa je naslov IP pri varnostni storitvi AH vključen v izračun vrednosti ICV, bo tak paket IP pri prejemniku takoj zavržen. Vrednost ICV je izračunana z uporabo skrivnega ključa, ki je poznan le pošiljatelju in prejemniku, zato je v usmerjevalniku NAT po preslikavi naslova IP nemogoče ponoviti izračuna te vrednosti. Podobno velja za storitev prevajanja naslovov vrat PAT (Port Address Translation), ki se uporablja za preslikavo več notranjih ali zasebnih v en sam zunanji ali javni naslov IP. Poudariti je seveda treba, da omenjena pomanjkljivost ne velja za varnostno storitev ESP, saj v tem primeru glava paketa IP ni niti šifrirana niti overjena.

8 Zaključek

Protokol IPsec sestavljajo kompleksna, celo ohlapna določila. Ta določila dopuščajo veliko različnih pristopov, katerih izbira je v veliki meri prepuščena izvedbam posameznih proizvajalcev. Že zaradi tega so možne različne varnostne luknje, npr. možnost izvedbe s storitvijo ESP brez overjanja in zagotavljanja celovitosti podatkov, kompleksna specifikacija IKE z izmenjavo velikega števila sporočil, ki dopušča napade preprečevanja storitve DoS itd. Zato tudi ne moremo govoriti o neki splošni varnosti, ko analiziramo varnost internetnega prometa v omrežjih IP z izvedbo protokola IPsec, ampak je treba obdelati vsako posamezno izvedbo posebej, še posebej zato, ker je protokol tako široko zastavljen.

Določila protokola IPsec se sicer z leti dopolnjujejo, predvsem na pobudo kriptografske skupnosti, ki z analiziranjem različnih izvedb protokolov opozarja na njihove možne pomanjkljivosti. Vendar pa je med teorijo, določili standarda, izvedbo in uporabo šifrirnih mehanizmov pri končnem uporabniku pogostokrat velika vrzel ter zato dolga pot od enega do

drugega konca te verige. Izsledki kriptografske skupnosti so sicer večinoma vključeni v določila protokola, vendar le kot dodatna priporočila in zato proizvajalcem ne preprečujejo, da pošiljajo na trg varnostno šibke ali nepopolne izvedbe protokola IPsec. Za spodbujanje izvedb učinkovitega protokola IPsec bi morala biti določila protokola bolj natančno določena in restriktivna, vsi načini izvedb, kot tudi varnostni mehanizmi in šifrirni algoritmi, ki so teoretično ali praktično dokazani kot varnostno šibki, pa s protokolom prepovedani. Kompleksnost določil protokola in posledično izvedbe protokola z varnostnimi luknjami ostajajo torej še vedno realnost.

Kljub kritikam omogoča protokol IPsec, z upoštevanjem ustreznih pravil in priporočil izvedbe ter z ustrezno močnimi šifrirnimi algoritmi, trenutno najvišjo možno varnost internetnega prometa na ravni paketov IP, še posebej v kombinaciji s standardom X.509, torej z infrastrukturo javnih ključev PKI in digitalnimi potrdili. Najbolj splošno uporabna izvedba protokola IPsec je pri tem izvedba z varnostno storitvijo ESP v tunelskem načinu delovanja, z vklopljenim overjanjem izvora in zagotavljanjem celovitosti podatkov, z uporabo protokolov samodejnega dogovora o ključu ter vzpostavljanja in upravljanja varnostnih zvez SA.

Ker pa celotna varnost sloni na najšibkejšem členu verige, je uspeh neposredno odvisen tudi od izvedbe same in delovnega okolja, v katerem je protokol uporabljen. Učinkovitost implementacije protokola IPsec je namreč odvisna tudi od dejavnikov in mehanizmov, ki niso neposredno pod okriljem določil standarda, npr. od uporabe operacijskih sistemov z varnostnimi luknjami in slabimi generatorji naključnih števil, napačne ali slabe uporabe sicer močnih šifrirnih algoritmov, površnih postopkov in praks pri upravljanju s sistemi, slabe zaščite izvora podatkov, neupoštevanja varnostnih politik in pravilnikov, nedoslednega upoštevanja vseh določil protokola itd. Poleg tega je varnost računalniških sistemov in omrežij v širšem kontekstu odvisna tudi od fizičnih in predvsem človeških dejavnikov. Ravno slednji so ključnega pomena za zagotavljanje najvišje možne varnosti internetnega prometa v omrežjih IP.

Zagotavljanje varnosti internetnega prometa v omrežjih IP, pa tudi informacijske varnosti in varnosti sploh, ni stanje, temveč proces in protokol IPsec je pomemben kamenček v mozaiku tega procesa.

Literatura

[1] Sasa Jurišić: Računalniška varnost in kriptografija (prosojnice s predavanj na Fakulteti za računalništvo in informatiko), Ljubljana, 2008, http://lkrv.fri.uni-lj.si/~ajurisic/kirv08/prosojnice.html.

[2] Denis Trček: Managing Information Systems Security and Privacy, Ljubljana, 2006.

[3] S. Kent, K. Seo: Security Architecture for the Internet Protocol, 2005, http://www.ietf.org/rfc/rfc4301.txt.

[4] S. Kent: IP Authentication Header, 2005, http://www.ietf.org/rfc/rfc4302.txt.

[5] S. Kent: IP Encapsulating Security Payload (ESP), 2005, http://www.ietf.org/rfc/rfc4303.txt.

[6] Edward C. Kaufman: Internet Key Exchange (IKEv2) Protocol, 2005, http://www.ietf.org/rfc/rfc4306.txt.

[7] N. Ferguson, B. Schneier: A Cryptographic Evaluation of IPsec, Counterpane Internet Security, Inc., 2000, http://www.schneier.com/paper-ipsec.html.

[8] Jean Paul Degabriele, Kenneth G. Paterson: Attacking the IPsec Standards in Encryption-only Configurations, IEEE Symposium on Security and Privacy 2007, pp. 335-349, http://eprint.iacr.org/2007/125.pdf.

[9] Kenneth G. Paterson, Arnold K.L. Yau: Crptography in Theory and Practice - The Case of Encryption in IPSec, S. Vaudenay (Ed.): Advances in Cryptology - EUROCRYPT 2006, LNCS Vol. 4004, pp. 12-29, Springer-Verlag 2006, http://eprint.iacr.org/2005/416.pdf

[10] S. Vaudenay: Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS..., L.R. Knudsen (Ed.): Advances in Cryptology - EUROCRYPT 2002, LNCS Vol. 2332, pp. 534-545, Springer-Verlag 2002, http://lasecwww.epfl.ch/pub/lasec/doc/Vau02a.ps.

[11] B.Canvel, A.P. Hiltgen, S. Vaudenay, M. Vuagnoux: Password Interception in a SSL/TLS Channel, D. Boneh (Ed.): Advances in Cryptology - CRYPTO 2003, LNCS Vol. 2729, pp. 583-599, Springer-Verlag 2003, http://canvel.free.fr/crypto/pdf/crypto03.pdf