

# IPSec

Sjálfstætt verkefni í Tölvuöryggi

Háskólinn í Reykjavík, Tölvunarfræðideild, Haustönn 2004.

Leiðbeinendur: Dr. Gísli Hjálmtýsson og Björn Brynjúlfsson.

Nemandi: Sigurjón Sveinsson.

## 1 Inngangur

Vegna eftirspurnar um örugg samskipti tveggja neta, sem fara yfir opin og ótryggt miðil sem internetið er, hafa verið þróaðar aðferðir sem kallaðar hafa verið VPN (e. Virtual Private Network). Í slíkum samskiptum er mikilvægt að þeir aðilar sem að þeim koma noti svipaða tækni fyrir samskiptin og hefur einn öryggisstaðall, IPSec, notið mikilla vinsælda við útfærslu á þessum samskiptum.

Þessi greinagerð mun fjalla um IPSec og hvað það gerir. Hinum mismunandi stöðlum, sem IPSec samanstendur af, verður lýst og þær þjónustur sem þeir veita verða kynntar.

Vegna tæknilegrar umfjöllunar verður gert ráð fyrir að lesendur þessarar greinagerðar hafi þekkingu á tölvusamskiptum og lagskiptingu þeirra, sérstaklega TCP/IP staðlinum.

## 2 Kynning á IPSec

IPSec er samsett úr nokkrum stöðlum sem IETF (e. Internet Engineering Task Force) skilgreindi. IPSec veitir öryggisþjónustur á netlagi í tölvusamskiptum.

Samskiptastaðallinn IPv4 er þeim annmörkum háður að þar er ekki gert ráð fyrir öryggisþjónustum til að tryggja auðkenningu með stafrænum skilríkjum og dulritun með lyklum. Þessar þjónustur eru því ekki útfærðar beint í þeim staðli. Til að taka á þessum annmörkum kom IETF fram með IPSec staðalinn. Staðallinn er samsettur úr nokkrum RFC (e. Request for Comments) sem taka á mismunandi þáttum staðalsins. Þessi RFC skjöl eru meðal annars RFC 2401 [7], RFC 2402 [3], RFC 2406 [2] og RFC 2409 [4]. Þess má geta að IPSec er útfært í IPv6 sem kemur til með að taka við IPv4.

### 2.1 Hverjir eru kostir IPSec?

#### 2.1.1. IPSec er staðall

IPSec er alþjóðlegur staðall sem öllum er heimilt að útfæra og margir framleiðendur netbúnaðar útfæra hann í sínum tækjum. Kostir þess að nota staðal er að með því eru öryggisþáttur netsamskiptanna ekki bundinn við einhverja sérstaka framleiðendur heldur geta tæki frá öllum þeim framleiðendum, sem útfæra IPSec í sínum búnaði, átt samskipti sín á milli. Þessi þáttur gerir það að verkum að samskiptin verða ekki háð tækjabúnaði eða hugbúnaðarlausnum frá einum eða fáum framleiðendum. Einnig geta framleiðendur skeytt saman IPSec og öðrum stöðlum eins og t.d. PPTP og þannig notast við eigin tækni ásamt IPSec.

### 2.1.2. IPsec er skalanlegt

Þegar IPsec var hannað var það haft í huga að hægt væri að dreifa IPsec á marga nethnúta. Sjálfvirkni í lykaskiptum og tengingum milli hnúta gerir það að verkum að allt utanumhald verður viðaminna og það gerir IPsec skalanlegt og stækkanlegt [1].

### 2.1.3. IPsec er útfært á netlaginu

Útfærsla IPsec fer fram á netlaginu (e. network layer) og þar með er öryggi samskiptanna ekki háð einhverjum forritum heldur geta öll samskipti milli aðila verið tryggð með IPsec

Þar sem tölvusamskipt í dag eru að langmestu leyti byggð á TCP/IP samskiptastöðlunum geta notendur sett upp IPsec og notað það óháð netbúnaði sínum og innri uppbyggingu netanna svo lengi sem að TCP/IP sé samskiptamátinn [1].

## 3 Uppbygging IPsec

IPsec samanstendur í grófum dráttum af þrem stöðlum, þar af sjá tveir um að tryggja samskiptin sjálf. IKE (e. Internet Key Exchange) sér um að miðla lykllum milli samskiptaaðila. AH (e. Authentication Header) sér um aðgangsstýringar, heilindi, upprunastaðfestingu og endurtekningarvarnir. ESP (Encapsulating Security Payload) sér um að dulrita gögnin og að dylja upplýsingar um gagnastreymi [1].

Þessir þrjú staðlað geta verið notaðir hver í sínu lagi og saman eftir því hvað aðstæður krefjast. AH og ESP notast við dreifilykla til að tryggja dulritun og auðkenningu og því þarf IKE til að dreifa lykklunum.

### 3.1 Flutningshamur og hjúpunarhamur

IPsec getur starfað í tveim hömum, flutningsham (e. transport mode) og hjúpunarham (e. tunnel mode).

#### 3.1.1. Flutningshamur

Flutningshamur tryggir ekki allan IP pakkann og er ætlaður fyrir pakkasendingar milli tveggja endastöðva. Flutningshamur er ekki útfærður á þeim hnútum sem eru milli endastöðvanna eins og í beinum og gáttum. Þetta stafar af því hvernig IP pakkar eru uppbyggðir, þeim sundrað og settir saman [1].

#### 3.1.2. Hjúpunarhamur

Til að tryggja allann pakkann þarf svokallaðan hjúpunarham. Þá er upphaflegi IP pakkinn tekinn í heild sinni og varinn með þjónustum IPsec. Nýr IP haus er settur á pakkann og hann sendur á áfangastað.

## 4 Lotur

Til að halda utan um samskipti milli tveggja aðila þurfa þessir aðilar að notast við upplýsingar varðandi samskipti þessi. Það eru aðallega tveir þættir sem þarf að nota, öryggistenging (e. Security Association) og öryggisstefna (e. Security Policy) [1].

## 4.1 Öryggistenging

Öryggistenging (e. Security Association) er nokkurs konar samningur milli tveggja aðila sem eiga í samskiptum. Þessi samningur skilgreinir alls kyns upplýsingar sem þarf að halda til haga svo að samskiptin geti farið fram. Þessar upplýsingar eru vistaðar í gagnagrunni á hverjum hnúti. Hver hnútur heldur svo utan um tvo slíka gagnagrunna, einn fyrir umferð frá honum og einn fyrir umferð til hans.

Öryggistengingar virka bara í aðra áttina, sem þýðir að tveir aðilar að samskiptum eru ekki að nota sama gagnagrunninn sín á milli heldur eru þeir með sitt hvort gagnagrunninn fyrir samskiptin. Öryggistengingar eru einnig háðar stöðlum. Þannig er ekki sama öryggistenging notuð fyrir AH og ESP í hnút þó svo að samskiptin séu við sama aðilann [1].

## 4.2 Öryggisstefna

Allir IP pakkar sem fara í gegnum netkort sem notar IPSec verða að lúta þeim reglum sem settar eru um netumferð á því netkorti. Þessar reglur eru skilgreindar í öryggisstefnunni. Ein öryggisstefna er skilgreind fyrir hvert netkort og eru þessar stefnur geymdar í SPD gagnagrunni (e. Security Policy Database) og eru tvær töflur í grunninum, eina fyrir umferð frá hnútinum og ein fyrir umferð til hans.

Í töflunum eru færslur sem skilgreina aðgerðir á öllum pökkum. Allar aðgerðir verða að vera ein af þremur: hleypa áfram (e. bypass), hafna (e. reject) eða meðhöndla (e. process). Þegar pakkar fara í gegnum netkortið eru þeir bornir saman við færslurnar í töflunum og meðhöndlaðir eins og færslurnar segja til um.

# 5 IKE lykkladreifing

Tveir hnútar sem vilja koma á samskiptum með IPSec þurfa að byrja á því að auðkenna hvorn annan. Þessi gagnkvæma auðkenning hnútanna er framkvæmd með því að nota fyrirfram ákveðna lykla eða stafræna undirskrift sem báðir hnútar deila. Þegar auðkenning hefur farið fram búa hnútarnir til lotulykla sem verða notaðir í þeim samskiptum sem eftir koma. Þessir lykklar virka aðeins í aðra áttina og þarf einn lykil fyrir hvora þjónustunna (AH og ESP) ef báðar eru notaðar. Þar af leiðandi þarf samtals fjóra lykla (tvö pör) fyrir hverja lotu. En þess ber að geta að það er ekki nauðsynlegt að nota bæði AH og ESP. Eins og kemur fram í kafla 6.3 er AH ekki nauðsynleg þjónusta og í raun vel hægt að komast af án hennar við útfærslu IPSec.

## 5.1 IKE fasar

IKE hefur tvo fasa (e. phases). Fasi 1 er notaður til gagnkvæmnar auðkenningar hnúta á jafningjagrundvelli og fara þá fram þau skipti á lyklum sem minnst var á hér að framan. Þessi samskipti sem fara fram í fasa 1 eru kölluð ISAKMP (e. Internet Security Association and Key Management Protocol) Security Association. ISAKMP Security Association hefur eigindi sem verða að fylgja og þau eru: Dulritunarreiknirit, tætifallsreiknirit, auðkenningarreiknirit og Diffie-Hellman upplýsingar [4].

Í fasa 2 fer fram dreifing á lykllum fyrir aðrar þjónustur. En í stað þess að ein tenging komist á, eins og fasa 1, þá geta komist á margar tengingar í framhaldi af fasa 2. IPSec öryggistengingar eru myndaðar í fasa 2 og ein tenging í fasa 1 getur búið til marga lotulykla fyrir fasa 2 [1].

## 5.2 IKE hamur: Aðal hamur og ýtinn hamur

Þegar IKE er í fasa 1 getur IKE verið í tveim hömum þegar skipti á lykllum fara fram: Aðal ham (e. main mode) og ýtnum ham (e. aggressive mode). Báðir hamarnir geta hvor um sig verið notaðir til að koma á traustri og auðkenndri tengingu ásamt því að koma á ISAKMP Security Association.

Aðalmunurinn á þessum tveim hömum er að ISAKMP Security Association stillingar taka sex aðgerðir í aðal hamnum en þrjú í ýtnum ham. Einnig hefur aðal hamur þann kost að bjóða upp á PFS (e. Perfect Forward Secrecy) og einkennahuld (e. identity protection). Kostur þess að hafa PFS er að þó svo að lotulyklar eða gamlir leynilyklar komist í uppnám eru eldri lyklar óhultir því ekki er hægt að draga neinar ályktanir um þá frá þeim sem eru í hættu.

## 6 ESP og AH

Það eru tveir staðlar sem sjá um að tryggja heilindi gagnanna í IPSec með auðkenningu og dulritun og þeir eru ESP (e. Encapsulating Security Payload) og AH (e. Authentication Header). Hægt er að nota þá báða í einu eða í sitt hvoru lagi og er það stillt í öryggistengingunni. Þetta þýðir að það er hægt að velja að auðkenna IPSec pakkana án þess að dulrita gögnin sjálf, dulrita gögnin án þess að tryggja auðkenningu eða hvoru tveggja í einu. En það er þó ekki mögulegt að velja hvorugan möguleikann, það verður að nota í það minnsta einn [2].

AH og ESP geta verið notaðir í flutningsham og hjúpunarham IPSec. Þegar IPSec pakkinn er búin til er það öryggistenging þeirrar sendingar sem segir til um hvorn haminn á að nota. IPSec pakkinn er svo búin til eftir þeim skilgreiningum. Munurinn á samsetningu IPSec pakkanna sést á mynd 1 og 2.

### 6.1 AH auðkenning

AH auðkenning snýst um það að viðtakandi IP pakka getur sannreynt að honum hafi ekki verið breytt á leiðinni milli sendanda og móttakanda og að hann sé sannarlega frá sendandanum. Til þess að sannreyna þessar upplýsingar eru notuð tætiföll á borð við MD5 og SHA-1 [3]. Þessi tætiföll taka dullykil og IP pakka sem inntak og með stærðfræðilegum útreikningum skila streng af ákveðinni lengd sem úrtak. Þetta úrtak er kallað prófsumma (e. checksum). Þessi strengur er mislangur eftir því hvaða reikniriti er beitt, MD5 eða SHA-1 t.d. en sem dæmi má nefna að MD5 skilar 128 bita streng sem frálagi og SHA-1 160 bita frálagi. Við gerð þessara prófsummna eru notaðir leynilyklar (e. secret key) sem sendandi og móttakandi hafa komið sér saman um og nota til þess IKE lykkladreifinguna sem er í IPSec staðlinum.

Sendandinn reiknar út prófsummu fyrir hvern IP pakka sem hann sendir frá sér án þess að taka AH hausinn með, hann er settur í eftir að prófsumman ef reiknuð. Þessi prófsumma er sett í AH haus IPSec pakkans en það fer eftir því hvort samskiptin eru stillt á hjúpunarham eða flutningsham hvar nákvæmlega í pakkann AH hausinn fer sem sjá má á mynd 1.



### 6.3 Af hverju þarf ekki nauðsynlega að útfæra AH?

Eina þjónustan sem AH veitir er að auðkenna sendandann og tryggja heilindi IP pakka. Þessa þjónustu veitir ESP einnig. Þarna er því um ákveðna skörun á þjónustu milli þessara tveggja staðla.

Niels Ferguson og Bruce Schneier hjá Counterpane Labs komu árið 1999 fram með gagnrýni á IPSec. Þar kemur fram að þessi skörun á auðkenningu milli AH og ESP flækir IPSec staðalinn og myndar þannig veikleika í öryggi IPSec [5]. Af þessum sökum ákváðu aðstandendur FreeS/WAN verkefnisins, sem útfærir IPSec, að hætta að nota AH við auðkenningu í sinni útfærslu og nota einungis ESP staðalinn [6]. Sem sýnir að það er hægt að útfæra IPSec án þess að notast við AH.

## 7 Vandamál við notkun IPSec

Það getur verið vandkvæðum háð að nota og útfæra IPSec. Sérstaklega þegar IPSec pakkar þurfa að fara í gegnum eldveggi og aðra nethnúta.

### 7.1 Tvístrun og samsetning IPSec pakka

Beinar og gáttir geta tvístrað IPSec pökkum ef þeir eru of stórir. Pakkar sem hafa verið tvístraðir þurfa þó að vera settir saman aftur áður en móttakandi beitir ESP til að dulráða gögnin eða auðkenna við móttöku.

### 7.2 NAT í eldveggjum

NAT var sett í eldveggi staðarneta til að maska eða hjúpa heilt net, jafnvel mörg net, á bak við eina IP tölu á Internetinu. Þegar IP pakkar fara í gegnum beini, sem notar NAT, út á internetið breytir beinirinn IP haus pakkans. Beinirinn skiptir um IP tölu sendanda, port númer og breytir prófsummum í TCP og UDP hausum. Við þessar breytingar og af öðrum ástæðum til viðbótar er illmögulegt að nota NAT til að áframsenda IPSec pakka í gegnum eldveggi [8].

#### 7.2.1. Prófsummur í TCP og UDP.

TCP og UDP haus er með prófsummu sem endurspeglar IP tölu og port bæði sendanda og móttakanda. Þegar venjulegir IP pakkar fara í gegnum NAT er þessum upplýsingum breytt. En í IPSec eru þessi gögn dulrituð með öllum IP pakkanum og því er ekki hægt að uppfæra þau þegar þau fara í gegnum NAT. Og af þessum sökum kemur röng summa í prófsummutékki hjá móttakanda gagnanna [8]. Þó svo að prófsumma sé valmöguleiki í UDP er það skylda að útfæra í TCP enda mun strangari staðall.

#### 7.2.2. NAT tafir í IKE UDP pökkum.

IKE lykkladreyfing fer fram með UDP pökkum. Í NAT er því oft hagað þannig að port möppun er eytt mjög fljótt vegna eðli UDP samskipta. Sá sem byrjar IKE lykklaskipti, *A*, býr til UDP porta möppun í NAT í upphafi þeirra samskipta. Þegar móttakandinn *B* ætlar svo að svara *A* getur verið að möppunin sé ekki lengur til staðar í NAT og því er UDP pakki *B* hunsaður. Með því verður rof í IKE lykkladreyfingunni og öryggistenging kemst því ekki á milli *A* og *B*.

### 7.2.3. IPSec getur ekki sent á marga hnúta í gegnum NAT

Þegar ESP dulritar IPSec pakka er ekki hægt að sjá neina TCP né UDP hausa. Þeir eru dulritaðir í pakkanum með öllu hinu og því ekki aðgengilegir án þess að dulráða pakkann. Þar af leiðandi eru allar upplýsingar TCP og UDP hausa um port möppun óþekktar og því er ekki hægt að beina þessum pökkum á marga hnúta innan staðarnets innan við NAT [8].

## 8 Lokaorð

IPSec er nokkuð viðamikill öryggisstaðall sem hefur uppfyllt vöntun á öryggi í IPv4 samskiptastaðlinum. Þegar IP staðallinn var endurskoðaður á sínum tíma, og IPv6 kom fram í framhaldi af því, var IPSec bætt við sem hluta af þeim staðli. Það má því ætla að í framtíðinni, eftir því sem IPv6 verður útbreiddara, að öryggi og upplýsingaleynd í tölvusamskiptum muni aukast og verða meðfærilegri.

## 9 Heimildaskrá

- [1] Wipur Jayawickrama, CISSP, ágúst 2003. *Demystifying IPSec: Protocols, Implementations and Limitations* Bridge Point ([www.bridgepoint.com.au](http://www.bridgepoint.com.au)).  
<http://www.bridgepoint.com.au/Documents/ipsecpaper.pdf>
- [2] Stephen Kent og Randall Atkinson, nóvember 1998. *RFC 2406 - IP Encapsulating Security Payload (ESP)*. The Internet Engineering Task Force.  
<http://www.ietf.org/rfc/rfc2406.txt>
- [3] Stephen Kent og Randall Atkinson, nóvember 1998. *RFC 2402 - IP Authentication Header*. The Internet Engineering Task Force.  
<http://www.ietf.org/rfc/rfc2402.txt>
- [4] Dan Harkins og Dave Carrel, nóvember 1998. *RFC 2409 - The Internet Key Exchange (IKE)*. The Internet Engineering Task Force.  
<http://www.ietf.org/rfc/rfc2409.txt>
- [5] Bruce Schneier og Niels Ferguson, 1999. *A Cryptographic Evaluation of IPsec*.  
<http://www.schneier.com/paper-ipsec.pdf>
- [6] Linux FreeS/WAN 09.02.2004. *AH removed from FreeS/WAN*.  
[http://www.freeswan.org/no\\_ah.html](http://www.freeswan.org/no_ah.html)
- [7] Stephen Kent og Randall Atkinson, nóvember 1998. *RFC 2401 - Security Architecture for the Internet Protocol*. The Internet Engineering Task Force.  
<http://www.ietf.org/rfc/rfc2401.txt>
- [8] Joseph Davies, ágúst 2002. *IPsec NAT Traversal Overview*.  
<http://www.microsoft.com/technet/community/columns/cableguy/cg0802.msp>