HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

IKE i IKEv2 protokoli

CCERT-PUBDOC-2007-09-205

CARNet CERT u suradnji s LS&S

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

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

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

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

Sadržaj

1. Uvod

IPSec je skup protokola stvoren od strane IETF (eng. *Internet Engineering Task Force*) standardizacijskog tijela s ciljem osiguravanja IPv4 i IPv6 protokola. Sigurnosne mogućnosti ovog protokola uključuju povjerljivost, autentifikaciju podataka i njihovu zaštitu od neovlaštenih izmjena. IPSec se sastoji od tri pod-protokola: AH (eng. *Authentication Heder*), ESP (eng. *Encapsulating Security Payload*) i IKE (eng. *Internet Key Exchange*) protokola.

IKE je protokol za ostvarivanje sigurnosnog udruživanja (eng. *Security Association - SA*) unutar IPsec (eng. *IP security*) skupa protokola. Sigurnosno udruživanje podrazumijeva razmjenu sigurnosnih podataka između dva mrežna subjekta, a s ciljem uspostavljanja sigurne komunikacije među njima.

IKE protokol postoji u dvije inačice: IKEv1 (odnosno IKE) i IKEv2. Iako je prva inačica ovog protokola fleksibilna te posjeduje brojne i raznolike mogućnosti, njegova složenost predstavlja značajnu zapreku popularizaciji. IKEv2 protokol nastao je evolucijom prve inačice protokola, značajno je jednostavniji i razumljiviji te pokazuje bolje performanse.

U nastavku je dan prikaz IPSec skupina protokola, s naglaskom na ulogu IKE protokola. Slijedi kratak opis ISAKMP, Oakley i SKEME protokola na kojima se IKE protokol temelji, te opis dviju faza IKE protokola. Nakon prikaza razloga za uvođenje nove inačice IKE protokola slijed opis funkcionalnosti IKEv2 protokola i njegova kvantitativna usporedba s prvom inačicom protokola.

2. Primjena IKE protokola u IPSec skupini protokola

2.1. IPSec skupina protokola

IPSec je skupina protokola namijenjen osiguravanju IP (eng. *Internet Protocol*) komunikacije korištenjem autorizacije i/ili kriptiranjem IP podatkovnih paketa. Ovaj protokol sadrži i različite protokole za razmjenu kriptografskih ključeva.
Sigurnosni protokoli prilagođeni korištenju na Internetu, kao što su SSL (eng. *Secure Socket Layer*), TLS (eng. *Transport Layer Security*) i SSH (eng. *Secure Shell*) protokoli, djeluju na transportnom sloju i slojevima iznad njega (slojevi 4 do 7 OSI modela). Za razliku od spomenutih protokola, IPsec djeluje na mrežnom sloju, trećem sloju OSI (eng. *Open System Interconnection*) mrežnog modela, što ga čini fleksibilnijim i omogućuje mu zaštitu komunikacije prema protokolima 4. sloja, kakvi su popularni TCP (eng. *Transmission Control Protocol*) i UDP (eng. *User Datagram Protocol*) protokoli. Dodatna prednost IPSec protokola pred sigurnosnim protokolima viših slojeva je u tome što za njegovo korištenje nisu potrebne izmjene programskog koda aplikacija koje ga koriste.
IPSec protokol IP mrežama pruža sljedeće sigurnosne karakteristike:

- Nepovredivost podataka – osigurava postojanost podataka tako što onemogućuje njihovo neovlašteno stvaranje, izmjenu ili brisanje na putu od pošiljaoca ka primatelju.
- Autorizacija – jamči da su primljeni podaci istovjetni poslanima te da zapis o identitetu pošiljatelja odgovara stvarnom pošiljaocu.
- Tajnost – omogućuje privatnost podataka tako da samo naznačeni primatelji znaju što se šalje. Pošiljatelj podatke prije slanja kriptira korištenjem kriptografskih algoritama i kriptografskih ključeva. Ovako dobiveni šifrirani podaci se šalju, a njih je izrazito teško dekodirati bez odgovarajućeg kriptografskog ključa.
- Sigurnost neovisna o aplikaciji – IPsec sigurnosna zaglavlja umeću se između standardnih zaglavlja IP protokola i podataka koji pripadaju višim slojevima OSI modela. Zbog toga svaka IP usluga, kakve su *telnet*, FTP i *sendmail*, te svaka korisnička aplikacija koja koristi IP, na primjer *TCP BSD Socket* i *XTI Streams* aplikacije, mogu koristiti IPsec protokol bez prilagodbi.

2.2. Uloga IKE protokola unutar IPSec skupine protokola

IPSec sadrži tri pod-protokola:

- AH protokol koristi se kod osiguravanja nepovredivosti podataka i njihove autorizacije.
- ESP protokol omogućuje tajnost i nepovredivost podataka te se koristi kod njihove autorizacije. Njegovo zaglavlje sadrži i redni broj poruke te pruža oblik zaštite od napada ponovnim slanjem podataka.
- IKE protokol koristi se za stvaranje i distribuiranje kriptografskih ključeva pomoću kojih se stvaraju ESP i AH zaglavlja. Ovaj protokol pored toga provodi provjeru identiteta udaljenog računalnog sustava te time ESP i AH protokolima omogućuje autorizaciju podataka.

Prije no što IPSec pošalje autorizirane ili kriptirane podatke, pošiljatelj i primalac moraju usuglasiti korištene protokole te enkripcijske algoritme i ključeve. Ovaj se postupak provodi pomoću IKE protokola. Osim toga, IKE protokol provodi primarnu autorizaciju, odnosno utvrđivanje identiteta udaljenog računala prije usuglašavanja kriptografskih algoritama i protokola.

3. Osnova IKE protokola

IKE protokol razvio se na temelju tri starija protokola:

- ISKAMP (eng. *Internet Security Association and Key Management Protocol*),
- Oakley i
- SKEME (eng. *Versatile Secure Key Exchange Mechanism for Internet*).

ISAKMP pruža okvir za implementaciju autentifikacije i razmjene ključeva, ali ih ne definira. Oakley i SKEME protokoli definiraju niz tehnika razmjene ključeva.

3.1. ISAKMP

ISAKMP protokol definira postupke:

- autentifikacije učesnika komunikacije,
- stvaranja i upravljanja SA udruživanjem,
- tehnike stvaranja kriptografskih ključeva i
- izbjegavanja sigurnosnih prijetnji.

Ovim protokolom određeni su formati podatkovnih paketa korištenih za uspostavljanje, usuglašavanje, izmjenu i brisanje SA udruživanja. Sigurnosna udruženja sadrže sve podatke potrebne za izvođenje različitih mrežnih sigurnosnih usluga, kao što su:

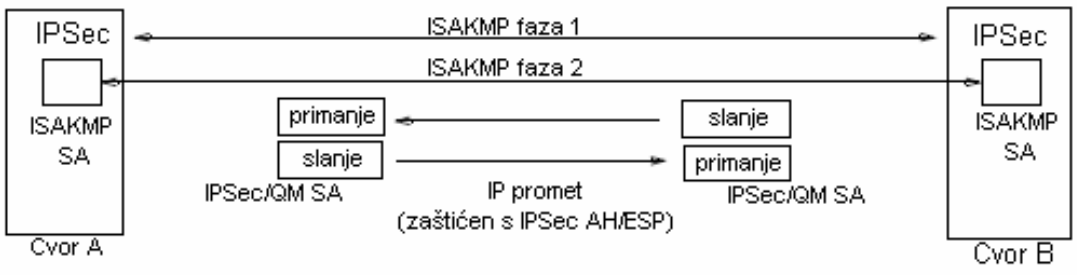
- usluge IP sloja, npr. autentifikacija zaglavlja i ugrađivanje sadržaja, tzv. *payload encapsulation*,
- usluge transportnog i aplikacijskog sloja te
- samozaštita vlastitog prometa.

ISAKMP protokol pored toga definira podatkovne strukture za razmjenu enkripcijskih ključeva i autorizacijskih podataka, a koje su neovisne o načinu stvaranja ključeva, enkripcijskim algoritmima i mehanizmima autorizacije.

Uspostavljanje SA udruživanja prema ISAKMP protokolu unutar IKE protokola provodi se u dvije faze:

1. MM (eng. *Main Mode*), prva faza ISAKMP protokola odvija se također u dva koraka:
   - Dogovaranje i uspostavljanje ISAKMP SA udruživanja, sigurnog komunikacijskog kanala za daljnju ISAKMP komunikaciju. Dva sustava stvaraju dijeljenu Diffie-Hellman vrijednost na kojoj se temelji dijeljeni simetrični ključ. Pomoću spomenutog ključa kriptira se sav daljnji ISAKMP promet.
   - Utvrđivanje identiteta udaljenog sustava, tzv. primarna autorizacija.
2. QM (eng. *Quick Mode*), druga faza ISAKMP protokola, korištenjem sigurnog komunikacijskog kanala stvorenog u MM fazi, uspostavlja jedno ili više IPSec SA udruživanja. Uobičajeno je uspostavljanje dvaju SA udruživanja, jednog za primanje i jednog za slanje.

Opisani postupak uspostavljanja SA udruživanja prikazan je slikom Slika 1.



Slika 1: Uspostavljanje SA udruživanja prema ISAKMP protokolu unutar IKE protokola

ISAKMP protokol moguće je implementirati na bilo kojem protokolu transportnog sloja OSI mrežnog modela. Pri tome sve implementacije moraju sadržavati mogućnost slanja i primanja putem UDP porta 500.

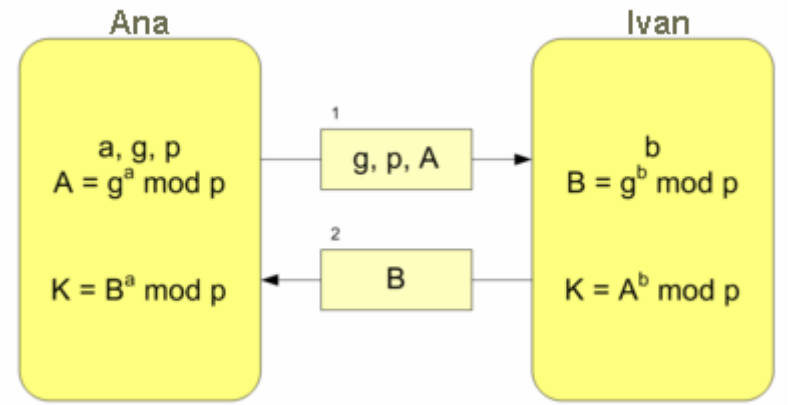
3.2. Oakley

Oakley je protokol za usuglašavanje enkripcijskih ključeva (eng. *key-agreement protocol*) koji autoriziranim korisnicima omogućuje sigurnu razmjenu podataka o ključevima preko nesigurne veze korištenjem Diffie-Hellman (DH) protokola.

3.2.1. Diffie-Hellman protokol

DH algoritam prvi puta su 1976. godine objavili Whitfield Diffie i Martin Hellman, iako je kasnije utvrđeno kako je ranije osmišljen unutar britanske obavještajne agencije GCHQ (eng. *Government Communications Headquarters*) od strane Malcoma J. Williamsona.

DH razmjena ključeva dvama korisnicima, koji nemaju prethodnih saznanja jedan o drugome, omogućuje zajedničko uspostavljanje tajnog dijeljenog ključa preko nesigurnog komunikacijskog kanala. Radi se o anonimnoj razmjeni ključeva, dakle DH protokol ne provodi autentifikaciju korisnika.



Slika 2: Izvorni algoritam DH razmjene ključeva

Na slici Slika 2 prikazan je izvorni algoritam DH razmjene ključeva, koji je ujedno i najjednostavniji. Prikazana razmjena izvodi se u pet koraka:

1. Ana i Ivan dogovaraju korištenje primarnog broja *p=23* i baza *q=5*.
2. Ana odabire tajni cijeli broj *a=6* te Ivanu šalje:
$$g^a \bmod p = 5^6 \bmod 23 = 8$$
3. Ivan odabire tajni cijeli broj b=15 te Ani šalje:
$$g^b \bmod p = 5^{15} \bmod 23 = 19$$
4. Ana proračunava:
$$(g^b \bmod p)^a \bmod p = 19^6 \bmod 23 = 2$$
5. Ivan proračunava:
$$(g^a \bmod p)^b \bmod p = 8^{15} \bmod 23 = 2$$

U posljednjem koraku oba korisnika došla su do iste vrijednosti koju je potom moguće koristiti kao tajni dijeljeni ključ. Pri tome je za sigurnu implementaciju potrebno odabrati znatno veće vrijednosti parametara *a* i *b*, kako bi se otežao napad metodom pokušaja i pogreške.

3.3. SKEME

SKEME protokol omogućuje:

- razmjenu ključeva temeljenu na javnim ključevima, na centrima za distribuciju ključeva te razmjenu putem vlastoručne instalacije,
- brzo i sigurno osvježavanje ključeva,
- PFS (eng. *Perfect Forward Secrecy*) i
- promjenu korištenih kriptografskih oznaka.

Ovaj je protokol podijeljen u tri osnovne faze:

1. SHARE,
2. EXCH i
3. AUTH.

3.3.1. SHARE faza SKEME protokola

Tijekom prve faze SKEME protokola uspostavlja se ključ K_0 između korisnika *A* i *B* kojima su međusobno prethodno poznati samo javni ključevi. SHARE faza ne autorizira korisnike niti dijeljeni ključ K_0 već pruža bazičnu razinu sigurnosti: ako korisnik *A* ispravno koristi protokol tada može biti siguran da nikome osim korisniku *B* dijeljeni ključ K_0 nije poznat, iako pri tome nije zagarantirano da korisnik *B* posjeduje ključ K_0. Isto vrijedi i u obrnutom smjeru.

Korisnici tijekom ove faze razmjenjuju polovice ključa, kriptirane korištenjem javnih ključeva drugog korisnika, te nakon toga izgrađuju tajni dijeljeni ključ pomoću jednosmjerne funkcije (eng. *hash*) *H*:

1. $A \rightarrow B: PKE_B(K_A)$

Korisnik *A* korisniku *B* šalje svoju polovicu ključa K_A kriptiranu javnim ključem (eng. *Public Key Encription – PKE*) korisnika *B*.

2. $B \rightarrow A: PKE_A(K_B)$
   Korisnik *B* korisniku *A* šalje svoju polovicu ključa K_B kriptiranu javnim ključem korisnika *A*.
3. $K_0 = H(K_A, K_A)$
   Oba korisnika iz polovica ključa K_A i K_B konstruiraju dijeljeni tajni ključ K_0 zajedničkom jednosmjernom funkcijom *H*.

3.3.2. EXCH faza SKEME protokola

Tijekom druge faze SKEME protokola korisnici razmjenjuju Diffie-Hellman eksponente. Ova je faza neovisna o SHARE fazi. Koraci u kojima se provodi EXCH faza su:

1. $A \rightarrow B: g^x \bmod p$
   Korisnik *A* korisniku *B* šalje DH eksponent $g^x \bmod p$.
2. $B \rightarrow A: g^y \bmod p$
   Korisnik *B* korisniku *A* šalje DH eksponent $g^y \bmod p$.

3.3.3. AUTH faza SKEME protokola

Posljednja, treća, faza SKEME protokola provodi autentifikaciju DH eksponenata razmijenjenih tokom EXCH faze. Autentifikacija se provodi korištenjem dijeljenog tajnog ključa, utvrđenog SHARE fazom:

1. $A \rightarrow B: F_{K0}(g^y, g^x)$
   Korisnik *A* korisniku *B* šalje autentifikacijsku vrijednost proračunatu iz usuglašenog dijeljenog ključa i razmijenjenih DH eksponenata.
2. $B \rightarrow A: F_{K0}(g^x, g^y)$
   Korisnik *B* korisniku *A* šalje autentifikacijsku vrijednost proračunatu iz usuglašenog dijeljenog ključa i razmijenjenih DH eksponenata.

4. Funkcionalnosti IKE protokola

IKE protokol temelji se na usuglašavanju SA udruženja među dvama korisnicima. Sigurnosno udruženje je kombinacija dogovorenih ključeva, protokola i SPI (eng. *Security Parameter Index*) indeksa, koja definira sigurnosne parametre potrebne za zaštitu komunikacije između pošiljaoca i primatelja. SPI indeks predstavlja jedinstvenu identifikacijsku vrijednost unutar SA udruženja koja se koristi za razlikovanje različitih sigurnosnih udruženja prisutnih na istom računalu. Na primjer, na računalu koje istovremeno provodi sigurnosnu komunikaciju s nekoliko računala može biti prisutno više udruženja. Ovo je čest slučaj kod računala koja djeluju kao poslužitelji datoteka ili poslužitelji za udaljeni pristup, a koja poslužuju veći broj klijenata. Računalo koje prima podatkovni paket u takvim situacijama koristi SPI indeks za određivanje kojem SA udruženju će primljeni paket biti pridijeljen.

4.1. Faze IKE protokola

Razmjena ključeva prema IKE protokolu provodi se u dvije faze:

1. Prva faza IKE protokola odnosi se na usuglašavanje MM (eng. *Main Mode*) SA udruživanja.
2. Tijekom druge faze IKE protokola provodi se usuglašavanje QM (eng. *Quick Mode*) SA udruživanja.

4.1.1. Prva faza IKE protokola

Prva faza IKE protokola odnosi se na usuglašavanje sigurnosne politike koja obuhvaća niz sigurnosnih parametara korištenih tijekom provođenja IKE protokola. Zajednička sigurnosna politika mora biti prihvaćena od strane oba korisnika. Nakon usuglašavanja sigurnosne politike, prihvaćeni sigurnosni parametri pridjeljuju se SA udruživanju kod svakog korisnika te se tako dobivena sigurnosna udruživanja koriste za svu daljnju IKE komunikaciju. Moguće je definirati veći broj sigurnosnih politika s pridruženim prioritetima. Time se povećava vjerojatnost postojanja identičnih sigurnosnih politika kod dvaju korisnika.

Ovu fazu moguće je implementirati MM (eng. *Main Mode*) i AM (eng. *Aggressive Mode*) metodama, pri čemu svaka IKE implementacija mora sadržavati MM metodu, dok je AM metoda preporučena. MM metoda predstavlja IKE implementaciju IPE (eng. *Identity Protect Exchange*) razmijene iz ISAKMP protokola. Prve dvije poruke razmijenjene u sklopu ove metode odnose se na dogovaranje sigurnosne politike, sljedeće dvije poruke razmjenjuju DH javne vrijednosti, a posljednje dvije MM poruke autentificiraju razmijenjene DH javne vrijednosti.
AM metoda je IKE inačica AE (eng. *Aggressive Exchange*) razmjene iz ISAKMP protokola. Prve dvije poruke ove metode usuglašuju sigurnosnu politiku i razmjenjuju DH javne vrijednosti. Drugom porukom se autentificira korisnik koji odgovara na zahtjev dok se trećom porukom autentificira korisnik inicijator komunikacije.
Bez obzira na korištenu metodu, tijekom prve faze IKE protokola provode se sljedeći koraci:

1. **Dogovaranje sigurnosne politike**, u okviru kojega se utvrđuju sljedeći parametri:
   - Enkripcijski algoritam:
     - DES (eng. *Data Encription Standard*) ili
     - 3DES (eng. *Triple DES*).
   - Algoritam jednosmjerne funkcije (eng. *hash algorithm*):
     - MD5 (eng. *Message Digest algorithm 5*) ili
     - SHA1 (eng. *Secure Hash Algorithm*).
   - DH grupa:
     - Grupa 1 – ključ dug 768 bita,
     - Grupa 2 – ključ dug 1024 bita ili
     - Grupa 2048 – ključ dug 2048 bita.
   - Metoda autentifikacije:
     - dijeljeni ključ (eng. *preshared key*),
     - potpis s javnim ključem (eng. *public key signature*),
     - enkripcija javnim ključem (eng. *public key encription*) ili
     - revidirana enkripcija javnim ključem (eng. *revised public key encription*).
2. **Razmjena DH javnih vrijednosti** tijekom koje se ne razmjenjuju DH ključevi, već samo podaci potrebni DH algoritmu za utvrđivanje dijeljenog tajnog ključa. Nakon ove razmijene IKE protokol na oba računala konstruira glavni ključ (eng. *master key*) koji se koristi za zaštitu postupka autentifikacije.
3. **Autentifikacija** se provodi kako bi se onemogućilo izvođenje napada preusmjeravanjem prometa (eng. *man-in-the-middle attack*). Svi podaci prenošeni tijekom postupka autentifikacije zaštićeni su jednosmjernom funkcijom te kriptirani DH ključem stvorenim u drugom koraku. Spomenuti podaci obuhvaćaju:
   - oznaku identiteta, koja se razlikuje ovisno o odabranoj metodi autentifikacije:
     - za autentifikaciju certifikatom to je jedinstveno (eng. *distinguished*) i opće (eng. *general*) ime certifikata,
     - za autentifikaciju Kerberos V5 protokolom ili dijeljenim ključevima to je IPv4 adresa,
     - ako se autentifikacija provodi na temelju FQDN (eng. *Fully Qualified Domain Name*) imena oznaka identiteta sadrži FQDN oznaku korisnika.
   - korišteni port i
   - korišteni protokol.

Pošiljatelj započinje prvu fazu IKE protokola slanjem ponude potencijalnog SA udruživanja primatelju kojemu nije dozvoljena izmjena primljene ponude. U slučaju da se dogodi izmjena ponude, pošiljatelj odbacuje primljeni odgovor. Primatelju je na ponudu dozvoljeno odgovoriti potvrdno ili porukom koja sadrži moguće alternative ponuđenom udruženju.

4.1.2. Druga faza IKE protokola

Tijekom druge faze IKE protokola provodi se usuglašavanje SA udruživanja na razini IPSec protokola. Ova faza implementirana je QM (eng. *Quick Mode*) metodom koja se koristi za dogovaranje sigurnosnih usluga koje izlaze iz okvira ISAKMP protokola i nužna je u svakoj implementaciji IKE protokola. Pojedine implementacije mogu sadržavati i NGM (eng. *New Group Mode*) metodu koja se koristi za

definiranje privatnih skupina za DH razmjenu. QM i NGM metode nemaju analogije unutar ISAKMP protokola.
QM metoda sastoji se od sljedećih koraka:

1. **Dogovaranje sigurnosne politike**, u okviru kojega se utvrđuju sljedeći parametri:
   - IPSec protokol: AH ili ESP,
   - Algoritam jednosmjerne funkcije: MD5 ili SHA1
   - Enkripcijski algoritam: 3DES ili DES.

   Nakon odabira sigurnosne politike, na svakom računalu stvorena su dva SA udruženja: jedno za slanje i jedno za primanje.
2. **Podaci uz ključ sjednice se razmjenjuju ili osvježavaju**,
3. **SA udruženja, ključevi i SPI indeksi prosljeđuju se IPSec protokolu.**

Sva komunikacija provedena tijekom druge faze zaštićena je SA udruženjem stvorenim u okviru MM metode. Prva faza provodi zaštitu utvrđivanjem identiteta dok druga faza pojačava tu zaštitu osvježavanjem ključeva prije slanja samih podataka.
Jedno MM SA udruženje može biti korišteno za stvaranje većeg broja QM SA udruženja čime se cjelokupan proces razmjene ključeva ubrzava, a ponovno dogovaranje i ponovna autentifikacija nisu nužni dok je nadređeno MM SA udruženje aktivno. Riječ je o tome da su DH razmjene vremenski dugotrajne pa se smanjivanjem njihova broja postiže značajno poboljšanje performansi. To je osnovni motiv razlaganja IKE protokola na dvije faze. Broj dozvoljenih QM sigurnosnih udruženja određen je postavkama IPSec sigurnosne politike.

5. Razlozi za uvođenje IKEv2 protokola

IKEv2 protokol uveden je zbog:

- definiranja cjelokupnog IKE protokola jednim dokumentom, koji nadomješta dokumente RFC 2407, RFC 2408 i RFC 2409, te kako bi se u protokol ugradile izmjene koje omogućuju NAT-T (eng. *Network Address Translation – Traversal*) komunikaciju, EA (eng. *Extensible Authentication*) autentifikaciju i dohvaćanje udaljenih adresa (eng. *Remote Address acquisition*),
- pojednostavljenja IKE protokola zamjenom osam razmjena jednom razmjenom koja se provodi u četiri poruke,
- kako bi se uklonili DOI (eng. *Domain of Interpretation*), SIT (eng. *Situation*) i LDI (eng. *Labeld Domain Identifier*) polja te *Commit i Authentication only* bitovi,
- povećanja brzine IKE protokola u najuobičajenijem slučaju i to skraćivanjem prvotne razmjene na četiri poruke,
- zamijene kriptografske sintakse korištene za zaštitu IKE podatkovnih paketa sintaksom temeljenom na ESP zaglavlju kako bi se pojednostavila implementacija i sigurnosna analiza,
- smanjenja broja mogućih pogrešaka povećanjem pouzdanosti protokola: poruke se šalju u nizu i na svaku se odgovara potvrdom o primitku,
- povećanja robusnosti smanjenjem količine proračuna koje neinicijalizirajući korisnik provodi prije no što utvrdi da inicijator komunikacije prima poruke na navedenoj IP adresi te ne sudjelovanjem u razmjeni prije no što se provede kriptografska autentifikacija inicijatora,
- ispravljanja pojedinih kriptografskih slabosti,
- slanja TS (eng. *Traffic Selector*) odabira unutar zasebne poruke, umjesto zajedno s identifikacijskim podacima s ciljem povećanja fleksibilnosti,
- definiranja postupaka u slučaju pojedinih pogrešaka ili primitka nerazumljivih podataka te kako bi se olakšalo stvaranje budućih revizija protokola s unazadnom kompatibilnošću,
- pojednostavljenja i razjašnjenja postupka održavanja zajedničkog stanja u slučaju poteškoća u radu mreže ili prilikom napada uskraćivanjem usluga (eng. *Denial of Service*).

6. Funkcionalnosti i prednosti IKEv2 protokola

6.1. Prednosti IKEv2 protokola

IKEv2 protokol je u odnosu na IKE protokol jednostavniji, fleksibilniji i sigurniji.

6.1.1. Fleksibilnost i jednostavnost

Najveće i najznačajnije preinake uvedene u drugoj inačici IKE protokola odnose se na povećanje razumljivosti teksta kojim je protokol propisan kao i na značajno pojednostavljenje samog protokola. Radi se o tome da brojne analize prvoj inačici ovog protokola zamjeraju pretjeranu složenost kojom je uvelike otežana njegova implementacija. Kod IKEv2 protokola smanjen je broj faza kao i broj poruka poslanih tokom svake faze.

6.1.2. Sigurnost

Ranjivost na napade uskraćivanjem usluga značajan je nedostatak prve inačice IKE protokola koji je kod IKEv2 protokola umanjen uvođenjem zamjenskih mehanizama. Kako bi se otežali spomenuti napadi, korisnik koji nije započeo komunikaciju može od inicijatora zatražiti slanje posebne podatkovne strukture (eng. *cookie*) kako bi se potvrdila njegova vjerodostojnost.
Jedan od oblika napada uskraćivanjem usluga je slanje velikog broja zahtjeva kako bi se zauzeli svi raspoloživi procesorski i memorijski resursi na napadnutom računalu. Zbog toga je unutar IKEv2 ugrađen mehanizam prepoznavanja takvih poruka te čak i mogućnost identificiranja IP adrese s koje je napad pokrenut.

6.1.3. Nova struktura

Stalan izvor pomutnje kod prve inačice IKE protokola međuodnos je atributa, transformacija i prijedloga. Zahvaljujući hijerarhijskom prestrukturiranju navedenih pojmova druga inačica IKE protokola mnogo je shvatljivija. Na primjer, kod prve inačice protokola rok valjanosti SA udruženja dogovara se na početku stvaranja sjednice i oba korisnika moraju se pridržavati dogovorene vrijednosti tog argumenta. Kod IKEv2 protokola korisnik odabire trajanje sigurnosnog udruženja neovisno o izboru drugog korisnika.

6.2. Kvantitativna usporedba IKE i IKEv2 protokola

Kako bi se utvrdilo stvarno poboljšanje koje korisnici mogu očekivati prelaskom na drugu inačicu IKE protokola provedena je kvantitativan usporedba dvaju inačica protokola [16], čiji rezultati su ovdje preneseni. Usporedba je provedena na temelju simulacija provedenih pomoću NIIST programskog paketa.

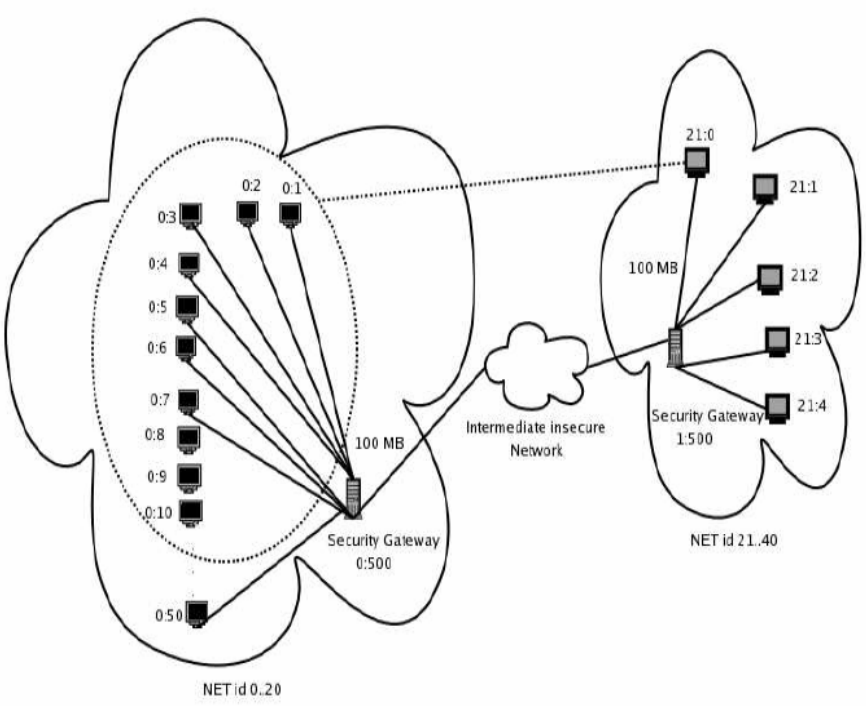
6.2.1. NIIST simulacijski alat

NIIST (eng. *NIST IPSec and IKE Simulation Tool*) je simulacijski alat razvijen od strane NIST (eng. *National Institute of Standards and Technology*) instituta. Implementiran je u Java programskom jeziku te je integriran unutar SSF (eng. *Scalable Simulation Framework*) okruženja i SSFNet (eng. *SSF Network Model*) modela kako bi omogućio simuliranje velikih računalnih mreža sa stajališta sigurnosti. NIIST je oblikovan tako da omogućuje usporedbu performansi ovisno o parametrima vezanim uz aplikacije korištene u komunikaciji (eng. *end-to-end applications*). Njime je moguće provesti detaljnu analizu IPSec/IKE protokola i njihov utjecaj na performanse protokola kao što je TCP. Pri tome se u obzir ne uzimaju sigurnosne karakteristike ispitivanih protokola.

6.2.2. Simulacijski postav

Računalna mreža simulirana s ciljem usporedbe performansi IKE i IKEv 2 protokola prikazana je slikom Slika 3. Sustav se sastoji od VPN (eng. *Virtual Private Network*) mreža međusobno povezanih preko SG (eng. *Security Gateway*) pristupnika IPSec tunelima. Tijekom analize simulirano je *N* VPN mreža od kojih svaka sadrži *M* računala i jedan SG pristupnik. Računala su s pripadajućim pristupnikom

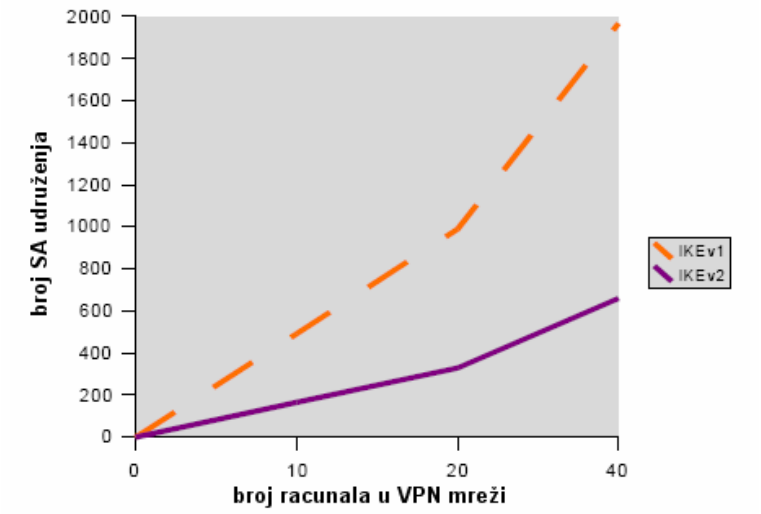
povezana vezom brzine 100 Mbps dok su pristupnici međusobno povezani WAN (eng. *Wide Area Network*) mrežom propusnosti 1.5 Mbps. Pri tome je *N/2* VPN mreža sastavljeno od 50 TCP klijenata, dok druga polovica VPN mreža sadrže svaka po 10 TCP poslužitelja. Skupine od po 10 klijenata povezane su na pojedinog poslužitelja.



Slika 3: Prikaz simulirane mreže kod kvantitativne usporedbe IKE i IKEv2 protokola

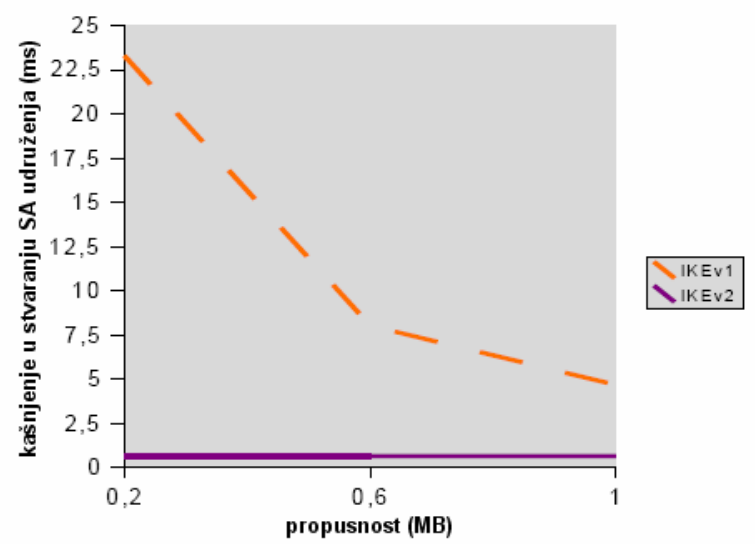
6.2.3. Rezultati

S povećanjem broja računala u VPN mrežama raste broj stvorenih SA udruženja, a s njim i opterećenje mreže. Na slici Slika 4 prikazan je utjecaj veličine mreže na broj stvorenih SA udruženja kod IKE i IKEv2 protokola.



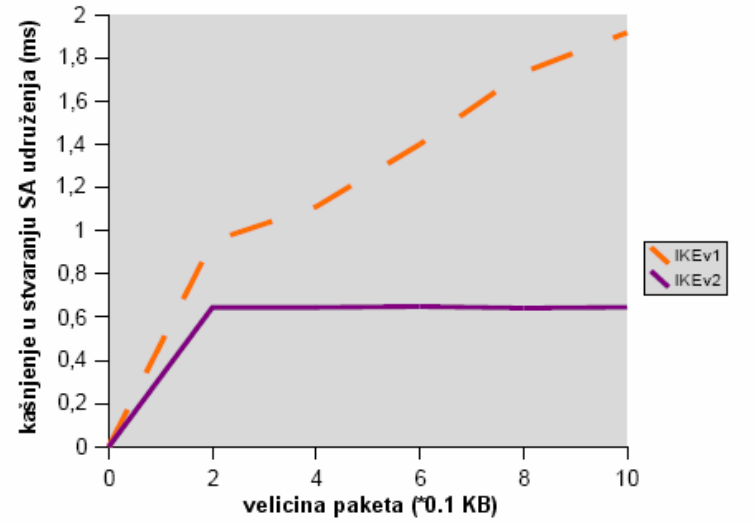
Slika 4: Utjecaj veličine VPN mreže na broj SA udruženja kod IKE i IKEv2 protokola

Ovisnost kašnjenja u stvaranju SA udruženja o raspoloživoj propusnosti veze prikazana je na slici Slika 5.

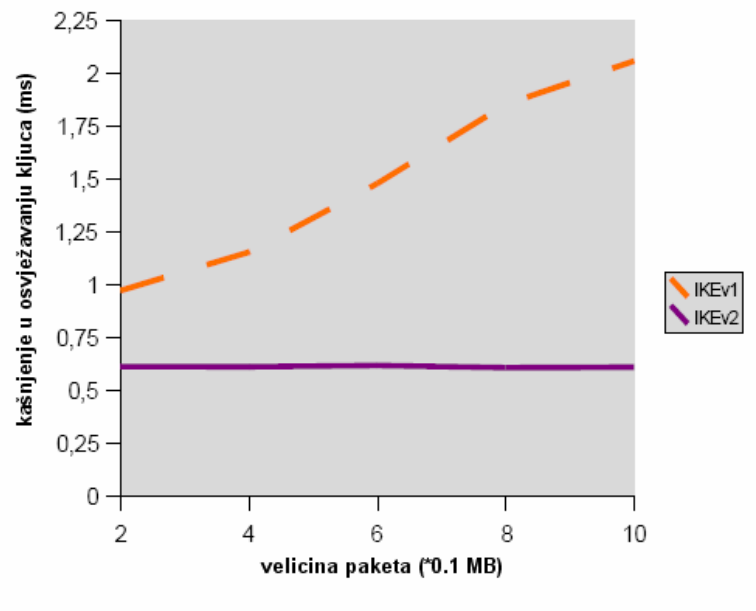


Slika 5: Utjecaj propusnosti veze na kašnjenje u stvaranju SA udruženja kod IKE i IKEv2 protokola

Veličina paketa razmjenjivanih između SG pristupnika također može značajno utjecati na performanse IKE protokola pa su na slikama Slika 6 i Slika 7 prikazane ovisnosti kašnjenja u stvaranju SA udruženja i kašnjenja u osvježavanju ključa o ovom parametru.



Slika 6: Utjecaj veličine paketa na kašnjenje u stvaranju SA udruženja kod IKE i IKEv2 protokola



Slika 7: Utjecaj veličine paketa na kašnjenje u osvježavanju ključa

7. Zaključak

IKE protokol, i njegova nova inačica IKEv2, predstavlja jedan od tri protokola koji čine IPSec skupinu protokola za osiguravanje IP komunikacije. Sigurnosne karakteristike IPSec protokola obuhvaćaju nepovredivost podataka, autentifikaciju i tajnost, a implementacija i primjena ovog protokola moguće su bez izmjena programskog koda aplikacija koje ga koriste. Pri tome je za nepovredivost podataka i njihovu autorizaciju zadužen AH protokol, ESP protokol uz autorizaciju i nepovredivost omogućuje i očuvanje tajnosti podataka, a IKE protokol se koristi za stvaranje i distribuiranje kriptografskih ključeva pomoću kojih se stvaraju ESP i AH zaglavlja.

IKE protokol razvio se na temelju triju starijih protokola. Prvi od njih je ISAKMP protokol koji pruža okvir za implementaciju autentifikacije i razmjene ključeva, ali ih ne definira. Druga dva protokola na kojima se IKE temelji, Oakley i SKEME protokoli, definiraju niz tehnika razmjene ključeva.

IKE protokol provodi usuglašavanje SA udruženja među dvama korisnicima. Sigurnosno udruženje je kombinacija dogovorenih ključeva, protokola i SPI indeksa, koja definira sigurnosne parametre potrebne za zaštitu komunikacije. IKE protokol provodi se u dvije faze. U prvoj fazi usuglašava se MM SA udruženja, a u drugoj se provodi usuglašavanje QM SA udruženja. Prva je faza računski zahtjevnija te se udruženje dogovoreno njome može koristiti za zaštitu većeg broja drugih faza protokola, čime se postiže značajno ubrzanje cjelokupne razmjene.

IKEv2 protokol nastao je evolucijom prve inačice protokola s ciljem pojednostavljenja istoga, uklanjanja određenih sigurnosnih nedostataka i kriptografskih ranjivosti te povećanja performansi. Teoretske analize kao i kvantitativne usporedbe pokazuju superiornost IKEv2 protokola nad svojim prethodnikom.

8. Reference

[1] IPsec, http://en.wikipedia.org/wiki/IPsec, rujan 2007.

[2] D. Harkins, D. Carrel: The Internet Key Exchange (IKE), http://tools.ietf.org/html/rfc2409, rujan 2007.

[3] C. Kaufman: The Internet Key Exchange (IKEv2) Protocol, http://tools.ietf.org/html/rfc4306, rujan 2007.

[4] D. Harkins, C. Kaufman, R. Perlman: Overview of IKEv2, http://www3.ietf.org/proceedings/01dec/slides/ipsec-10.pdf, rujan 2007.

[5] The Internet Key Exchange Protocol, version 2, http://reeves.csc.ncsu.edu/Classes/csc574/13-IKE.pdf, rujan 2007.

[6] HP-UX IPSec version A.01.06 Administrators Guide, http://docs.hp.com/en/J4256-90003/J4256-90003.pdf, rujan 2007.

[7] Internet Security Association and Key Management Protocol, http://en.wikipedia.org/wiki/ISAKMP, rujan 2007.

[8] Oakley protocol, http://en.wikipedia.org/wiki/Oakley_protocol, rujan 2007.

[9] Diffie-Hellman key exchange, http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange, rujan 2007.

[10] Hugo Krawczyk: SKEME: A Versatile Secure Key Exchange Mechanism for Internet, The Proceedings of the 1996 Symposium on Network and Distributed Systems Security, 1995.

[11] Internet Key Exchange Security Protocol, http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/isakmp.htm, rujan 2007.

[12] Internet Key Exchange, http://technet2.microsoft.com/windowsserver/en/library/f54655de-7129-408e-a7a9-b1a29baefa171033.mspx?mfr=true, rujan 2007.

[13] IKE, Internet Key Exchange, http://www.networksorcery.com/enp/protocol/ike.htm, rujan 2007.

[14] P.-C. Cheng: An architecture for the Internet Key Exchange Protocol, http://www.research.ibm.com/journal/sj/403/cheng.html, rujan 2007.

[15] Radia Perlman: Understanding IKEv2: Tutorial, and rationale for decisions, http://tools.ietf.org/html/draft-ietf-ipsec-ikev2-tutorial-01, rujan 2007.

[16] H.Soussi, M. Hussain, H. Afifi, D. Seret: IKEv1 and IKEv2: A Quantitative Analyses, http://www.math-info.univ-paris5.fr/~seret/paperb4F.pdf, rujan 2007.